

PAPER DETAILS

TITLE: Sayisal Koruma Koalisyonu Hizli Degerlendirme Modeli: Elektronik Belgelerin Güvenilirliđi
Açısından Bir İnceleme

AUTHORS: Özhan SAGLIK

PAGES: 211-223

ORIGINAL PDF URL: <https://dergipark.org.tr/tr/download/article-file/2750428>



Bilgi Yönetimi Dergisi

Cilt: 5 Sayı: 2 Yıl: 2022

<https://dergipark.org.tr/tr/pub/by>



Hakemli Makaleler Araştırma Makalesi

Makale Bilgisi

Gönderildiği tarih: 04.11.2022
Kabul tarihi: 28.11.2022
Erken görünüm: 14.12.2022
Yayınlanma tarihi: 30.12.2022

Article Info

Date submitted: 04.11.2022
Date accepted: 28.11.2022
Date early view: 14.12.2022
Date published: 30.12.2022

Anahtar sözcükler

*Elektronik Belgeler, Sayısal
Koruma, Güvenilirlik*

Keywords

*Electronic Records, Digital
Preservation,
Trustworthiness*

DOI numarası

10.33721/by.1199232

ORCID

0000-0002-1436-7431



Sayısal Koruma Koalisyonu Hızlı Değerlendirme Modeli: Elektronik Belgelerin Güvenilirliği Açısından Bir İnceleme

*Digital Preservation Coalition Rapid Assessment Model: A
Review in Terms of Trustworthiness of Electronic Records*

Özhan SAĞLIK

Bursa Uludağ Üniversitesi Kütüphane Dokümantasyon Daire Başkanlığı Öğr.
Gör. Dr., ozhan.saglik@gmail.com

Öz

Kurumlarda oluşan ve arşivlik değere sahip olan belgelerin uzun dönemli korunması gerekir. Bunun için sayısal koruma tekniklerinden yararlanıldığı bilinmektedir. Bu teknikler, aynı zamanda belgelerin güvenilirliğinin korunmasına yardımcı olmaktadır. Kurumların sayısal koruma faaliyetlerini uygularken hangi durumda olduklarını ve gelecekte nereye varmak istediklerini değerlendirebilmek için mevcut yeteneklerin analiz edilmesi gündeme gelmekte ve bir analiz aracına ihtiyaç duyulmaktadır. Bu ihtiyacı karşılamak amacıyla pek çok model hazırlanmıştır. Bunlardan biri de Digital Preservation Coalition (DPC - Sayısal Koruma Koalisyonu) tarafından geliştirilen Hızlı Değerlendirme Modeli'dir (HDM - Rapid Assessment Model). Model, kurumların mevcut sayısal koruma yeteneklerini değerlendirirken geleceğe ilişkin de bir plan sunmaktadır. Bundan dolayı HDM'nin belgelerin uzun dönemli korunmasını hedefleyen güvenilirlikle ilişkilendirilebileceği düşünülmüştür. Bu çalışmada HDM'de belirtilen sayısal koruma yetenekleri, elektronik belgelerin (e-belge) güvenilirliği açısından incelenmektedir. Bu inceleme sonucunda hem sayısal koruma kapasitelerini değerlendirmek isteyen kurumlara bir metodolojinin zeminini oluşturmak hem de sayısal korumayla ilgili yetenekleri güvenilirlikle örtüştürmek istenmiştir. Nitel araştırma deseninden faydalanan bu çalışmada doküman analizinden yararlanılmıştır. Hem saha gözlemleri hem de yapılan araştırmalar, kurumlarda sayısal koruma yetenekleri ve güvenilirlik konusunda yeterli farkındalığın bulunmadığını göstermektedir. Durum böyle olunca çalışmanın sorusu HDM'de belirtilen yetenekler güvenilirlikle nasıl ilişkilendirilebilir şeklindedir. Çalışma sonucunda HDM'de yer alan sayısal koruma yeteneklerinin belgelerin güvenilirlik analizinde kullanılabileceği gözlenmiştir. Ancak, HDM'nin geliştirilmesi gereken yönleri de fark edilmiştir. Bunlardan biri kararlaştırılan hedeflere erişmek için somut kriterlerin belirlenmesidir. Bu kriterlerin güvenilirlik analizlerinde kullanılabileceği kanaati oluşmuştur. Yapılacak yeni çalışmalarla bu gibi kanaatlerin hipoteze dönüştürülmesi, hem kurumların sayısal koruma kapasitelerini güçlendirmelerine yardımcı olacak hem de güvenilirlik analizlerinin zenginleşmesine katkıda bulunacaktır. İşbu çalışma ile kurumlarda arşivlik değere sahip olan belgeleri daha iyi korumak noktasında bir farkındalık oluşturmaya beklenmektedir.

Abstract

Records created in organizations which have archival value should be preserved for a long time and for this reason digital preservation techniques are adopted. These techniques also help to the preservation of the trustworthiness of records. In order to evaluate the situation of organizations while implementing their digital preservation activities and where they want to reach out in the future, the analysis of the existing capabilities comes to the fore, and an analysis tool is needed. Many models have been prepared to satisfy this need. One of them is the Rapid Assessment Model (RAM) which is developed by Digital Preservation Coalition (DPC).

The model provides a plan for the future while evaluating the organizations' current digital preservation capabilities. Therefore, it is thought that RAM can be associated with the trustworthiness which aims long-term preservation of the records. In this study, the digital preservation capabilities specified in the RAM are examined in terms of the trustworthiness of electronic records.

As a result of this examination, it is aimed to both establish the basis of a methodology for organizations that want to evaluate their digital preservation capacities and to match their digital preservation capabilities with trustworthiness. In this study, the document analysis method was used as a qualitative research design. Both field observations and researches show that organizations do not have enough awareness about digital preservation capabilities and trustworthiness. Then the question of the study is how the capabilities specified in RAM can be associated with trustworthiness. As a result of the study, it has been observed that the digital preservation capabilities of RAM can be used in the trustworthiness analysis of records. However, aspects of RAM that need to be improved have also been recognized. One of them is the determination of concrete criteria to achieve the agreed aims. It has been concluded that these criteria can be adopted in trustworthiness analyzes. Transforming such opinions into hypotheses with new studies to be done will help organizations strengthen their digital preservation capacity and enrich trustworthiness analysis. It is expected to raise awareness in organizations to preserve better the records which have archival value with this study.

1. Giriş

Kurumlarda fonksiyonların yürütülmesi sırasında tabii olarak oluşan ve arşivlik değere sahip olan belgelerin uzun dönemli korunması gerekir. Bu gerekliliğin başarılı bir şekilde yerine getirilmesi için sayısal koruma (digital preservation) tekniklerinden yararlanıldığı bilinmektedir. Belgelerin güvenilirliğinin de korunmasına yardımcı olan sayısal koruma, belgelere sürekli erişim için ihtiyaç duyulan yönetilebilir faaliyetler dizisi olarak tanımlanabilir (Digital Preservation Coalition - [DPC] Sayısal Koruma Koalisyonu, 2022).

Sayısal korumayla ilgili bu faaliyetler, kurumların mevcut yeteneklerini analiz etmesini gündeme getirmektedir. Bundan dolayı kurumlar, bir analiz aracına ihtiyaç duymaktadır. Bu analiz aracılığıyla kurum şu an hangi durumda, gelecekte hangi konuma varmak istiyor gibi sorular cevaplandırılabilir. Durum böyle olunca, olgunluk modeli geliştirme, sertifika alma ve kurum içi değerlendirme yapma gibi yöntemlere başvurulabilmektedir. Bu yöntemler, aynı zamanda belgelerin güvenilirliğinin korunmasında kullanılmaktadır. Hâliyle bu konuda hem akademik araştırmalar hem de bilimsel saha çalışmalarında çeşitli yaklaşımlar geliştirilmiştir. Saha çalışmalarına Electronic Resource Preservation and Access Network (ERPANET - Elektronik Kaynak Koruma ve Erişim Ağı), Cultural, Artistic and Scientific Knowledge for Preservation, Access and Retrieval (CASPAR - Koruma, Erişim ve Bulup Getirme için Kültürel, Sanatsal ve Bilimsel Bilgi), Preservation and Long-Term Access Through Networked Services (PLANETS - Ağ Bağlantılı Hizmetler Aracılığıyla Koruma ve Uzun Dönemli Erişim), Alliance Permanent Access to the Records of Science in Europe Network (APARSEN - Avrupa'daki Bilim Kayıtlarına Kalıcı Erişim Birliği Ağı), CoreTrustSeal, Go FAIR ve International Research on Permanent Authentic Records in Electronic Systems (INTERPARES - Elektronik Sistemlerde Belgelerin Özgünlüğünün Korunması Üzerine Uluslararası Araştırma) gibi projeler örnek verilebilir (ERPANET, 2022; CASPAR, 2022; PLANETS, 2022; APARSEN, 2022; CoreTrustSeal, 2022; Go FAIR, 2022; INTERPARES, 2022). Bunlardan INTERPARES'te daha çok kurumsal belgeler incelendiğinden, bu Proje'nin çıktılarından daha fazla yararlanmanın mümkün olduğu düşünülmektedir.

Akademik araştırmalar değerlendirildiğinde ise Basma Makhoul Shabou (2015), Devan Ray Donaldson (2015; 2016; 2019), Mpho Ngoebe ve Jonathan Mukwevho (2018) ile Özhan Sağlık'ın (2021) güvenilirlik üzerine çalışmalar gerçekleştirdiği görülmektedir. Shabou İsviçre özelinde, Ngoebe ve Mukwevho Güney Afrika çerçevesinde, Donaldson da ABD kapsamında güvenilirliği kritik etmiştir. Sağlık ise doktora tezinde Türkiye'de oluşan elektronik imzalı belgelerin delil değerini bakanlıklar örnekleminde arşivsel güvenilirlik açısından incelemiştir.

Türkiye'de kurumların sayısal korumayla ilgili mevcut yeteneklerinin değerlendirilmesine yönelik Sağlık'ın bildirisi (2022) dışında pek fazla çalışma olmasa da bazı araştırmalarla karşılaşılmaktadır. Alır ve Küçük (2003), sayısal koruma stratejilerine vurgu yaparak dünyada bu konuda gerçekleştirilen projeleri tanıtmışlardır. Çakmak, doktora tezinde kültürel bellek kurumlarında politika geliştirme üzerine bir model önermiştir (Çakmak, 2016). Bunun yanı sıra, Öztemiz ve Özel (2019) sayısal koruma süreçlerini dijital kütüphane bağlamında ele almıştır. Bunlarla birlikte, birtakım sayısal

koruma süreçleri üzerine çeşitli araştırmalar dikkat çekmektedir. Aldemir ve Oğuz (2006), sayısal korumada web arşivlemeye vurgu yapmış, web arşivlemenin bir sayısal koruma yöntemi olarak kullanılabileceğinden bahsetmişlerdir. Yalçınkaya (2020), sosyal medya içeriklerinin arşivlik değerine dikkat çekerek bunların arşiv bilimi yaklaşımıyla korunması gerektiğini dile getirmiştir. Tonta (2020), dijital kültürel kaydın korunmasında kurumların dikkat etmesi gereken hususları vurgulamıştır.

Tüm bu araştırmaların yanı sıra, kurumsal belgelerin uzun vadeli korunmasıyla ilgili yapılan çalışmalar da sayısal korumayla ilişkilendirilebilir. Aydın ve Özdemirci (2011), elektronik belgelerin arşivlenmesinde gerçekliğin ve bütünlüğün korunmasına dikkat çekmiştir. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Projesi olarak gerçekleştirdiği araştırmasında Külcü (2014), kamu üniversitelerinde e-belgelerin özgünlüğüne ilişkin bir yaklaşımın varlığını sorgulamıştır. Sağlık (2021), doktora tezinde bakanlıklarda oluşan elektronik imzalı belgelerin uzun dönemli korunmasını delil değeri ve güvenilirlikle ilişkilendirerek analiz etmiştir. Şahin ve Saydam (2022) ise İstanbul'daki ilçe belediyeleri özelinde sayısal süreklilik uygulamalarının ne ölçüde benimsendiğini incelemiştir. Bahsedilen bu çalışmalar, sayısal koruma farkındalığının gelişimine ivme kazandırsa da kurumların sayısal koruma yeteneklerinin bir sistematik çerçevesinde ele alınıp değerlendirildiği görülememektedir. Hâliyle kurumların sayısal koruma konusundaki mevcut yeteneklerinin analiz edilmesine duyulan ihtiyaç devam etmektedir.”

Tüm bunlarla birlikte, International Conference on Digital Preservation (IPRES - Uluslararası Sayısal Koruma Konferansları) külliyatında kurumların sayısal koruma yeteneklerinin değerlendirilmesine yönelik pek çok çalışmayla karşılaşmaktadır. Bunlardan bazılarında HDM aracılığıyla kurumların sayısal koruma yeteneklerinin kritik edildiği gözlenmektedir (McMeekin ve Currie, 2022; Sağlık, 2022; Popham ve Mitcham, 2022). Ancak çoğu çalışmada sayısal koruma yeteneklerinin değerlendirilmesi sistematik bir çerçeve içerisinde ele alınmamakta; yazarların çeşitli kurumlardaki gözlemleri aktarılmaktadır (Addis, 2021; Humbert, Roussel ve Vasseur, 2019; Lucker, Veenendaal, Sierman ve Ras, 2018; Van der Nat ve Ras, 2017; Shiers vd., 2016; Molinaro vd., 2015; Pennock, Wheatley ve May, 2014; Lehtonen, Helin, Koivunen ve Lehtonen, 2013; Katre, 2012; Massol, Rouchon ve Bechard, 2011; Zierau ve Jensen, 2010; Sinclair vd., 2009). Oysaki, farklı malzemelere sahip olan kurumların sayısal koruma yeteneklerini ölçmeye yönelik dernekler gibi oluşumlar tarafından çıkarılan kılavuzlara ihtiyaç duyulmaktadır. Çünkü bu kılavuzlar pek çok farklı türde malzemeye sahip olan kurumların ihtiyaçları göz önünde tutularak hazırlanmaktadır. Söz konusu kılavuzlara National Digital Stewardship Alliance (NDSA - Ulusal Sayısal Savunuculuk Birliği) Koruma Düzeyleri, DigCurV Curriculum Framework (Sayısal Kütasyon Eğitim Çerçevesi) ve Digital Preservation Capability Maturity Model (DPCMM - Sayısal Koruma Yetenek Olgunluk Modeli) ile DPC tarafından geliştirilen Rapid Assessment Model (Hızlı Değerlendirme Modeli - HDM) (NDSA, 2020; DigCurV, 2015; DPCMM, 2015; DPC, 2022) örnek verilebilir. Bu çalışmalardan DPC tarafından hazırlanan HDM, kurumların sayısal koruma yeteneklerini çok kapsamlı bir analiz yapmadan hızlı ve etkin bir şekilde değerlendirebilmesiyle öne çıkmaktadır.

Kurumların mevcut sayısal koruma yeteneklerini değerlendirmek ve geleceğe ilişkin bir planlama sunmak amacıyla DPC tarafından geliştirilen HDM'de bilgi işlem yeteneği, sürekli iyileştirmeler, içeriğin korunması ile keşif ve erişim gibi kurumsal ve hizmet ölçeğinde yetenekler hazırlanmıştır. Kurumların yeteneklerini değerlendirmeleri için 0, 1, 2, 3 ve 4 olmak üzere olgunluk seviyeleri belirlenmiştir. Burada kurum sayısal koruma açısından nerede, gelecekte nerede olmak istiyor ve varılmak istenen noktaya ulaşmak için neler yapılmalı gibi sorular sorulmaktadır (DPC, 2022). Bunun neticesinde kurumda oluşan belgelerin güvenilirliğine ilişkin bir karine de ortaya çıkabilir.

Bu çalışmada HDM'de belirlenen yetenekler, e-belgelerin güvenilirliği açısından incelenmektedir. Çalışmada hem sayısal koruma kapasitelerini değerlendirmek isteyen kurumlara bir metodolojinin zeminini oluşturmak hem de sayısal korumayla ilgili yetenekleri güvenilirlikle örtüştürmek istenmiştir. Bunun neticesinde kurumlarda arşivlik değere sahip olan belgeleri daha iyi korumak noktasında bir farkındalık oluşabileceği düşünülmektedir. Nitel araştırma deseninden faydalanan bu çalışmada doküman analizinden yararlanılmış; bu konuda yazılan eserler kritik edilmiştir.

Hem saha gözlemleri hem de yapılan araştırmalar, kurumlarda sayısal koruma yetenekleri ve güvenilirlik konusunda yeterli farkındalığın bulunmadığını göstermektedir (Külcü, 2014; Sağlık, 2021;

Şahin ve Saydam, 2022). Durum böyle olunca çalışmanın sorusu “HDM’de belirtilen yetenekler güvenilirlikle nasıl ilişkilendirilebilir” şeklindedir. Çalışma neticesinde kurumlarda bir farkındalık oluşması beklenmektedir.

Bu çalışma, Giriş dâhil 5 kısımdan oluşmaktadır. İlk kısım olan Giriş’te çalışmanın yöntemi ve amacı açıklanmış, ilgili literatür değerlendirilmiştir. İkinci kısımda HDM tanıtılmış, burada yer alan sayısal koruma yetenekleri ifade edilmiştir. HDM’de yer alan olgunluk seviyeleri göz önünde bulundurularak açıklanan bu yetenekler, söz konusu seviyelerin örnek faaliyetleriyle dile getirilmiştir. Üçüncü kısımda ise güvenilirlik anlayışı aktarılmaktadır. HDM’nin güvenilirlik açısından analizi ise dördüncü kısımda yapılmıştır. Son kısım olan Sonuç ve Öneriler kısmında, çalışmanın bulguları değerlendirilmiş ve HDM ile ilgili öneriler sunulmuştur.

2. Sayısal Koruma Koalisyonu Hızlı Değerlendirme Modeli

Kurumlar, elektronik ortamda oluşan ve uzun dönemli koruma değerine sahip olan belgelerini geleceğe aktarmak ister. Bunun için sertifika alma, değerlendirme ve model geliştirme gibi çeşitli eylemlere ihtiyaç duyabilmektedirler. Bu eylemlerden biri de kurumların sayısal koruma yeteneklerinin değerlendirilmesidir. Bu iş, kurum dışından yapılabildiği gibi kurum içerisinden de gerçekleştirilebilir. Bu hedefle geliştirilen modellerden biri de DPC tarafından hazırlanan HDM’dir.

HDM, Adrian Brown tarafından geliştirilen Sayısal Koruma Olgunluk Modeli’ne (2013) dayanmaktadır. Bunun yanı sıra, HDM’nin hazırlanmasında NDSA Koruma Düzeyleri (2020), DPCMM (2015), Kurumsal Hazıroluşluk Değerlendirme Seti (Miller, Blake ve Sorsby, 2012) ve CoreTrustSeal’dan (2022) yararlanılmıştır. Bahsi geçen bu çalışmalar, oldukça farklı alanlarda yetkinlikler içermektedir. Mesela CoreTrustSeal’de veri depoları, NDSA Koruma Düzeyleri’nde teknik hususlar, DPCMM’de ise dosya formatları gibi meseleler tartışılmaktadır. Ancak, HDM’de farklı türde malzemeye sahip olan DPC üyelerine sayısal koruma yetenekleriyle ilgili bir değerlendirme sunmak hedeflenmiştir. Bu üyeler arasında galeri, kütüphane, arşiv ve müze kurumları olabildiği gibi finans ve bilim kuruluşları da bulunmaktadır. Durum böyle olunca, teknolojik göç ya da öykünme gibi belli koruma stratejilerinden bağımsız, sektör ayırt etmeksizin her kurum için uygulanabilir nitelikte bir model hazırlanmıştır. Model hazırlanırken iyi uygulama örneklerinden de faydalanılmıştır. Ancak HDM, bir sertifika aracı olarak tasarlanmamıştır (DPC, 2022).

HDM, kurumların mevcut sayısal koruma yeteneklerini ölçüp, gelecekte varılmak istenen noktayı belirlemek amacıyla geliştirilmiştir. Bu geliştirme yapılırken politika ve strateji hazırlama, teknolojik altyapı, içeriğin korunması ve üstveri yönetimi gibi kurumsal ve hizmet düzeyinde yetenekler oluşturulmuştur. Kurumlar, HDM aracılığıyla bu yeteneklerini sayısal koruma olgunluğu açısından hızlı bir şekilde değerlendirebilmekte ve geleceğe yönelik planlama yapabilmektedir (DPC, 2022). Buradaki hızlı ifadesi ile kastedilen anlam, kısa sürede etkili bir değerlendirme sunmaktır. Böylece uzun dönemli korunacak arşiv malzemesine sahip kurumlar, bu değerlendirme sonuçlarını belgelerin güvenilirliğine ilişkin bir karine olarak ele alabilir.

HDM, 0-4 arasında bir olgunluk seviyesi sunmaktadır. 0, kurumun ilgili yetenek seviyesinde “düşük farkındalığı” olduğunu ifade etmektedir. 1 ise kurumun “farkındalık” sahibi olduğunu belirtmektedir. 2 seviyesi, kurumun o yetenekle ilgili temel faaliyetleri gerçekleştirdiğini göstermektedir. Bir yetenek düzeyinde kurumun yönetilebilir eylemleri 3 ile temsil edilirken, optimum düzeydeki yetenekler 4 ile değerlendirilmektedir. Değerlendirilen yetenekler, kurumsal ve hizmet olmak üzere iki bölümde incelenmektedir. 0 ve 1 seviyelerinde kurumların herhangi bir faaliyeti bulunmazken, 2, 3 ve 4. seviyelerde kurumlara bir örnek teşkil etmesi açısından bazı faaliyetler açıklanmaktadır.

2.1. Kurumsal Yetenekler

HDM’de ele alınan kurumsal yetenekler, daha çok idari süreçlerle ilgili olup kurumsal uygulanabilirlik, politika ve strateji, yasal dayanak, bilgi işlem yeteneği, sürekli iyileştirmeler ve topluluk şeklindedir. Kurumsal uygulanabilirlik, belge ve arşiv yönetimi süreçlerinin yönetişimi, kurumsal yapılanması, personel ve kaynağının sağlanması gibi faaliyetleri içerir. Temel seviyede belge ve arşiv yönetimi süreçleri kurum içerisinde desteklenmekte ve kaynak ayrılmaktadır. Örneğin, personelin sorumlulukları tanımlanmakta ve bir bütçe tahsis edilmektedir. Yönetilebilir seviyede ise

belge ve arşiv yönetimi süreçleri, kurum içerisinde yönetilmekte ve desteklenmektedir. Söz konusu süreçlerle ilgili analizler ve raporlar hazırlanmaktadır. Belge ve arşiv yönetimi, kurum için stratejik bir önceliktir. Optimum seviyede belge ve arşiv yönetimi faaliyetleri kurumda proaktif olarak yönetilmekte, iyileştirilmekte ve geliştirilmektedir. Uzman personel istihdamı yapılmakta, bilgi ve belge yönetimi daire başkanlığı gibi sayısal korumadan sorumlu bir birim oluşturulmakta ve raporlamalar geleceği öngörerek hazırlanmaktadır (DPC, 2022, s. 8-9).

HDM’de ele alınan kurumsal yeteneklerin ikincisi politika ve stratejidir. Bu yeteneğin konusu belge ve arşiv yönetimini yönlendiren politikalar, stratejiler ve prosedürlerdir. Temel yetenek seviyesindeki faaliyetlere kurumun temel bir sayısal koruma politikasının mevcut olması örnek verilebilir. Kurumlarda elektronik belgeleri yönetmek için prosedürler hazırlanmaktadır. Yönetilebilir seviyede kurumdaki belge ve arşiv yönetimi politika ve prosedürleri kapsamlıdır. Bu seviyede süreçlerle ilgili politikalar diğer kurumsal politikalarla uyumludur. Süreçler dokümanite edilmekte; prosedürler geliştirilmektedir. Optimum yetenek seviyesinde ise kurum, proaktif olarak politika ve prosedürleri değerlendirmektedir. Burada süreç iyileştirmeleri söz konusudur. Örneğin politika ve prosedürler proaktif olarak izlenir ve bunlar ihtiyaçların değişimine göre gözden geçirilir (DPC, 2022, s. 10).

Yasal dayanakla ilgili olan yeteneklerde belgelerin sağlanması, korunması ve erişimiyle ilgili yasal hak ve sorumlulukların ilgili mevzuata ve etik ilkelere uyumlu olarak yönetilip yönetilmediği değerlendirilmektedir. Temel yetenek seviyesinde elektronik belgelerle ilgili önemli yasal hak ve sorumlulukların etik ilkelere riayet edilerek kim tarafından gerçekleştirileceği belirlenmekte ve kayıt altına alınmaktadır. Yönetilebilir seviyede gerçekleştirilen faaliyetlere belge ve arşiv yönetiminde yasal sorunlar ve risklerin yönetimiyle ilgili yetki ve sorumlulukların açıkça belirlenmesi örnek verilebilir. Bunlarla ilgili gerçekleştirilen işlemlerin dokümantasyonu yapılmaktadır. Optimum seviyede ise belge ve arşiv yönetimiyle ilgili yasal sorunlar ve riskler proaktif olarak izlenmekte ve gerektiğinde kanun yapımcılarla iletişime geçilmektedir (DPC, 2022, s. 11).

Bilgi işlem yeteneğinde kritik edilen husus bilgi teknolojileridir. Bu yeteneğin temel seviyesinde kurumların teknik altyapı ve destek gibi temel bilgi işlem faaliyetlerine ulaşp ulaşmadığı değerlendirilmektedir. Örneğin elektronik belge yönetim sistemleri (EBYS) ve elektronik arşiv (e-arşiv) için temel seviyede bilgi işlem desteği mevcuttur. Sistemler, temel düzeyde dokümanite edilmektedir. Yönetilebilir seviyede kurumlar kapsamlı bir şekilde yönetilen teknik altyapı ve destek gibi temel bilgi işlem faaliyetlerine ulaşabilmektedir. Bu seviyede belge ve arşiv yönetim sistemleri düzenli aralıklarla bakıma alınmakta ve güncellenmektedir. Sistemlerin dokümantasyonu kapsamlı bir şekilde yapılmaktadır. Optimum seviyede ise EBYS ve e-arşiv, proaktif bir biçimde sayısal koruma gereksinimleri dikkate alınarak geliştirilmektedir (DPC, 2022, s. 12).

HDM’de yer alan bir diğer kurumsal yetenek, sürekli iyileştirmelerdir. Burada mevcut belge ve arşiv yönetimi yetenekleri değerlendirilmekte, hedefler belirlenmekte ve ilerlemenin takip edilmesine yönelik süreçler kararlaştırılmaktadır. Temel seviyede kurumlar, mevcut yetenekleri ve geliştirilecek yönleri konusunda temel bir anlayışa sahiptir. Örneğin, belge ve arşiv yönetimi konusunda geliştirilmesi gereken hususlar belirlenmektedir. Yönetilebilir seviyede belirlenen hedefler üst yönetici tarafından onaylanmakta ve hedeflere ulaşmak için yol haritası oluşturulmaktadır. Türk Standartları Enstitüsü tarafından hazırlanan 13298’in kurumsal akreditasyon sertifikasının alınması gibi dış değerlendirme/tetkik yaptırılması ve iyileştirme önerilerinin dikkate alınıp uygulanması ise optimum seviyenin örneklerindendir (DPC, 2022, s. 13).

Kurumsal yeteneklerin sonuncusu ise topluluk yeteneğidir. Burada belge yönetimi ve arşivcilik camiasının katkısı söz konusudur. Örneğin temel seviyede kurumlar ilgili toplulukların etkinliklerine katılmaktadır. Yönetilebilir seviyede ise ilgili topluluklar kuruma davet edilmektedir. Gerektiğinde uzman görüşüne başvurulmakta, kazanımlar camiayla paylaşılmaktadır. Optimum seviyenin faaliyetlerine çalıştay, sempozyum ve toplantı gibi etkinlikler düzenlenmesi ile mevcut çalışma gruplarına katkıda bulunulması örnek verilebilir (DPC, 2022, s. 14).

2.2. Hizmet Yetenekleri

HDM’de yer alan hizmet yetenekleri daha çok teknik süreçlerle ilgili olup, sağlama, transfer ve sisteme dâhil etme, bit akışının korunması, içeriğin korunması, üstveri yönetimi ile keşif ve erişim

şeklinde. Sağlama, transfer ve sisteme dâhil etme yeteneğinde belgelerin sağlanması ve arşive transferiyle ilgili süreçler değerlendirilmektedir. Temel seviyede söz konusu süreçler dokümanite edilmekte ve kılavuzlar hazırlanmaktadır. Yönetilebilir seviyede ise belgelerin bütünlük kontrolleri yapılmaktadır. Standartlaştırılmış bir iş akışı bulunur. Optimum seviyede paydaşlarla işbirliği gerçekleştirilmektedir. Süreçler gelecek düşünülerek tasarlanmakta; otomatikleştirilme hedeflenmektedir (DPC, 2022, s. 15-16).

Hizmet yeteneklerinin ikincisi bit akışının korunmasıdır. Bit akışı, belgedeki içeriği, form özelliklerini ve kontekst bilgisini anlamlandırmayı sağlayan elektronik ortamdaki en küçük yapıtaşdır. Belgenin anlamlı olabilmesi için bu bit akışının korunması gerekir. Durum böyle olunca bu yetenekle ilgili faaliyetler, belgelerin depolanması ve bütünlüğün sağlanmasına yönelik süreçlerle ilişkilidir. Temel seviyede elektronik belgeler için hasredilmiş bir depo mevcuttur. Erişim yetkileri belirlenmekte; sağlama toplamları (checksum) oluşturulmaktadır. Yönetilebilir seviyede ise içeriğin korunmasına yönelik uygulamalar benimsenmektedir. Örneğin, bütünlük kontrollerinde karşılaşılan sorunlar giderilmekte; erişimler yapılandırılarak dokümanite edilmektedir. Optimum seviyede risk yönetimi uygulanmaktadır. Farklı konumlarda birden fazla kopya bulundurulmaktadır. Farklı teknolojiler kullanılmaktadır. Bununla birlikte, belgelere yapılan erişimler log kayıtlarına kaydedilmektedir (DPC, 2022, s. 17).

İçeriğin korunmasında ise belgelerin kontekstini ve işlevselliğini muhafaza etmek ve zaman içerisinde sürekli erişilebilirliğini ve kullanılabilirliğini sağlamaya yönelik süreçler değerlendirilmektedir. Örneğin, temel seviyede dosya formatları belirlenmektedir. Belgelere erişimde yaşanan sorunlar analiz edilmektedir. Yönetilebilir seviyede ise teknoloji izleme uygulamaları yapılmakta ve risk altındaki belgeler tespit edilmektedir. Belgelerdeki değişimler kayıt altına alınmakta; uzun vadeli koruma için ihtiyaç duyulan uygulamalar belirlenmektedir. İhtiyaç duyulan bu uygulamaların gerçekleştirilmesi ve koruma planları çerçevesinde süreçlerin yönetilmesi optimum seviyenin örnek faaliyetleri arasındadır (DPC, 2022, s. 18-19).

Hizmet yeteneklerinin bir diğeri üstveri yönetimidir. Burada koruma, keşif ve kullanıma ilişkin yeterli üstverinin üretilmesi ve muhafazasına yönelik süreçler değerlendirilmektedir. Temel seviyede malzemeler koleksiyon düzeyinde tanımlanmaktadır. İçerikle birlikte üstveriler de kayıt altına alınmaktadır. Yönetilebilir seviyede ise uygun üstveri standartları belirlenmektedir. Tanımlamada kurum içi kılavuzlar ve kontrollü sözlükler kullanılmaktadır. Belgeler ile üstveri dosyaları arasında yapısal bir ilişki kurulmaktadır. Bu ilişkiyi sürekli kılmak için ihtiyaç duyulan faaliyetler ise optimum seviyede gerçekleştirilmektedir. Bu seviyede üstveriler harmanlanabilir yapıdadır ve üstveri kullanımı uzun vadeli koruma stratejisiyle ilişkilendirilmektedir (DPC, 2022, s. 20).

Hizmet yeteneklerinin sonuncusu keşif ve erişimdir. Bu yetenekte belgelerin keşfini ve kullanıcıların erişimini sağlamaya yönelik süreçler değerlendirilmektedir. Temel seviyede her belgede değil ancak gizlilik ve kişisel veri gibi nedenlerle bazı belgeler için keşif aracı mevcuttur. Bu duruma rağmen, kullanıcılar kurum içi ya da dışından belgelere erişebilmektedir ve bu erişimler kayıt altına alınmaktadır. Yönetilebilir seviyede her belge için keşif aracı söz konusudur. Bazı belgeler için tam metin arama imkânı bulunmaktadır. Erişim sistemleri kullanıcılardan gelen geri bildirimlere göre güncellenmektedir. Erişimin proaktif olarak iyileştirilip geliştirilmesi ise optimum seviyede gerçekleşmektedir. Bu seviyede veri görselleştirme gibi teknikler kullanıcıya sunulmakta; kullanıcılara erişim desteği sağlanmaktadır. Belgeler, erişilebilir formatlarda kullanıcılara takdim edilmektedir. Bunun için birlikte çalışabilirlik esasları benimsenmektedir (DPC, 2022, s. 21-22).

3. Güvenilirlik

Güvenilirlik, belgelerin taşıyıcı ortam, içerik, düzenleyen ve kontekst gibi özniteliklerin muhafaza edilmesi olarak bilinmektedir. Bu özniteliklerin korunup güvenilirliğin devamlılığıyla alakalı olarak doğrudan belgelerle çalışan hukuk, diplomatik ve tarih disiplinleri de farklı yaklaşımlar geliştirmişlerdir. Güvenilirliğin bu disiplinlerde farklı tanımlandığı dikkat çekmektedir. Mesela, hukuki güvenilirlikte bir belgenin mevzuatta yer alan özellikleri haiz olup olmadığı incelenmekte; belge üretmede yetki mekanizması ve belge yönetimi süreçlerinde prosedürlerin tesis edilip edilmediği kontrol edilmektedir (Sağlık, 2021, s. 58; Sağlık, 2021a, s. 37; Çiçek, 2009, s. 212; MacNeil, 2000, s.

53-56). Diplomatik güvenilirlikte ise belgenin karakteristiğini açıklayan form unsurlarının uygun şekilde bulunup bulunmadığı değerlendirilmektedir. Taşıyıcı ortam, içerik, form özellikleri, belgedeki işlem ve kişiler, arşivsel bağ, üstveriler, kontekst gibi özellikler kritik edilerek prosedürler analiz edilmektedir. Bunların yanı sıra, e-imza, mühür, kullanılan donanım ve yazılımların özellikleri, log kayıtları, denetim günlükleri ve veri tabanı kayıtları incelenmektedir (Sağlık, 2021, s. 58; Sağlık, 2021a, s. 37; MacNeil, 2000, 73-75, 91, 96-97, 100-102). Bir diğer güvenilirlik yaklaşımı da tarihi güvenilirliktir. Burada, belgenin içerdiği bilgilerin, yer ve olayların doğru olarak verilir verilmediği kontrol edilmektedir. Özellikle belgede geçen bilgilerin, açıklanan tarih, yer, kişi ve dönemle uyumu gerekir (Sağlık, 2021, s. 59; Sağlık, 2021a, s. 37; Çiçek, 2009, s. 212).

Ancak, e-belgelerin güvenilirlik analizinde yukarıda bahsedilen yaklaşımlar tek başına yeterli olamayabilir. Çünkü, belgelerin oluşumuna kaynaklık eden mevzuat ve kullanılan bilgi teknolojileri meselenin daha geniş bir bakış açısıyla ele alınmasını gündeme getirmiştir. Bu bakış açısı arşivsel güvenilirlik olarak adlandırılmaktadır (Sağlık, 2021, s. 59; INTERPARES, 2008; Bushey, 2016). Diğer güvenilirlik anlayışlarında olduğu gibi arşivsel güvenilirlikte de özgünlük, tamlık ve gerçeklik kritik edilmektedir (INTERPARES, 2008, s. 335, 816; Sağlık, 2021, s. 59). İşbu çalışma kapsamında arşivsel güvenilirlik anlayışı temel alınmıştır.

Belgenin özniteliklerinin üretildikten sonra işlem gördüğü ve dosyalanıp arşivlendiği dönem içerisinde değişmemesi olarak açıklanan özgünlük, tanımlanabilirlik ve bütünlük olmak üzere iki adımda incelenmektedir. Tanımlanabilirlik, belgeleri diğer belgelerden ayırt eden ve türüne göre oluşan karakteristik unsurların nitelenmesini ifade eder. Bunlara belgedeki kişiler, üretim ve iletim tarihi, konu, arşivsel bağ, dosya kodu ve belgenin ekleri örnek verilebilir. Özgünlüğün diğer bir adımı ise belgenin tüm bileşenleriyle birlikte bozulmamış ve değiştirilmemiş olmasını ifade eden bütünlüktür. Bütünlükte belgenin konteksti, form özellikleri ve içeriğinin korunması hedeflenir (Sağlık, 2021, s. 60; Sağlık, 2021a, s. 38; Rogers, 2015, s. 26; Çiçek ve Sağlık, 2019, s. 150-151).

Özgünlüğün yanı sıra bir diğer güvenilirlik unsuru tamlıktır. Tamlık arz eden bir belgede kesin, doğru, hakikate uygun ve tahrifattan uzak olmak özellikleri aranmaktadır. Bir diğer güvenilirlik unsuru olan gerçeklik ise belgenin üretim prosedürlerindeki kontrollerle belge formunun tamlığına dayanarak değerlendirilmektedir. Bu kontroller, belgenin üretimi ve alımı, dosyasına kaldırılması ve belgedeki kişilerin yetkileri olarak belirtilmektedir. Belge formunun tamlığı, belgeyi hukuki bir sonuç doğurmaya elverişli hâle getirecek entelektüel formun tüm elemanlarının mevcut olmasını ifade etmektedir (Sağlık, 2021, s. 61; Çiçek ve Sağlık, 2019, s. 152-153, Sağlık, 2021a, s. 38).

Güvenilirliğin korunması için bazı yöntemlere ihtiyaç duyulmaktadır. Bu yöntemler, belgenin üretildikten, alındıktan ve dosyasına kaldırıldıktan sonra değiştirilmediğini göstermelidir. Bunun için belgelerin arşivcilik standartlarına göre tanımlanması, arşivsel bağının açığa çıkarılıp provenansın tesis edilmesi, e-imza ve e-mühür eklenmesi ile log kayıtlarının kontrol edilmesi gibi yöntemlerden yararlanılmaktadır (Sağlık, 2021, s.61-62; Rogers, 2015, s. 28, 35; Meehan, 2006, s. 142; Cook, 2013, s. 99-100).

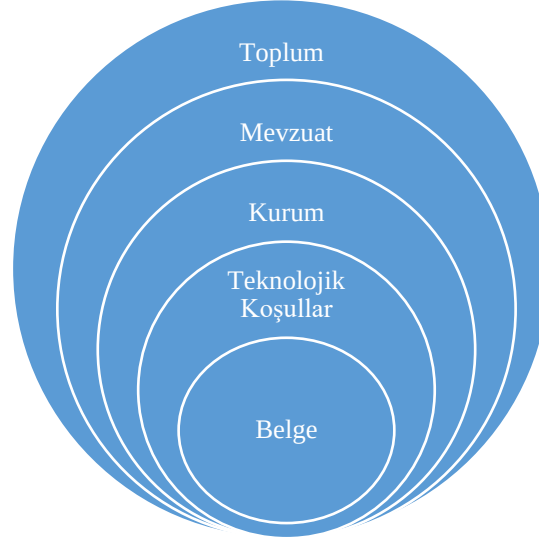
4. HDM'nin Güvenilirlik Açısından İncelenmesi

Güvenilirliğin analiz edilmesine yönelik hem akademik araştırmalar hem de bilimsel saha çalışmalarında çeşitli yaklaşımlar geliştirilmiştir. Saha çalışmalarına ERPANET, CASPAR, PLANETS APARSEN, CoreTrustSeal, Go FAIR ve INTERPARES örnek verilebilir (ERPANET, 2022; CASPAR, 2022; PLANETS, 2022; APARSEN, 2022; CoreTrustSeal, 2022; Go FAIR, 2022; INTERPARES, 2022). Bunlardan INTERPARES'te daha çok kurumsal belgeler incelenmiştir. Hâliyle INTERPARES'in çıktılarında daha fazla yararlanmanın mümkün olduğu düşünülmektedir. Akademik araştırmalar değerlendirildiğinde ise Basma Makhoul Shabou (2015), Devan Ray Donaldson (2015; 2016; 2019), Mpho Ngoebe ve Jonathan Mukwevho (2018) ile Özhan Sağlık'ın (2021) güvenilirlik üzerine çalışmalar gerçekleştirdiği görülmektedir. Shabou, İsviçre özelinde; Ngoebe ve Mukwevho Güney Afrika çerçevesinde; Donaldson da ABD kapsamında güvenilirliği kritik etmiştir. Sağlık ise doktora tezinde Türkiye'de oluşan e-imzalı belgelerin delil değerini bakanlıklar örneklemine arşivsel güvenilirlik açısından analiz etmiştir. Durum böyle olunca, HDM'de yer alan düzeylerin Sağlık tarafından geliştirilen güvenilirlik analiziyle

ilişkilendirilebileceği düşünülmüştür. Bu analizde belgelerin güvenilirliği, belge, teknolojik koşullar, kurum, mevzuat ve toplum düzeylerinde kritik edilmektedir (Sağlık, 2021, s. 64-66).

Şekil 1

Güvenilirlik Düzeyleri



(Kaynak:Sağlık, 2021, s. 64)

Belge düzeyinde kontekst, arşivsel bağ, üstveriler ve taşıyıcı özellikler gibi belgeyi oluşturan unsurlar değerlendirilmektedir. Burada hangi üstveriler kullanıldı, format değişimine ihtiyaç duyulup duyulmadığı kontrol ediliyor mu, form özellikleri kayıt altına alındı mı gibi sorular sorulmaktadır. Teknolojik koşullar düzeyinde belgelerin üretildiği, transfer edildiği ve saklandığı uygulama yazılımları ve kullanılan donanımlar incelenmektedir. Bütünlük kontrollerinin yapılması, saklama yöntemlerinin çeşitlendirilmesi, erişim yetkilerinin etkinleştirilmesi gibi hususlar analiz edilmektedir. Kurum düzeyinde ise belge yönetimi ve arşivcilikle ilgili politika ve prosedürler değerlendirilmektedir. Bunlar incelenirken belge yönetimi politikasının varlığı, çalışanların sürekli eğitimi gibi hususlar dikkate alınmaktadır (Sağlık, 2021, s. 64-66).

Kurumlar, belge yönetimi ve arşivcilikle ilgili politika ve prosedürleri hazırlayıp, teknolojik koşulları günün gereklerine uygun bir şekilde geliştirse ve belgelerle ilgili zengin üstveri tayin etse de fonksiyonlarını yürütürken ilgili mevzuata göre hareket eder. Mevzuatta belgelerin saklama süresi, form özellikleri, benimsenmesi gereken teknolojik koşullar gibi hususlar yer alabilir. Durum böyle olunca, söz konusu hususlar mevzuat düzeyinin kritik unsurlarını oluşturur. Bunların yanı sıra, ülkelerin milli arşivlerinin belge yönetimi ve arşivcilik uygulamaları da mevzuat düzeyinde değerlendirilmektedir. Burada milli arşivler belgelerin arşivleme kurallarını belirledi mi, teknolojik göç prosedürleri oluşturuldu mu, kullanılacak formatlar tayin edildi mi gibi sorular sorulabilmektedir (Sağlık, 2021, s. 65).

Güvenilirlik analizinin son düzeyinde vatandaşların e-belgelere güven duymak için hangi unsurları aradıkları incelenmektedir. Hâliyle bu aşama, toplum düzeyi olarak adlandırılmaktadır. Burada vatandaşlarda güveni tesis eden araçlar nelerdir, belgelere hangi oranda güven duyuluyor, duyulan bu güven nasıl artırılabilir gibi sorular araştırılmaktadır (Sağlık, 2021, s. 65-66).

Tüm bu analiz düzeyleri göz önünde bulundurulduğunda kurumların belge, teknolojik koşullar ve kurum düzeylerinde daha etkin olduğu düşünülmektedir. Çünkü toplum ve mevzuat düzeylerinde kurumların kendi tasarrufları dışındaki faaliyetler söz konusudur. Örneğin toplum düzeyinde vatandaşların düşünceleri kritik edilmekte, mevzuat düzeyinde ise hükümetlerin çıkarmış olduğu kanun, yönetmelik ve genelgeler incelenmektedir. Durum böyle olunca hem vatandaşların düşünceleri hem de çıkarılan mevzuat, kurumların doğrudan kendi inisiyatifleriyle şekillenmemektedir. Belge, teknolojik koşullar ve kurum düzeyinde ise organizasyonlar daha dinamikler (Sağlık, 2021, s. 66).

Bu değerlendirmeler neticesinde HDM’de belirtilen yeteneklerin güvenilirlik düzeyleriyle ilişkilendirilebileceği görülmüştür. Bu ilişkilendirme şöyle belirtilebilir:

Tablo 1

Sayısal Koruma Yetenekleri ve Güvenilirlik Düzeyleri

Yetenekler	Güvenilirlik Düzeyi
Kurumsal Uygulanabilirlik	Kurum
Politika ve Strateji	Kurum
Yasal Dayanak	Mevzuat
Bilgi İşlem Yeteneği	Teknolojik Koşullar
Sürekli İyileştirmeler	Kurum
Topluluk	Toplum
Sağlama, Transfer ve Sisteme Dâhil Etme	Kurum
Bit Akışının Korunması	Teknolojik Koşullar
İçeriğin Korunması	Belge
Üstveri Yönetimi	Belge
Keşif ve Erişim	Teknolojik Koşullar

Bu yetenekler, birden fazla güvenilirlik düzeyiyle de ilişkilendirilebilir. Örneğin bilgi işlem yeteneği, hem kurum hem de teknolojik koşullar düzeyiyle ilintilidir. Ancak tüm yetenekler, özü açısından değerlendirilerek bir güvenilirlik düzeyiyle bağlantılandırılmıştır.

HDM’nin ilk yeteneklerinden olan kurumsal uygulanabilirlik, belge ve arşiv yönetimi süreçlerinin yönetimi ve ilgili personelin gelişimi gibi konuları içerdiğinden (DPC, 2022, s. 8-9) kurum düzeyiyle ilişkilendirilmiştir. Politika ve strateji yeteneğinde ise belge yönetimi ve arşivcilik süreçleriyle ilgili politika ve prosedürler incelenir (DPC, 2022, s. 10). Hâliyle bu yetenek de kurum düzeyiyle ilgilidir. Yasal dayanak yeteneğinde, her ne kadar kurumun kendi geliştirdiği süreçlerle şekillenme söz konusu olsa da temelinde mevzuata uyumlu hareket etme gerekliliği yer almaktadır (DPC, 2022, s. 11). Durum böyle olunca bu yetenek, mevzuat düzeyiyle ilintilendirilmiştir.

Bilgi işlem yeteneğinde belge ve arşiv yönetimiyle ilgili bilgi teknolojileri değerlendirilmektedir (DPC, 2022, s. 12). Hâliyle bu yetenek, arşivsel güvenilirliğin teknolojik koşullar düzeyiyle ilişkilendirilmiştir. Bununla birlikte, kurumların mevcut belge ve arşiv yönetimi yetkinliklerini değerlendirip, hedefler belirlediği yetenek, sürekli iyileştirmelerdir (DPC, 2022, s. 13). Bu yeteneğin kurum düzeyiyle ilgili olduğu düşünülmüştür.

Tüm bunlarla birlikte, kurumsal yeteneklerin sonuncusu olan topluluk yeteneğinde belge yönetimi ve arşivcilik camiasıyla birlikte hareket etme durumu vardır. Örneğin; odak grup toplantıları yapılabilir, çalıştaylar düzenlenebilir. Bu yeteneğin gerçekleşmesi için konuyla ilgili bireylerin katılımına ihtiyaç vardır (DPC, 2022, s. 14). Söz konusu yetenek arşivsel güvenilirliğin toplum düzeyiyle ilişkilendirilmiştir.

HDM’nin kurumsal yeteneklerinin yanı sıra hizmet yetenekleri de bulunmaktadır. Bunlardan ilki, sağlama, transfer ve sisteme dâhil etmedir. Burada belgelerin transferi ve arşive devri gibi süreçlerin dokümantasyonuna odaklanılmaktadır (DPC, 2022, s. 15-16). Bu yetenek, belge ve teknolojik koşullarla ilgili olabileceği de dokümantasyon yönetiminin daha çok arşivsel güvenilirliğin kurum düzeyiyle ilintili olabileceği düşünülmüştür.

Hizmet yeteneklerinin bir diğeri, bit akışının korunmasıdır. Burada belgelerin bütünlüğüne yönelik adımlar değerlendirilir. Teknolojik kaynaklar ön plandadır (DPC, 2022, s. 17). Hâliyle bu yetenek, teknolojik koşullarla ilişkilendirilmiştir. Bir başka hizmet yeteneği olan içeriğin korunmasında ise

belgelerin kontekstini ve işlevini muhafaza etmeye yönelik adımlar söz konusudur (DPC, 2022, s. 18-19). Bu adımlar, arşivsel güvenilirliğin belge düzeyiyle ilgilidir.

Üstveri yönetiminde arşivlenen belgelerle ilgili yeterli üstverilerin kullanılıp kullanılmadığı analiz edilmektedir (DPC, 2022, s. 20). Durum böyle olunca bu yetenek, belge düzeyiyle ilişkilendirilmiştir. HDM'deki son yetenek ise keşif ve erişimdir. Burada belgelere kullanıcıların erişimini sağlamaya yönelik süreçler incelenmektedir (DPC, 2022, s. 21-22). Erişim sistemleri, yazılımlarla ilişkili olduğundan bu yetenek arşivsel güvenilirliğin teknolojik koşullar düzeyiyle ilintilendirilmiştir.

5. Sonuç ve Öneriler

Kurumlarda oluşan belgelerden arşivlik değere sahip olanların uzun dönemli korunması gerekir. Bu gerekliliği sağlamak için sayısal koruma yeteneklerinin geliştirilmesine ihtiyaç vardır. Söz konusu ihtiyacı gidermede başvurulacak olgunluk modeli geliştirme, sertifika alma ve kurum içi değerlendirme yapma gibi yöntemlerden biri de DPC tarafından hazırlanan HDM'dir. Bu model, kurumların mevcut sayısal koruma yeteneklerini ölçüp, gelecekte varılmak istenen noktayı belirlemek amacıyla geliştirilmiştir. Model kapsamında politika ve strateji hazırlama, teknolojik altyapı, içeriğin korunması ve üstveri yönetimi gibi kurumsal ve hizmet düzeyinde yetenekler oluşturulmuştur. Kurumlar, HDM aracılığıyla bu yeteneklerini sayısal koruma olgunluğu açısından hızlı bir şekilde değerlendirebilmekte ve geleceğe yönelik planlama yapabilmektedir.

HDM'de yer alan kurumsal yetenekler, kurumsal uygulanabilirlik, politika ve strateji, yasal dayanak, bilgi işlem yeteneği, sürekli iyileştirmeler ve topluluk şeklindedir. Hizmet yetenekleri ise DPC tarafından sağlama, transfer ve sisteme dâhil etme, bit akışının korunması, içeriğin korunması, üstveri yönetimi ile keşif ve erişim olarak belirlenmiştir. Bu yetenekler, bir e-belgenin varlığını oluşturan özniteliklerin değerlendirilmesini sağladığından aynı zamanda güvenilirlikle de ilişkilidir.

Güvenilirlik, belgelerin taşıyıcı ortam, içerik, düzenleyen ve kontekst gibi özniteliklerin muhafaza edilmesi olarak bilinir. Bu özniteliklerin muhafazasında ise arşivcilik, bilgi teknolojileri ve hukuk gibi disiplinlerin geliştirdiği yöntemlerden yararlanılmaktadır. Bu yöntemlere belgelerin arşivcilik standartlarına göre tanımlanması, arşivsel bağının açığa çıkarılıp provenansın tesis edilmesi, e-imza ve e-mühür eklenmesi ile log kayıtlarının kontrol edilmesi gibi örnekler verilebilir. Söz konusu yöntemlerden yararlanarak belgelerin güvenilirliği analiz edilir.

Güvenilirliğin belge düzeyiyle ilişkilendirilen HDM yetenekleri, içeriğin korunması ve üstveri yönetimidir. Bilgi işlem yeteneği, bit akışının korunması ile keşif ve erişim teknolojik koşullar düzeyiyle ilişkilendirilmiştir. Kurum düzeyiyle ilintilendirilenler ise kurumsal uygulanabilirlik, politika ve strateji, sürekli iyileştirmeler, sağlama, transfer ve sisteme dâhil etmedir. Tüm bunlarla birlikte, yasal dayanak yeteneğinin mevzuat düzeyiyle; topluluk yeteneğinin de toplum düzeyiyle ilişkili olduğu görülmüştür. Bu ilişkilendirmeler neticesinde kurumlar sayısal koruma kapasitelerini ölçüp, planlama yapmak için HDM'yi kullanırken, analizler neticesinde belgelerin güvenilirliklerinin ne ölçüde korunduğuna dair bir karineye sahip olabileceklerdir.

HDM'nin kurumlara yönelik bu faydalarının yanı sıra, hedeflere ulaşmak için somut kriterlerin belirlenmesi açısından geliştirilmesi gereken yönleri bulunmaktadır. Örneğin temel seviyeden yönetilebilir seviyeye geçmek için hangi eylemlere ihtiyaç duyulmaktadır? Bu eylemler, güvenilirliğin hangi düzeyleriyle ilişkilidir? Söz konusu eylemler, bir kriter hâline getirilerek güvenilirlik analizlerinde nasıl kullanılabilir? Yapılacak yeni çalışmalarla bu gibi sorulara ışık tutulması, hem kurumların sayısal koruma kapasitelerini güçlendirmelerine yardımcı olacak hem de güvenilirlik analizlerinin zenginleşmesine katkıda bulunacaktır.

Teşekkür

Çalışmanın son okumasını yaparak görüşleriyle beni yönlendiren değerli meslektaşım Emine Pınar Gevheroğlu'na teşekkür ederim.

Etik Standartlar ile Uyumluluk

Çıkar Çatışması: Yazar herhangi bir çıkar çatışmasının olmadığını beyan eder.

Etik Kurul İzni: Bu çalışma için etik kurul iznine gerek yoktur.

Yazar Katkı Beyanı: Makale tek yazarlıdır.

Finansal Destek: Yoktur.

Kaynakça

- Addis, M. (2021). Scalable and Sustainable Long Term Digital Preservation of Scientific Datasets. 17. *International Conference on Digital Preservation*. <https://osf.io/uerq9>
- Aldemir, A. ve Oğuz, E. S. (2006). Sayısal (Dijital) Kültürün Korunması: Web Arşivleme. *Türk Kütüphaneciliği*, 20(3), 283-312.
- Alır, G. ve Küçük, M. E. (2003). Dijital Koruma (Arşivleme) Stratejileri ve Bazı Uygulama Örnekleri. *Türk Kütüphaneciliği*, 17(4), 340-356.
- Alliance Permanent Access to the Records of Science in Europe Network [APARSEN]. (2022). <http://www.alliancepermanentaccess.org>
- Aydın, C. ve Özdemirci, F. (2011). Elektronik Belgelerin Arşivlenmesinde Gerçekliğin ve Bütünlüğün Korunması. *Bilgi Dünyası*, 12(1), 105-127.
- Brown, A. (2013). *Practical Digital Preservation: A how-to Guide for Organizations of any Size*. Facet Publishing.
- Bushey, J. (2016). *The Archival Trustworthiness of Digital Photographs in Social Media Platforms*. Yayınlanmamış Doktora Tezi. University of British Columbia.
- Cook, T. (2013). Evidence, Memory, Identity and Community: Four Shifting Archival Paradigms. *Archival Science*, 13(2-3), 95-120.
- CoreTrustSeal. (2022). <https://www.coretrustseal.org>
- Cultural, Artistic and Scientific Knowledge for Preservation, Access and Retrieval [CASPAR]. (2022). <http://casparpreserves.digitalpreserve.info>
- Çakmak, T. (2016). *Türkiye’de Kültürel Bellek Kurumlarında Dijitalleştirme ve Dijital Koruma Politikaları: Bir Model Önerisi*. Yayınlanmamış Doktora Tezi. Hacettepe Üniversitesi.
- Çiçek, N. (2009). *Modern Belgelerin Diplomatliği*. Derlem Yayınları.
- Çiçek, N. ve Sağlık, Ö. (2019). Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı. Yalçınkaya, B. vd. (Yay. haz.). *Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ* içinde (141-170). Ankara Üniversitesi.
- DigCurV. (2015). *DigCurV Curriculum Framework*. <https://digcurv.gla.ac.uk>
- Digital Preservation Capability Maturity Model [DPCMM]. <https://www.securelyrooted.com/dpcmm>
- Digital Preservation Coalition [DPC]. (2022). *Sayısal Koruma Koalisyonu Hızlı Değerlendirme Modeli (DPC RAM)*. <http://doi.org/10.7207/dpcram22-01>
- Donaldson, R. D. (2015). *Development of a Scale for Measuring Perceptions of Trustworthiness for Digitized Archival Documents*. Yayınlanmamış Doktora Tezi. University of Michigan.
- Donaldson, R. D. (2016). The Digitized Archival Document Trustworthiness Scale. *International Journal of Digital Curation*, 11(1), 252-270.
- Donaldson, R. D. (2019). Trust in Archives– Trust in Digital Archival Content Framework. *Archivaria*, 88, 50-83.
- Electronic Resource Preservation and Access Network [ERPANET]. (2022). <https://www.erpanet.org>

- Humbert, M., Roussel, S. ve Vasseur, E. (2019). Building the Future Digital Preservation in French Archival Services: Processes, Functions and Staffing for an Effective Digital Preservation. Ras, M., Sierman, B. ve Puggioni, A. (Yay. haz.). 16. *International Conference on Digital Preservation* içinde (46-52). Dutch Digital Heritage Network.
- International Research on Permanent Authentic Records in Electronic Systems [INTERPARES]. (2022). <http://www.interpares.org>
- INTERPARES. (2008). *INTERPARES 2: Experiential, Interactive and Dynamic Records*. Ed. L. Duranti ve R. Preston. http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf
- Go FAIR. (2022). <https://www.go-fair.org>
- Lehtonen, J., Helin, H., Koivunen, K. ve Lehtonen, K. (2013). On Preparedness of Memory Organizations for Ingesting Data. Borbinha, J., Nelson, M. Knight, S. (Yay. haz.). 10. *International Conference on Digital Preservation* içinde (276-279). Portekiz Milli Kütüphanesi.
- Lucker, P., Veenendaal, R. v., Sierman, B. ve Ras, M. (2018). Preservation Watch at the National Archives of the Netherlands. 15. *International Conference on Digital Preservation* içinde.
- Katre, D. (2012). An Overview of Digital Preservation Considerations for Production of “Preservable” E-Records: An Indian E-Government Case Study. Moore, R., Ashley, K. ve Ross, S. (Yay. haz.). 9. *International Conference on Digital Preservation* içinde (134-141). Toronto Üniversitesi.
- Külcü, Ö. (2014). *INTERPARES 3 Kurumsal Bilgi Sistemleri İçerisinde Belge Yönetimi: Türkiye’deki Kamu Üniversitelerinde Gerçekleştirilen Uygulamalara Yönelik Bir Durum Analizi*. 1011 TÜBİTAK Projesi, Proje No: 109K518.
- MacNeil, H. (2000). *Trusting Records: Legal, Historical and Diplomatic Perspectives*. Springer.
- Massol, M., Rouchon, O. ve Bechard, L. (2011). Certification and Quality: A French Experience. Borbinha, J. vd. (Yay. haz.). 8. *International Conference on Digital Preservation* içinde (11-19). Singapur Milli Kütüphanesi ve Nanyang Teknoloji Üniversitesi.
- McMeekin, S. ve Currie, A. (2022). Ain’t No Mountain High Enough: Developing a New Competency Framework for Digital Preservation. 18. *International Conference on Digital Preservation* içinde (99-107). DPC.
- Meehan, J. (2006). Towards an Archival Concept of Evidence. *Archivaria*, 61, 127-146.
- Miller, L., Blake, M. ve Sorsby, M. (2012). Evaluation of the Assessing Institutional Digital Assets (AIDA) Toolkit. *Science & Technology Libraries*, 31(1), 92-99.
- Molinaro, M. (2015). Long Term Preservation Strategies & Architecture: Views from Implementers. 12. *International Conference on Digital Preservation* içinde.
- National Digital Stewardship Alliance [NDSA]. (2020). *Sayısal Koruma Düzeylerinin Kullanımı: V2.0 için Genel Bir Bakış*. <https://osf.io/QGZ98>
- Van der Nat, J. ve Ras, M. (2017). A Dutch Approach in Constructing a Network of Nationwide Facilities for Digital Preservation Together. 14. *International Conference on Digital Preservation* içinde (99-107).
- Öztemiz, S. ve Özel, N. (2019). Dijital Küratörlük: Kavramsal Bir Değerlendirme. *DTCF Dergisi*, 59(2), 1208-1226.
- Pennock, M., Wheatley, P. ve May, P. (2014). Sustainability Assessments at the British Library: Formats, Frameworks, & Findings. Coates, S. vd. (Yay. haz.). 11. *International Conference on Digital Preservation* içinde (141-148). Victoria Eyalet Kütüphanesi.
- Preservation and Long-Term Access Through Networked Services [PLANETS]. (2022). <https://www.planets-project.eu>

- Popham, M. ve Mitcham, J. (2022). From Ray Cats to DPC RAM: How Best to Preserve a Digital Memory of the Nuclear Decommissioning Process. 18. *International Conference on Digital Preservation* içinde 315-318. DPC.
- Rogers, C. (2015). *Virtual Authenticity: Authenticity of Digital Records from Theory to Practice*. Yayınlanmamış Doktora Tezi. University of British Columbia.
- Sağlık, Ö. (2021). *Elektronik Belge Yönetimi Uygulamalarındaki Koşullar Işığında E-İmzalı Belgelerin Delil Değerinin Arşivsel Güvenilirlik Açısından İncelenmesi*. Yayınlanmamış Doktora Tezi. İstanbul Üniversitesi.
- Sağlık, Ö. (2021a). Arşivlenen Elektronik Belgelerin Güvenilirliğini Tehdit Eden Riskler: Teknolojik Koşullar Açısından Bir İnceleme. *Bilgi ve Belge Araştırmaları Dergisi*, 16, 29-47.
- Sağlık, Ö. (2022). Digital Preservation Capabilities of the Bursa Uludag University: Survey in the light of Digital Preservation Coalition Rapid Assessment Model. 18. *International Conference on Digital Preservation* içinde (470-472). DPC.
- Shabou, B. M. (2015). Digital Diplomats and Measurement of Electronic Public Data Qualities What Lessons Should be Learned? *Records Management Journal*, 25(1), 56-77.
- Shiers, J. vd. (2016). CERN Services for Long Term Data Preservation. 13. *International Conference on Digital Preservation*, 168-177.
- Sinclair, P. vd. (2009). Are you Ready? Assessing Whether Organizations are Prepared for Digital Preservation. 6. *International Conference on Digital Preservation* içinde (174-181). İsviçre Milli Kütüphanesi.
- Şahin, L. Ö. ve Saydam, V. (2022). Digital Continuity Practices in Municipalities: A Study on Municipalities in Istanbul. *Bilgi Yönetimi*, 5(1), 131-146.
- Tonta, Y. (2020). Dijital Kültürel Kaydın Korunması. *Türk Kütüphaneciliği*, 34(2), 229-248.
- Yalçınkaya, B. (2020). Geleceğin Arşivlerinin İnşası: Sosyal Medyanın Arşivlenmesi Hakkında Bir Değerlendirme. *Bilgi Yönetimi*, 3(1), 25-38.
- Zierau, E. ve Jensen, C. (2010). Preservation of Digitised Books in a Library Context. Rauber, A. vd. (Yay. haz.). 7. *International Conference on Digital Preservation* içinde (61-70).