Bilgi ve Belge Araştırmaları Dergisi
The Journal of Information and Documentation Studies

Bilgi ve Belge Araştırmaları Dergisi, Sayı: 16, 2021, 29-47
DOI: 10.26650/bba.2021.16.993556 Araştırma Makalesi / Research Article

Arşivlenen Elektronik Belgelerin Güvenilirliğini Tehdit Eden Riskler: Teknolojik Koşullar Açısından Bir İnceleme*

Risks Threaten The Trustworthiness of Archived Electronic Records: A Review in Terms of Technological Conditions

Özhan Sağlık[1]

*Bu çalışma; yazarın İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı'nda yürüttüğü "Elektronik Belge Yönetimi Uygulamalarındaki Koşullar Işığında E-İmzalı Belgelerin Delil Değerinin Arşivsel Güvenilirlik Açısından İncelenmesi" adlı doktora tezine dayanarak hazırlanmıştır..

[1] Öğretim Görevlisi, Bursa Uludağ Üniversitesi, Kütüphane ve Dokümantasyon Daire Başkanlığı, Bursa, Türkiye

ORCID: Ö.S. 0000-0002-1436-7431

Sorumlu yazar/Corresponding author:
Özhan Sağlık,
Bursa Uludağ Üniversitesi, Kütüphane ve Dokümantasyon Daire Başkanlığı, Bursa, Türkiye
E-posta: ozhan.saglik@gmail.com

Başvuru/Submitted: 15.09.2021
Revizyon Talebi/Revision Requested: 10.09.2021
Son Revizyon/Last Revision Received: 24.09.2021
Kabul/Accepted: 25.10.2021
Online Yayın/Published Online: 16.11.2021

Atıf/Citation: Sağlık, Ö. (2021). Arşivlenen elektronik belgelerin güvenilirliğini tehdit eden riskler: teknolojik koşullar açısından bir inceleme. *Bilgi ve Belge Araştırmaları Dergisi, 16,* 29–47. http://doi.org/10.26650/bba.2021.16.993556

ÖZ
Elektronik belgeler, özgünlük, tamlık ve gerçeklik özelliklerini arşivlendiklerinde de muhafaza edebilmelidir. Bu durum belgelerin güvenilirliği için temel kriterlerden biridir. Ancak, belgelerin muhafaza koşulları, güncellemeler ve kayıt ortamının kırılganlığı uzun dönemde problem oluşturabilecek risk faktörleri olarak gözükmektedir. E-belgelerin arşiv malzemesi olduğu dönemde ortaya çıkma ihtimali bulunan bu riskler, güvenilirliği tehdit edebilir. Bu tehdit, belgelerin özgünlüğü ve gerçekliğinden şüphe duyulmasına sebep olabilir. Sorun oluşturabilecek çok sayıda risk faktörü, hem tez gibi akademik çalışmalarda hem de bilimsel yayınlarda tespit edilmiştir. Bu makalede söz konusu risklerden belgedeki bit akışının bozulması, belge ile bileşenleri arasındaki ilişkinin kopması, e-belgenin muhafaza koşullarının sağlanamaması, özet değerlerinin eşleşememesi gibi teknolojik koşullar kaynaklı olanlar üzerinde durulacaktır. Çalışmanın teması, "belirtilen sorunlara hangi çözümler önerilebilir" şeklinde ortaya konulmuştur. Bu çözüm önerilerinin kurumlarda benimsenmesi için bir farkındalık oluşması hedeflenmektedir. Çalışmada nitel araştırma yöntemi benimsenmiş, doküman analizi tekniği kullanılmıştır.
Anahtar kelimeler: Elektronik belge yönetimi, arşivlenen e-belgeler, elektronik belgelerin güvenilirliği, riskler, teknolojik koşullar

ABSTRACT
The authenticity, accuracy, and reliability of electronic records must be maintained when they are archived because these criteria are essential for the trustworthiness. However, the storage conditions of the records, updates, and the fragility of carriers are considered risk factors in the long term that can endanger the fidelity of archived records and raise questions about their authenticity and reliability. Scholarly studies like Ph.D. dissertations and scientific publications have previously identified numerous risk factors. This qualitative study utilized the document analysis technique to highlight risks to records based on technological conditions, including bit decay, detachment of components, uncertain maintenance conditions, and disparity of hash values. In so doing, it aims to determine and postulate solutions to the specified problems to raise awareness for the adoption of the proposed solutions by organizations.
Keywords: Electronic records management system, archived electronic records, the trusworthiness of electronic records, risks, technological conditions

EXTENDED ABSTRACT

In recent years, scholarly efforts have been engaged with the new generation of information technology products labeled carrier media that often possess fragile structures and are prey to rapid technological changes. These attributes cause carrier media to pose numerous risks in their use and in the storage of records. Additionally, storage-environment-related risk factors such as heat, light, and humidity may also cause bit loss during recording. Further, software errors may be encountered, and the use-life of the storage devices could be shortened. The credibility of electronic records (e-records) could become questionable as these risks turn into problems that can damage the authenticity, accuracy, and reliability features required for trustworthiness.

In the circumstances, organizations should prioritize identifying potential risks that could threaten trustworthiness and develop solutions. These risks can be examined from many perspectives; however, the present study highlights the bit decay of the records, the detachment of their components, their uncertain maintenance conditions, and disparities of hash values. Such risks could transform into threats and cause doubts about the credibility of e-records if appropriate solutions are not devised. Records may lose their evidentiary value, their authenticity and integrity could be compromised, and they may not be trusted because of doubts about their reliability. Consequently, organizations may not be able to accurately explain their functions or sufficiently evidence how transactions were executed.

The results of the study of the effects of risks emanating from technological conditions on the trustworthiness of e-records suggest that the principle of pragmatism focusing on problem-solving may be adopted. A qualitative approach was adopted to conduct a case study to examine the research theme as it has evolved in the literature. The effect of risks arising from technological conditions on the trustworthiness of archived e-records was undertaken as a case study. The data obtained from the qualitative research was compiled under codes, categories, and themes. The theme for the study was determined as risks emanating from technological conditions. The categories included the risks examined in the study. The peer evaluation method was used to determine the validity of the codes and categories. Three experts who were Ph.D. candidates and had published articles on the relevant domain were consulted for their opinions.

The research problem was established as “risks arising from technological conditions that could threaten the trustworthiness of archived e-records.” The research question was iterated as: “What solutions can be offered to the specified problems emanating from technological conditions?” The investigation purposed to “raise awareness toward the adoption of solutions to risks that may threaten the trustworthiness of e-records.”

Organizations should update their storage hardware, periodically check the hash values of the records, and keep the records with error correction codes to avoid the risk of bit decay becoming a problem. Format identifiers such as DROID and JHOVE should be used, and unique identifiers should be assigned to the records and their components to counter the risk of detaching records from their elements.

The problem of not providing the necessary storage conditions is another risk that may be encountered. To combat this possibility, organizations should use storage devices with methods that are considered successful in storage. Records should be periodically transferred to new devices, and software should be regularly updated. Additionally, the constituents of records should be identified, and a guide should be established. Thus, quality control can be effected, and it may be determined whether processes are executed using the predetermined procedures.

Another risk that may be encountered concerns disparities in hash values. Organizations can create piecewise hashing to avoid this risk becoming a problem. Concurrently, the contexts of the records should be preserved along with their contents during such processes. The archival bond and diplomatic features must be preserved in such conditions, and predefined standard forms and templates should be created to accomplish this purpose. Also, the records should be authenticated using varied methods depending on their genres and functions. The authentication must be autonomously accomplished without human intervention.

As outlined, numerous solutions could be possible to counter the risks threatening the reliability of archived e-records. It would be a critical achievement if the National Archives could direct institutions by preparing a guide about the risks in question. In addition, records managers and organizational archivists should enhance their competencies to develop solutions against the mentioned risks.

GİRİŞ

Bilgi teknolojisi ürünü olan yeni nesil taşıyıcı ortamların teknolojinin çok hızlı değişmesi ve ürünlerin kırılgan bir yapıya sahip olması nedeniyle kullanım ve muhafaza sırasında birçok risk barındırdığı son yıllarda literatürü meşgul etmektedir. Sürekli yeni nesil ürünlerin piyasada kullanılmaya başlanması, elektronik belgelerin (e-belge) saklandığı depolama ortamlarının, kullanılan yazılımların ve belge formatlarının değişmesine sebep olmaktadır. Bu değişimin yanı sıra depolama ortamlarındaki ısı, ışık ve nem gibi risk faktörleri de kayıt ortamında bit kaybına sebep olabilmekte (Rosenthal, 2008, ss. 277-279), yazılım hatalarıyla karşılaşılabilmekte ve kullanılan cihazların kullanım ömrü kısalabilmektedir (Han ve Chan, 2008, s. 281; Young, 2020; Erickson ve Lunt, 2015, ss. 231-232). Durum böyle olunca, belgelerin güvenilirliği de sorgulanır hâle gelebilmektedir. Tüm bunlara kurumsal sürdürülebilirliğin sağlanamaması, yangın, sel gibi afetlere karşı planlar yapılamaması şeklindeki faktörler de sorun oluşturabilecek risk olarak eklenebilir (Rosenthal, Robertson, Lipkis, Reich ve Morabito, 2005). Hâliyle, karşılaşılabilecek muhtemel riskleri belirleyerek çözüm yolları geliştirmek kurumların öncelikleri arasında olmalıdır. Bunlar pek çok açıdan incelenmekle birlikte, bu çalışmada belgedeki bit akışının bozulması, belge ile bileşenleri arasındaki ilişkinin kopması, belgelere yetkisiz kişilerin erişmesi, e-belgenin muhafaza koşullarının sağlanamaması, şifrelemenin belgenin okunabilirliğini olumsuz etkilemesi, özet değerlerinin eşleşememesi ve teknolojik göç sürecinin layıkıyla gerçekleştirilememesi riskleri olarak öne çıkarılmaktadır.

Çözüm geliştirilmezse bu riskler tehdide dönüşerek e-belgelerin güvenilirliğinden şüphe duyulmasına neden olabilir. Özgünlüğü ve bütünlüğü bozulmuş, tamlığından şüphe duyulduğu için güvenilmeyen ve delil değeri özelliğini yitirmiş belgelerle karşılaşılabilir. Bunun neticesinde kurumlardaki fonksiyonlar doğru açıklanamadığı gibi işlemlerin nasıl yürütüldüğüne ilişkin deliller de yeteri kadar ortaya konulamayabilir.

Bu çalışmada öncelikle konuya ilişkin literatür değerlendirilmiştir. Ardından arşivlenen e-belgelerin güvenilirliğini tesis eden hususlar belirtilmiş, bu güvenilirlik için tehdit oluşturabilecek teknolojik koşullara dayalı riskler açıklanmıştır. E-belgedeki bit akışının bozulması, belge ile bileşenleri arasındaki ilişkinin kopması, belgelere yetkisiz kişilerin erişmesi, e-belgenin muhafaza koşullarının sağlanamaması, şifrelemenin belgenin okunabilirliğini olumsuz etkilemesi, özet değerlerinin eşleşememesi ve teknolojik göç sürecinin layıkıyla gerçekleştirilememesi gibi bu risklerin, bir makalenin hacmine sığmayacak kadar çok ve çeşitli olduğundan, burada bir kısmı ele alınabilmiştir. Bunlar, belgedeki bit akışının bozulması, belge ile bileşenleri arasındaki ilişkinin kopması, e-belgenin muhafaza koşullarının sağlanamaması ve özet değerlerinin eşleşememesidir. Sonuç ve öneriler kısmında ise bu risklere karşı kurumların alabileceği çözüm önerileri tartışılmaktadır.

1. Literatür Taraması

E-belge yönetimi uygulamalarında karşılaşılabilecek riskler hakkında pek çok çalışma bulunmaktadır. Bu çalışmaları doktora tezleri ve makaleler, milli arşiv gibi otorite kurumların yayınladığı rehberler ile çeşitli derneklerin çıkardığı yayınlar şeklinde ele almak mümkündür. Tezlerin konuyu derinlemesine tartıştığı, arşiv yayınlarının ülke genelinde kurumların çalışmalarına rehberlik ettiği, dernek yayınlarının ise model sunduğu görülmektedir.

Naomi Hay-Gibson'un Newcastle Üniversitesinde 2011'de yazdığı doktora tezi müstakil olarak e-belge yönetimi uygulamalarında karşılaşılabilecek riskleri inceleyen ilk çalışmalardan biridir. Hay-Gibson, bir saha araştırması yaparak risk değerlendirmesine nasıl yaklaşmak gerektiğini açıklamış, buna ilişkin tespitler yapmıştır. Burada özgünlük ve bütünlük gibi e-belgelerin güvenilirliğini tesis eden karakteristik özelliklere ilişkin risklerin neler olabileceğini tartışmıştır (Gibson, 2011). Bu akademik çalışmanın yanı sıra çeşitli arşivcilik derneklerinde yöneticilik yapan Toronto ve Pittsburgh Üniversitesinde misafir öğretim üyesi olarak çalışan Bearman ile e-belgelerin güvenilirliği konusunda çalışmaları bulunan British Columbia Üniversitesi öğretim üyesi Lemieux ve Amerika Birleşik Devletleri'nde çeşitli özel kurumlarda belge yöneticisi olarak görev yapan Krumwied'in makaleleri de dikkat çekmektedir. David Bearman, e-belgelerle ilgili risklere dikkat çeken ilk makalelerden birini kaleme almıştır (Bearman, 2006). Lemieux ve Krumwied (2011) ise 2011 yılındaki çalışmasında finans sektöründeki belgelerin güvenilirlikle ilişkilendirilebilecek yaşam döngüsündeki safhalarda karşılaştığı riskleri değerlendirmiştir.

Türkiye'de müstakil olarak elektronik belge yönetimi alanında belgelerin karşılaşabileceği riskleri ele alan tez niteliğinde akademik çalışmalar görülemese de konu hakkında kitap, makale bildiri gibi türlerde çalışmalar bulunmaktadır (Yıldız, 2010; Aydın ve Özdemirci, 2011; Külcü, Çakmak ve Özel, 2015; Çiçek, 2021). Ancak bunlardan müstakil olarak karşılaşılabilecek riskleri ele alan çalışmalardan İstanbul 29 Mayıs Üniversitesi Bilgi ve Belge Yönetimi Bölümü öğretim üyesi Bekir Kemal Ataman, Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümü öğretim üyesi Bahattin Yalçınkaya ile Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü öğretim üyeleri Tolga Çakmak ve Şahika Eroğlu'nun yayınları dikkat çekmektedir. Ataman, 2005 yılında yayınlanan makalesinde elektronik belgelerin arşivlenmesinde karşılaşılabilecek sorunlara değinmiştir (Ataman, 2005). Yalçınkaya, International Organization of Standardizaton (ISO) 18128 Belge Süreçleri ve Yönetimi için Risk Değerlendirme Standardı'nı (Risk Assessment for Records Processes and Systems) temel alarak e-belge yönetim sistemlerinde karşılaşılabilecek riskleri açıklamıştır (Yalçınkaya, 2014). Bununla birlikte, 2016 yılında yayınlanan başka bir makalesinde Yalçınkaya, elektronik belge yönetimi uygulamalarında başarıyı olumsuz etkileyebilecek risk unsurlarını incelemiştir (Yalçınkaya, 2016). Çakmak ve Eroğlu ise 2016 yılında yayınlanan bildirilerinde bilgi güvenliğiyle ilgili yaşanabilecek riskleri incelemiş (Çakmak ve Eroğlu, 2016); 2020 yılındaki makalelerinde ise e-belgelerin uzun

vadeli korunmasında karşılaşılabilecek risklerin neler olabileceğine değinmişlerdir (Çakmak ve Eroğlu, 2020). Ancak, söz konusu eserlerde çalışmaların odak noktasını güvenilirliği tehdit edebilecek risklerin oluşturmadığı görülmektedir.

Bu çalışmaların yanı sıra milli arşiv gibi otorite kurumların yayınladığı rehberler dikkat çekmektedir. Türkiye'de Devlet Arşivleri Başkanlığının bu yönde bir eseri görülemese de Kamu Sertifikasyon Merkezinin (KAMU SM) karşılaşılabilecek riskleri belirterek bir risk değerlendirmesi yaptığı rehber dikkat çekmektedir. Burada risklerin daha çok elektronik imza (e-imza) ve elektronik mühürlerle (e-mühür) ilgili olan açık anahtar altyapısı ve şifrelemeye yönelik olduğu anlaşılmaktadır (KAMU SM, 2015).

Farklı ülkelerin milli arşivlerinin ise e-belge yönetimi uygulamalarında karşılaşılabilecek riskler hakkında dikkat çeken çalışmalar yaptığı gözlenmektedir. Örneğin İngiliz Milli Arşivinin [The National Archives] (TNA) bu konuda kayda değer çalışmaları bulunmaktadır. 2017 yılında yayınlanan Risk Assessment Handbook adlı kitapta güvenin belgelerin karakteristik özelliklerinden biri olduğu belirtilmiş, bunun korunamaması hâlinde hangi sorunlarla karşılaşılabileceği ifade edilmeye çalışılmıştır (TNA, 2017). Bununla birlikte, sistem değişikliklerinde karşılaşılabilecek riskler açıklanarak güvenin korunması için nelerin yapılması gerektiği dile getirilmiştir (TNA, 2017a; TNA, 2017b; TNA, 2017c). TNA'nın risk değerlendirmesiyle ilgili son çalışması ise The Digital Archives Graphical Risk Assessment Model (Sayısal Arşivler Grafiksel Risk Değerlendirme Modeli - DIAGRAM)'dir. Burada, kullanılan donanım malzemeleri, sistem güvenliği ve kurumun teknolojik yeterliliği üzerinden bir risk puanı oluşturulmaktadır (TNA, 2021).

TNA'nın bu çalışmalarının yanı sıra Amerika Birleşik Devletleri'nin milli arşivi olan National Administration of Records and Archives (NARA), sürekli değişen teknolojik koşullar karşısında e-belgelerin sürdürülebilirliği için risk yönetimi planı hazırlamıştır. Burada riskler sınıflandırılarak risk iştahları belirlenmiştir. Ancak TNA'nın rehberlerinin aksine karşılaşılabilecek risklerin e-belgelerin güvenilirliğiyle ilişkilendirilmediği görülmektedir (NARA, 2010).

Milli arşiv gibi kurumların yaptığı bu çalışmaların yanı sıra çeşitli dernekler de risk değerlendirmesine ilişkin eserler yayınlamıştır. Bunlardan elektronik veri içeren sistemlerin güvenilirliğiyle ilişkilendirilen ve Research Libraries Group (Araştırma Kütüphaneleri Grubu) ile NARA tarafından geliştirilerek The Consultative Committee for Space Data Systems (Uzay Verisi Sistemleri için Danışma Komitesi - CCSDS) tarafından zenginleştirilen ve sonrasında ISO 16363 Audit and Certification of Trustworthy Digital Repositories (Güvenilir Sayısal Depolar için Denetim ve Sertifikasyon) standardına dönüşen güvenilir depolara ilişkin kriterler öne çıkmaktadır. Burada elektronik verilerin yönetimiyle alakalı politika ve prosedürlerin varlığı, bunları layıkıyla yönetebilmek için gerekli olan görevlerle malî ve idarî ihtiyaçların

belirlenmesi, güvenilirliklerinin onaylanması gibi hususlar kritik edilmektedir. Buradaki başarıya göre ilgili sistemler güvenilir olarak nitelendirilmektedir (ISO, 2012).

Bu çalışmaların yanı sıra Digital Preservation Coalition (Sayısal Koruma Koalisyonu - DPC) gibi kuruluşlar tarafından olgunluk modeli geliştirme çalışmaları kapsamında risk değerlendirmesi yapıldığı (DPC, 2021), Digital Curation Centre (Sayısal Kürasyon Merkezi - DCC) tarafından yayınlanan DRAMBORA (McHugh, Ross, Ruusalepp ve Hofman, 2007) ve Minnesota Tarih Cemiyetinin yayınladığı Trustworthy Information Systems Handbook (Güvenilir Bilgi Sistemleri El Kitabı) adlı yayında güvenilir bir arşivin şartlarından birinin risk değerlendirmesi yapılmasıyla ilişkilendirildiği görülmektedir (Minnesota, 2002). Burada ifade edilen çalışmalardan anlaşılacağı üzere e-belgelerin güvenilirliğiyle ilişkilendirilebilecek riskler oldukça çeşitlidir. Ülkelerin politik durumlarının belirsizleşmesinden teknolojik koşulların yenilenme hızına yetişilememesine, iklim koşullarının değişmesinden belgeleri layıkıyla yönetebilecek uzman istihdamı eksikliğine kadar geniş yelpazede risklerle karşılaşmak mümkündür. Ancak bunlar arasından bir tercih yapılarak bu makalede teknolojik koşullara yönelik risklere yoğunlaşılmıştır. Bu risklerden de belgedeki bit akışının bozulması, belge ile bileşenleri arasındaki ilişkinin kopması, güvenilirliği korumak için gerekli olan yazılım ve donanım koşullarının sağlanamaması ve özet değerlerinin eşleşememesi incelenmektedir.

2. Çalışmanın Problemi, Sorular, Yöntem ve Etik Onay

2.1. Çalışmanın Problemi

Sahada e-imzaların arşivlenmemesi, gerekli donanım ve yazılım koşullarının sağlanamaması, şifrelemenin standartlardan uzak yapılması gibi e-belgelerin güvenilirliğini tehdit edebilecek pek çok riskle karşılaşılmaktadır. Bu risklerin muhtemel sonuçlarına ilişkin çalışmalar Literatür Taraması Bölümü'nde ifade edilmiştir. Söz konusu çalışmalar, risklerin getirebileceği problemlerin çözümüne odaklanılması fikrini gündeme getirmektedir. Durum böyle olunca, bu risklerin e-belgelerin güvenilirliğine etkisini irdeleyen bu çalışmada pragmatizm felsefesinin benimsenebileceği düşünülmüştür. Çünkü bu felsefede problemlerin çözümüne odaklanılmaktadır (Creswell, 2016, s. 28).

Çalışmanın sorunu incelenirken literatürdeki kaynaklar üzerinden hareket edilmiştir. Hâliyle nitel araştırmanın gerçekleştirilebileceği kararlaştırılmış ve bir nitel araştırma türü olan durum çalışması benimsenmiştir. Bu çalışmada bir durum hakkında bilgi toplanmakta ve onun nitelemesi yapılmaktadır (Creswell, 2016, ss. 97-98). Bir durum olarak teknolojik koşullar kaynaklı risklerin arşivlenen e-belgelerin güvenilirliğine etkisi incelenmiştir.

2.2. Çalışmanın Sorusu

Çalışmanın problemi "arşivlenen e-belgelerin güvenilirliğini tehdit edebilecek teknolojik koşullar kaynaklı risklerdir". Bu riskler, belgelere erişememek ve onları sağlıklı koşullarda arşivleyememek şeklinde sonuçlara neden olabilecek sorunları gündeme getirmektedir. Çalışmanın sorusu ise "arşivlenen elektronik belgelerin güvenilirliğini tehdit eden teknolojik koşullar kaynaklı sorunlara hangi çözümler önerilebilir" şeklindedir. Amacı ise "e-belgelerin güvenilirliğini tehdit edebilecek risklere karşı getirilecek çözüm önerilerinin kurumlarda benimsenmesi için bir farkındalık oluşturmaktır".

2.3. Çalışmanın Yöntemi

Nitel araştırmalarda elde edilen verilerin kod, kategori ve temalar altında bir araya getirilmesi beklenir (Creswell, 2016, ss. 184-185). Literatürdeki kaynaklardan verilerin oluşturulduğu bu çalışmada tema, teknolojik koşullar kaynaklı riskler şeklinde belirlenmiştir. Kategoriler ise belgedeki bit akışının bozulması, belge ile bileşenleri arasındaki ilişkinin kopması, e-belgenin muhafaza koşullarının sağlanamaması ve özet değerlerinin eşleşememesi olarak ifade edilebilir. Risk olarak belirlenen bu kategorilere neden olan ve elimizdeki çalışmanın Güvenilirliği Tehdit Eden Riskler kısmında açıklanan hususlar ise kodları oluşturmaktadır.

Çalışmada belirlenen kod ve kategorilerin geçerliliği için akran değerlendirmesi yönteminden faydalanılmıştır. Çalışmanın temas ettiği alana ilişkin doktora çalışması yürüten ve aynı zamanda makale niteliğinde yayınları bulunan üç uzmanın görüşüne başvurulmuştur.[1] Elde edilen değerlendirmeler neticesinde kod ve kategorilerin temayla uyumlu olduğuna karar verilmiştir. Çalışmada nitel araştırma yöntemi benimsenmiş, doküman analizi tekniği kullanılmıştır.

2.4. Etik Kurul Kararı

Çalışma sırasında araştırma ve yayın etiğine uyulmuştur. "Elektronik Belge Yönetimi Uygulamalarındaki Koşullar Işığında E-imzalı Belgelerin Delil Değerinin Arşivsel Güvenilirlik Açısından İncelenmesi" başlıklı doktora tezi çalışması kapsamında yapılan bu araştırmanın İstanbul Üniversitesi Rektörlüğü, Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu Başkanlığı tarafından 10.07.2020 tarih ve 08 sayılı toplantısında araştırma ve yayın etiğine uygunluğu teyit edilmiştir (Karar no: 2020/16).

3. Arşivlenen Elektronik Belgelerin Güvenilirliği

Belgelerin güvenilirliğinin korunması için taşıyıcı ortam, içerik, düzenleyen, kontekst gibi özelliklerin muhafaza edilmesi gerektiği bilinmektedir. Söz konusu niteliklerin korunup

1 Marmara Üniversitesi Türkiyat Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı doktora öğrencileri Emin Gedikli, Varol Saydam ve Oytun Cibaroğlu.

korunmadığıyla alakalı olarak diğer alanlara göre belgeyle daha çok ilişkisi olduğu düşünülen hukuk, diplomatik ve tarih disiplinlerinde güvenilirlik konusunda yaklaşımlar geliştirilmiştir. Böylece belgelerin güvenilirliğini hukukî, diplomatik ve tarihî açıdan analiz etmek mümkün olmuştur.

Ancak, belgelerin delil değerinin korunmasını inceleyen güvenilirliğin ilgili disiplinlere göre farklı tanımlandığı dikkat çekmektedir (International Research on Permanent Authentic Records in Electronic Systems - Elektronik Sistemlerde Kalıcı Özgün Belgeler Üzerine Uluslararası Araştırma [INTERPARES], 2021). Mesela, hukukî güvenilirlik, belgenin yaşam döngüsü içerisinde onu üreten yetkilinin otorite ve garantisini gösteren hukukî delillere sahip olmasını ifade eder (Çiçek, 2009, s. 212). Bir belgenin mevzuatta yer alan özellikleri haiz olup olmadığının incelendiği hukukî güvenilirlikte, belge üretmede yetki mekanizması ve belge yönetimi süreçlerinde prosedürlerin tesis edilip edilmediği kontrol edilir (MacNeil, 2000, ss. 53-56). Hukukî güvenilirliğin yanı sıra belgelerin güvenilirliğinin incelemesinde kullanılabilecek diğer bir yaklaşım da diplomatik güvenilirliktir. Bu yaklaşımda belgenin karakteristiğini açıklayan form unsurlarının uygun şekilde bulunup bulunmadığı değerlendirilmektedir (Çiçek, 2009, s. 212). 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, e-mühür, kullanılan donanım ve yazılımların özellikleri, log kayıtları, denetim günlükleri ve veritabanı kayıtları incelenmektedir (MacNeil, 2000, ss. 73-75, 91, 96-97, 100-102; Çiçek, 2011, s. 97). Tarihî güvenilirlikte ise belgenin içerdiği bilgilerle yer ve olayların uyuşup uyuşmadığı kontrol edilir (Çiçek, 2009, s. 212).

Belgelerin güvenilirliğinin korunmasına yönelik yaklaşımların geliştirildiği INTERPARES gibi uluslararası saha çalışmalarında bu güvenilirlik yaklaşımlarından yararlanıldığı bilinmektedir. INTERPARES'de çok disiplinli bir ekiple çalışılsa da meselenin daha çok arşivcilik ve belge yönetimi bakış açısıyla incelendiği görülmektedir. Hâliyle, burada diplomatik güvenilirlik yöntemlerinden daha fazla yararlanılmıştır. Bunun neticesinde diplomatik analiz yöntemleri, arşiv biliminin bakış açısıyla zenginleştirilmiştir.

Bununla birlikte, diplomatik güvenilirliğin e-belgelerin güvenilirlik analizinde tek başına yeterli olamayabileceği ifade edilmektedir (Bushey, 2016). Çünkü belgelerin oluşumuna kaynaklık eden mevzuat ve kullanılan bilgi teknolojileri meselenin daha geniş bir bakış açısıyla ele alınmasını gerektirmiştir. Bu duruma örnek teşkil edecek çalışmalardan biri, INTERPARES'in araştırmacılarından Jessica Bushey'in sosyal medya platformlarındaki fotoğrafların güvenilirliğini incelediği doktora tezidir. Bu çalışmada diplomatik analiz yöntemlerinin yanı sıra, fotoğrafçılık ve yeni medya yaklaşımı ile delil hukukundan yararlanmıştır. Bushey, bu incelemeyi yaptığı çalışmanın başlığını arşivsel güvenilirlik olarak belirlemiştir (Bushey, 2016). O hâlde, arşivsel güvenilirlik yaklaşımına göre güncel belgeler, özgünlük, tamlık ve gerçekliği arşiv belgesi oldukları dönemde de muhafaza etmelidir (INTERPARES, 2002, ss. 335, 816). Bu nedenle

belgeler, güncel dönemdeki gibi arşiv malzemesiyken de özgün, tam ve gerçek olduğu müddetçe güvenilir kabul edilir.

Belgenin özniteliklerinin üretildikten sonraki zaman içerisinde değişmemesi olarak açıklanan "özgünlük" (Rogers, 2015, s. 26), tanımlanabilirlik ve bütünlük olmak üzere iki aşamada incelenmektedir. Tanımlama, belgenin delil değeri unsurlarından olan karakteristik özelliklerini belirterek onun diğer belgelerden ayırt edilmesini sağlar. Bu özelliklere, belgedeki kişiler, üretim ve iletim tarihi, konu, arşivsel bağ, dosya kodu ve belgenin ekleri örnek verilebilir (Çiçek ve Sağlık, 2019, ss. 150-151). Özgünlüğün bir diğer aşaması ise belgenin tüm yönleriyle bozulmamış ve değiştirilmemiş olmasını ifade eden bütünlüktür. Elektronik taşıyıcı ortamın kırılganlığı, teknolojik eskimeler ve sistemlerin standartlardan uzak bir şekilde geliştirilmesi belgelerin bütünlüğünü oluşturan unsurlardan bit akışını olumsuz etkileyebilir (Çiçek ve Sağlık, 2019, s. 151). Burada, bit akışı aracılığıyla görünen ve belgedeki yetki veya hakları göstermesi nedeniyle delil değeri unsurlarından biri olan içeriğin değişmemesi hedeflenir. Ancak, bit akışının korunup içeriğin değişmemesi tek başına bütünlüğün muhafazası için yeterli kabul edilmemektedir. Çünkü belgenin semantik yapısında yaşanacak bir kayıp, belgedeki yetki veya hakların yeteri kadar anlaşılamamasına neden olabilecektir (Çiçek ve Sağlık, 2019, s. 152). Bu nedenle belgedeki kontekst bilgisinin de korunmasına ihtiyaç duyulmaktadır. İçerik ve kontekstin korunması gerekliliği, belgelerin üretildikten sonra da bütünlüklerinin kontrol edilmesini gerekli kılmaktadır (Çiçek ve Sağlık, 2019, s. 152).

Özgünlüğün yanı sıra belgelerin bir diğer güvenilirlik unsuru "tamlık"tır. Tamlık arz eden bir belgede kesin, doğru, hakikate uygun ve tahrifattan uzak olmak özellikleri aranmaktadır. Buna göre, tamlık, hukukî sonuç meydana getirebilmek için belgenin üreticisi ve idarî-hukukî sistem tarafından ihtiyaç duyulan tüm elemanların varlığını ifade etmektedir. Çünkü belge, üretilme gerekçesi olan hukukî prosedüre ve görmesi gereken idarî işlem türüne göre belge vasfı kazanmaktadır (Çiçek ve Sağlık, 2019, s. 152).

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 ise belgeyi hukukî bir sonuç doğurmaya elverişli hâle getirecek entelektüel formun tüm elemanlarının mevcut olmasını ifade etmektedir (Çiçek ve Sağlık, 2019, ss. 152-153).

Özgünlük, tamlık ve gerçekliğin yani güvenilirliğin korunması için çeşitli analiz yöntemlerinin benimsenmesi gerekir. INTERPARES'in koordinatörlerinden Corinne Rogers'a göre benimsenecek yöntemler, belge üretildikten, alındıktan ve dosyasına kaldırıldıktan sonra da belgenin değiştirilmediğini, müdahaleye uğramadığını veya sahteciliğe maruz kalmadığını gösterebilmelidir. Rogers, bu yöntemleri entelektüel ve teknolojik olmak üzere iki başlıkta

değerlendirmektedir. Arşivcilik kaynaklı olduğu anlaşılan entelektüel yöntemler, belgenin arşivcilik standartlarına göre tanımlanmasını ve belgenin provenansını, kontekstini ve türüne göre yapısının sunulmasını içermektedir (Rogers, 2015, ss. 28, 35). Burada, taşıyıcı ortam, içerik, form özellikleri, belgedeki işlem ve kişiler, arşivsel bağ, üstveriler, kontekst ve belge formunun tamlığı ile diplomatik özellikler öne çıkmaktadır (MacNeil, 2000, ss. 91, 96-97). Teknolojik yöntemler ise kullanılan donanım ve yazılımın teknik boyutuyla ilişkili olup (Rogers, 2015, s. 35), e-imza, e-mühür, log kayıtları, denetim günlükleri ve veri tabanı kayıtlarının analiz edilmesini kapsamaktadır (MacNeil, 2000, ss. 73-75, 100-102).

Yukarıdaki hususların yanı sıra, Penn State Üniversitesi kütüphanecilerinden Jennifer Meehan belge ile belgedeki işlem ve faaliyet arasındaki ilişkinin incelenmesi gerektiğini ileri sürmektedir (Meehan, 2006, s. 142). Bu durum, belgenin aynı faaliyet kapsamında üretildiği diğer belgelerle olan ilişkisinin ortaya konulmasına duyulan ihtiyaçtan kaynaklanabilir. Bu ihtiyaç, arşivsel bağın açığa çıkarılmasını gerektirmektedir. Bunun için belgenin provenansı ile konteksti analiz edilerek belgelerin oluşumuna kaynaklık eden fonksiyonlar saptanır; aynı faaliyet kapsamında oluşan ve aralarında organik bağ bulunan belgeler bir araya getirilir (Çiçek, 2015, s. 154). Böylece, belge ile belgedeki faaliyet arasındaki ilişki ortaya konur (Meehan, 2006) ve arşivsel bağ açığa çıkarılır. Belgelerin güvenilirliğinin süreklilik arz etmesinin hedeflendiği arşivsel bağın açığa çıkarılması sürecinde kimliklendirme, tanımlama gibi çeşitli mekanizmalar ile bu mekanizmaların nasıl kullanılacağını gösteren prosedürlerden yararlanılmaktadır. Manitoba Üniversitesinde öğretim üyeliği yapan Kanadalı arşivci Terry Cook'a göre bu mekanizmalardan fonlara saygı, aslî düzeni korumak ve provenansı tesis etmek ilkeleriyle arşivsel bağı açığa çıkarmak mümkün olabilir (Cook, 2013, ss. 99-100).

INTERPARES'in koordinatörlerinden Luciana Duranti ve Corinne Rogers, belgenin güvenilirliğinin başarıyla korunması için güvenilir kişiler tarafından politikalar, prosedürler ve mekanizmalar geliştirilmesi gerektiğini ileri sürmektedir. Bu amaçla geliştirilen politika ve prosedürlerin belgelerin üretimi, doğrulanması, özgünlüğünün onaylanması ve korunması süreçlerine yönelik olduğu ifade edilmektedir. Bu süreçlerde kullanılacak arşivsel bağ, diplomatik analiz, log kayıtlarının incelenmesi gibi araçlar ise güvenilirliğin başarıyla korunması için gerekli olan mekanizmalara örnek verilebilir. Bu politika ve prosedürler ile mekanizmaları geliştirecek güvenilir kişilerin ise arşivlerde çalışan arşivciler olduğu belirtilmektedir (Duranti ve Rogers, 2011, ss. 376-377). O hâlde, arşivler ve arşivcilerin belgelerin güvenilirliğinin korunmasında önemli görevleri bulunduğu anlaşılmaktadır. Bu görev, binlerce yıldır arşivlerin başka kurumlarda üretilmiş ve sonrasında kendisine devredilmiş belgelerin güvenilirliğini koruması gibi bir özelliğe sahip olmasından kaynaklanmaktadır (Guo, Fang, Pan ve Li, 2016, ss. 171-172).

4. Güvenilirliği Tehdit Eden Riskler

Belgenin muhafaza edildiği ortamın koşulları, güncellemeler ve format olarak taşıyıcı kayıt ortamının kırılganlığı gibi daha çok belgenin arşiv malzemesi olduğu dönemde ortaya çıkan problemler, güvenilirliği tehdit eden riskler arasında değerlendirilmektedir. Bunlar, belgelere erişememek ve erişilse dahi, ilk üretildiği özgünlükte bulamamak gibi sonuçlara neden olabilecek sorunları gündeme getirmektedir. Bu sorunlar, belgelerin güvenilirliklerinden şüphe duyulmasına da sebep olabilir.

4.1. Bit Akışının Bozulması

Teknolojik koşullar kaynaklı risklerin başında bit akışının bozulması gelmektedir. Çünkü radyasyon, sabit disklerin okuma ve yazma yapan kısımlarının birbiriyle çarpışması, depolama donanımının eskimesi gibi nedenlerle kayıt ortamındaki belgenin bit akışı bozulabilmektedir. Bunun sonucunda belgeyi oluşturan bileşenlere erişimde sorun yaşanacağından belgenin yeniden üretilmesi[2] mümkün olmayabilir. E-belgeler, bileşenleri yeniden tanzim edilerek oluşturulduğundan bileşenlere ve belgeye ait bit akışının korunması gerekir. Bundan dolayı, özet değeri kontrolü ve hata düzeltme kodları oluşturmak gibi yöntemler kullanılmaktadır (Glassford, 2018, ss. 95-97; ISO, 2015, ss. 14-17).

4.2. Belge İle Bileşenleri Arasındaki İlişkinin Kopması

Bit akışının bozulması riskinin yanı sıra, zaman içerisinde belge ile üstveri, ekleri ve e-imza gibi bileşenleri arasındaki ilişkinin kopma ihtimali de söz konusudur. Bu ihtimal, farklı işletim sistemleri arasında belge transferi yapılmasından dolayı belge ile bileşenleri arasında organik bir ilişki kurulamaması gibi nedenlerden kaynaklanabilmektedir. Mesela, Linux ve Windows işletim sistemleri farklı dosya uzantıları kullanmaktadır. Her ne kadar, bu şekilde dosya uzantıları işletim sistemlerinin kendi içlerinde çözüm üretmeye imkân verse de farklı sistemler için problem oluşturabilmektedir. Örneğin işletim sistemleri belgeleri standart bir yapıda değil, sadece kendi kütüphanelerindeki yazılım dilleriyle oluştururursa bu iki sistem arasında belge alışverişi yapıldığında belgeler okunamayabilir (Niu, 2015, s. 67). Bununla birlikte, belge ile üstveri dosyası gibi bileşenleri arasında ayrılmaz bir ilişki kurulamamış olabilir. Bundan dolayı, Digital Record Object Identification (Sayısal Belge Nesnesi Kimliklendirme - DROID) ve

2 E-belgelerin ilk oluştuğunda meydana gelen bit yapısının korunması mümkün olamamaktadır. Çünkü belge sistem içerisindeki her iletiminde sahip olduğu yeni özelliklerle yeni bir bit yapısına kavuşmaktadır. Bu durum, e-belgelerin orijinalinin mevcut olamayacağı görüşünün ileri sürülmesine kaynaklık etmektedir. Bu görüşe göre, orijinal bir belge ilk oluştuğu özelliklerini koruyan belgedir. E-ortamda bu durum mümkün olmadığından belgenin orijinali değil, onunla aynı delil değerine sahip olan reprodüksiyonların bulunduğu ifade edilmektedir (INTERPARES, 2008, s. 120; Thibodeau, 2013, ss. 12-13, 15-17). Hâliyle ilk üretildiği gibi orijinal hali olmasa da söz konusu bileşenlerin korunup yeniden tanzim edilerek delil değerini hâlâ muhafaza eden ve hukukun kabul ettiği belgenin tekrar oluşturulabileceği fikri gündeme gelmiştir. Bu fikir, bileşenleri korunmuş bir belgeye dayanılarak orijinaline en yakın nüshanın oluşturulabileceğini ileri sürmektedir (INTERPARES, 2008, ss. 120-121; Duranti ve Thibodeau, 2006, s. 32).

JSTOR/Harvard Object Validation Environment (JSTOR/Harvard Nesne Doğrulama Ortamı - JHOVE) türünden format tanımlayıcıların kullanılarak işletim sistemlerinden bağımsız şekilde Elektronik Yazışma Paketi (EYP) gibi belgelerin standart bir yapıda üretilmesi (Kirschenbaum, Ovenden ve Redwine, 2010, ss. 17-19) ve belge ile bileşenlerine tek biçim tanımlayıcılar atanması önerilmektedir (TNA, 2017a, ss. 28-31).

4.3. E-Belgeler İçin Gerekli Muhafaza Koşullarının Sağlanamaması

E-belgelerin güvenilirliğini doğrudan etkileyen bir diğer husus da kullanılan donanımlar için uygun sıcaklık, nem ve ışık koşullarının sağlanmasıdır. Mesela saklama ünitelerinin belirlenen sıcaklık ve nem koşulları sağlanmadığı ve kullanım ömrü bittikten sonra yenilenmediği takdirde bozulduğu bilinmektedir. Bu koşulların belirli niteliklere sahip olması gerekir. Durum böyle olunca günümüz koşullarında Redundant Array of Independent Disks (Bağımsız Disklerin Artıklık Dizisi - RAID) 10 gibi saklamada başarılı olduğu kabul edilen yöntemlere sahip saklama cihazlarının kullanılması önerilmektedir (ISO, 18492, s. 4). Bununla birlikte, teknolojik eskimeyle karşı karşıya kalmamak için yeni cihazlara periyodik olarak belge aktarımı yapılabilir.

E-belgenin muhafaza sırasında nem ve ışık koşullarının sağlanamaması gibi diğer bir etken de gerekli yamaların yapılmamasıdır. Bunun neticesinde sistemden veri sızıntısı, belge yönetimi standartlarına uyum sağlayamamak ve belgelere uzun dönemli koruma yöntemlerinin uygulanmaması gibi sorunlar oluşabilir. Bu sorunlar, belgelerin bütünlüğünü bozabilecek mahiyettedir. Oysa belge bütünlüğünü korumak için yazılımların periyodik olarak güncellenmesi önerilmektedir (TNA, 2017b, ss. 11-12).

E-belgeler, format, işletim sistemi ve yazılım dilleri gibi çeşitli teknolojik bileşenlere bağımlıdır. Belgelerin uzun süreli korunup sürdürülebilirliğini sağlamak için söz konusu bileşenlerin bilinçli olarak ve kontrollü bir şekilde yönetilmesi gerekir. Bunun gerçekleşmesi için bileşenler kayıt altına alınmalı, tanımlanmalı ve dokümantasyonu oluşturulmalıdır. Bu aşamada kullanılması gereken yazılım ve donanımlar, ihtiyaç duyulan personel deneyim ve yeteneği ile malzemelerin kullanım ömrü gibi hususlar belirtilmelidir (TNA, 2017b; TNA, 2017a, ss. 5-6). Teknolojik bileşenler tanımlanırken belge formatı, kullanılacak cihazlar, teknolojik göç planları gibi belgenin erişim ve saklanmasını etkileyen hususlar ifade edilmektedir. Aynı zamanda, belgelerin üretilme koşulları ve onu meydana getiren bileşenler, belge ile üstveriler arasındaki ilişkinin kurulması, belgenin bütünlüğü ve tamlığının kontrol edilmesi ile log kayıtlarında yer alacak hususlarla benimsenecek güvenlik önlemleri açıklanır (TNA, 2017a, ss. 9-11).

E-belgelerin güvenilirliğinin korunmasında belgeye kimin ne zaman nasıl eriştiğini gösteren log kayıtlarından oldukça faydalanıldığı görülmektedir. Bundan dolayı, log kayıtlarının özgünlüğü korunarak belgeyle ilişkilendirilmeleri gerekir (TNA, 2017a, s. 32). Bu kayıtlar

aynı zamanda yeni formatlara aktarılabilir olmalıdır. Özgünlüğün korunduğunun tasdik edilmesi, insan müdahalesine gerek duymadan otonom bir şekilde gerçekleşmelidir. Log kayıtları aynı zamanda belgenin yaşam döngüsünde geçirdiği aşamaların dokümantasyonu olarak kullanılabilir (Duranti, 2010, s. 83).

Burada üstverilerden de yararlanılmaktadır. "Belgede yapılan işlemlerin kim tarafından gerçekleştirildiği, gerçekleşme tarihi, ortam yenilemesi öncesinde ve sonrasındaki döngüsel artıklık denetimi ve özet değerlerinin karşılaştırılması" gibi üstverilerin oluşturulabileceği ifade edilmektedir. Böylece, yapılan işlemlerin daha önceden belirlenen prosedürler dâhilinde yürütülüp yürütülmediği incelenebilir ve kalite kontrolü yapılabilir (ISO, 2005, ss. 9-12). Bu işlemler sırasında belgenin içeriğiyle birlikte konteksti de muhafaza edilmelidir (The National Electronic Commerce, 2002, s. 21). Durum böyle olunca, belgenin diplomatik özellikleri ile arşivsel bağının korunması gerekir. Bunun için önceden tanımlanmış standart form ve şablonlar oluşturulmalı, belge türü ve fonksiyona göre çeşitlenen yöntemlerle belgelerin özgünlüğünün korunduğu tasdik edilmelidir (Duranti, 2010, s. 82).

4.4. Özet Değerlerinin Eşleşmemesi

E-belgelerin güvenilirliğinin korunmasında kullanılan yöntemlerden biri de belge ilk ortaya çıktığında elde edilen özet değerin yaşam döngüsü boyunca muhafaza edilmesidir. Ancak, depolama ortamlarının güncellenmesi ve kullanılan işletim sisteminin değiştirilmesi gibi nedenlerle belgenin özet değerleri farklılaşmakta ya da birbirleriyle eşleşememektedir (Hasan, Winslett, Mitra, Hsu ve Sion, 2008, s. 366). Bunun neticesinde belgenin tahrif edilmiş olabileceği düşünülebilir. E-belgelerin güvenilirliği konusunda çalışmaları bulunan Corinne Rogers, teknolojik göç işlemleri sırasında e-belgenin oluşturulan özet değerleri korunursa sorunun hafifletilebileceğini dile getirmektedir (Rogers, 2015, s. 161). Bununla birlikte, özet değeri oluşturulurken satır satır özet değeri (piecewise hashing) oluşturmanın daha sağlıklı sonuçlar verebileceği ifade edilmektedir (Garnett, Winter ve Simpson, 2018).

SONUÇ VE ÖNERİLER

Arşivlenen e-belgelerin güvenilirliğini tehdit edebilecek teknolojik kaynaklı pek çok risk mevcuttur. Bu çalışmada söz konusu risklerden belgedeki bit akışının bozulması, belge ile bileşenleri arasındaki ilişkinin kopması, e-belgenin muhafaza koşullarının sağlanamaması ve özet değerlerinin eşleşememesi riskleri incelenmiştir. Çalışmada bu risklere yol açan hususların açıklanmasına gayret edilmiştir. Bununla birlikte, kurumların söz konusu risklere karşı alabileceği önlemler açıklanmıştır. Kurumlar bu riskleri yeteri kadar dikkate almazsa söz konusu riskler birer tehdide dönüşerek e-belgelerin güvenilirliğinden şüphe duyulmasına neden olabilir. Bunun neticesinde kurumlardaki fonksiyonlar doğru açıklanamadığı gibi işlemlerin

nasıl yürütüldüğüne ilişkin deliller de yeteri kadar ortaya konulamayabilir. Kurumların bu risklere karşı alabileceği çözüm önerileri ise şöyle belirtilebilir:

Teknolojik koşullardan kaynaklı olarak arşivlenen e-belgelerin güvenilirliğini tehdit edebilecek risklerin başında belgelerin bit akışının bozulması gelmektedir. Bu riskin soruna dönüşmemesi için kurumlar depolama donanımlarını güncellemeli, belgelerin özet değerlerini belirli aralıklarla kontrol etmeli ve belgeleri hata düzeltme kodlarıyla birlikte saklamalıdır. Kurumların karşılaşabileceği bir diğer risk de belge ile bileşenleri arasındaki ilişkinin kopmasıdır. Kurumlar bu riske karşılık DROID ve JHOVE gibi format tanımlayıcıları kullanmalı ve belge ile bileşenlerine tekbiçim tanımlayıcılar atamalıdır.

E-belgelerin güvenilirliğini tehdit edebilecek bir diğer risk de gerekli muhafaza koşullarının sağlanamamasıdır. Buna karşılık kurumlar günümüz koşullarında RAID 10 gibi saklamada başarılı olduğu kabul edilen yöntemlere sahip saklama cihazlar kullanılmalı, yeni cihazlara periyodik olarak belge aktarımı yapılmalı, yazılımlar periyodik olarak güncellenmeli, belge bileşenleri kayıt altına alınıp tanımlanmalı ve bir kılavuz oluşturulmalıdır. Bu kılavuzda ihtiyaç duyulan personel deneyim ve yeteneği ile malzemelerin kullanım ömrü gibi hususlar belirtilmeli; belge formatı, kullanılacak cihazlar, teknolojik göç planları gibi belgenin erişim ve saklamasını etkileyen hususlar ifade edilmelidir. Bununla birlikte, söz konusu kılavuzda belgelerin üretilme koşulları ve onu meydana getiren bileşenler, belge ile üstveri dosyasının tek biçim tanımlayıcıları, belgenin bütünlüğü ve tamlığının kontrol edilmesi ile log kayıtlarında yer alacak hususlarla benimsenecek güvenlik önlemleri açıklanmalıdır.

Bunların yanı sıra karşılaşılabilecek bir diğer risk, özet değerlerinin eşleşmemesidir. Kurumlar bu riskin bir soruna dönüşmemesi için özet değerlerini satır satır (piecewise hashing) oluşturabilir. Aynı zamanda bu işlemler sırasında belgenin içeriğiyle birlikte konteksti de muhafaza edilmelidir. Durum böyle olunca, belgenin diplomatik özellikleri ile arşivsel bağının korunması gerekir. Bunun için önceden tanımlanmış standart form ve şablonlar oluşturulmalı, belge türü ve fonksiyona göre çeşitlenen yöntemlerle belgelerin özgünlüğü tasdik edilmelidir. Özgünlüğün tasdik edilmesi, insan müdahalesine gerek duymadan otonom bir şekilde gerçekleştirilmelidir.

Bu yöntemlerle birlikte, log kayıtları da oluşturulmalıdır. Log kayıtları belgenin yaşam döngüsünde geçirdiği aşamaların dokümantasyonu olarak kullanılabilir. Bu amaçla değerlendirilecek log kayıtlarında belgede yapılan işlemin kim tarafından gerçekleştirildiği, gerçekleşme tarihi, döngüsel artıklık denetimi ve özet değerlerinin karşılaştırılması gibi üstveriler yer almalıdır. Böylece, yapılan işlemlerin daha önceden belirlenen prosedürler dâhilinde yürütülüp yürütülmediği incelenebilir ve kalite kontrolü yapılabilir.

Görüldüğü üzere arşivlenen e-belgelerin güvenilirliğini tehdit eden risklere karşı alınabilecek çözüm önerileri oldukça çeşitlidir. İngiltere ve ABD gibi ülkelerde olduğu gibi Devlet Arşivleri Başkanlığının söz konusu riskler hakkında bir rehber hazırlayarak kurumları yönlendirmesi oldukça önemli bir kazanım olarak değerlendirilmektedir. Bunların yanı sıra kurumlardaki belge yöneticisi ve arşivciler, bahsedilen risklere karşı çözüm önerileri geliştirmek için yetkinliklerini artırmalıdır.

Teşekkür: Makalenin son okumasını yaparak görüşleriyle beni yönlendiren tez danışmanım Prof. Dr. Niyazi ÇiÇEK'e teşekkür ederim.

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.
Finansal Destek: Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The author has no conflict of interest to declare.
Grant Support: The author declared that this study has received no financial support.

Kaynakça/References

Ataman, B. K. (2005). Elektronik ortamdaki bilginin arşivlenmesi. M. E. Küçük (Ed.), *Prof. Dr. Nilüfer Tuncer'e Armağan* (ss. 78-100) içinde. Ankara: Türk Kütüphaneciler Derneği.

Aydın, C. ve Özdemirci, F. (2011). Elektronik belgelerin arşivlenmesinde gerçekliğin ve bütünlüğün korunması. *Bilgi Dünyası*, *12*(1), 105-127. https://bd.org.tr/index.php/bd/article/view/224/220 adresinden erişildi.

Bearman, D. (2006). Moments of risk: Identifying threats to electronic records. *Archivaria*, 62, 15-46. https://archivaria.ca/index.php/archivaria/article/view/12912/14148 adresinden erişildi.

Bushey, J. (2016). *The archival trustworthiness of digital photographs in social media platforms* (Doctoral thesis). Retrieved from: https://dx.doi.org/10.14288/1.0300440

Cook, T. (2013). Evidence, memory, identity and community: Four shifting archival paradigms. *Archival Science*, *13*(2-3), 95-120. https://doi.org/10.1007/s10502-012-9180-7

Creswell, J. W. (2016). *Nitel araştırma yöntemleri: Beş yaklaşıma göre nitel araştırma ve araştırma deseni* (3. bs.). (M. Bütün ve S. B. Demir Ed.) (O. Birgin, S. Ünal, T. Özsevgeç, Y. Dede, A. Bacanak, A. Bakla, … S. B. Demir, Çev.). Ankara: Siyasal Kitabevi. (Orijinali 2009'da yayımlanmıştır).

Çakmak, T. ve Eroğlu, Ş. (2016). Enterprise information systems within the context of information security: A risk assessment for a health organization in Turkey. *Procedia Computer Science*, 100, 979-986. https://doi.org/10.1016/j.procs.2016.09.262

Çakmak, T. ve Eroğlu, Ş. (2020). Elektronik Arşivlerde dijital koruma ve bilgi güvenliği risk değerlendirmesi. A. H. Kuzucuoğlu ve Y. Şeşen (Ed.), *Bilgi Merkezlerinde Risk ve Kriz Yönetimi kitabı* içinde (ss. 51-78). Ankara: Hiperlink Yayınları.

Çiçek, N. (2009). *Modern belgelerin diplomatiği*. İstanbul: Derlem Yayınları.

Çiçek, N. (2011). Elektronik belgelerin diplomatik analizi ve arşivsel bağın kurulmasındaki önemi: Türkiye'deki uygulamalar ışığında bir inceleme. *Bilgi Dünyası*, *12*(1), 87-104. https://bd.org.tr/index.php/bd/article/view/223/219 adresinden erişildi.

Çiçek, N. (2015). *Kurumsal bilgi ve belge yönetimi*. İstanbul: Marmara Belediyeler Birliği.

Çiçek, N. (2021). Türkiye'de elektronik belgelerin geleceği için ulusal strateji ihtiyacı: Literatür ışığında bir inceleme. *Bilgi ve Belge Araştırmaları Dergisi*, 15, 33-57. https://dergipark.org.tr/tr/download/article-file/1749908 adresinden erişildi.

Çiçek, N. ve Sağlık, Ö. (2019). Blokzincir teknolojisinin elektronik belgelerin güvenilirliğinin korunmasında başarıya katkısı. B. Yalçınkaya, M. A. Ünal, B. Yılmaz ve F. Özdemirci (Ed.), *Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ* (ss. 141-170) içinde. Ankara: Ankara Üniversitesi.

Digital Preservation Coalition. (2021). *Rapid assessment model* [Web Page]. Retrieved from https://www.dpconline.org/digipres/dpc-ram

Duranti, L. (2010). Concepts and principles for the management of electronic records, or records management theory is archival diplomatics. *Records Management Journal*, *20*(1), 78-95. https://doi.org/10.1108/EUM0000000007248

Duranti, L, ve Thibodeau, K. (2006). The concept of record in interactive, experiential and dynamic environments: The view of Interpares. *Archival Science,* 6, 13-68. http://doi.org/10.1007/s10502-006-9021-7

Duranti, L, ve Rogers, C. (2011). Educating for trust. *Archival Science, 11*(3-4),373-390. http://doi.org/10.1007/s10502-011-9152-3

Erickson, C.L. ve Lunt, B.M. (2015). Alternatives for long-term storage of digital information. In C. Lee, J. Crabtree, L. Konstantelos, N. McGovern, Y. Maeda, M. Pennock, …., E.Zireau (Eds.), *12. International Conference on Digital Preservation* (pp. 231-232). North Carolina [ABD]: School of Information and Library Science University of North Carolina at Chapel Hill. Retrieved from http://phaidra.univie.ac.at/view/o:429524

Garnett, A., Winter M. ve Simpson, J, (2018). Checksums on modern filesystemb, or: On the virtuous consumption of CPU cycles. In M. Potterbusch, N. McGovern, A. Whiteside, C. Mumma, E. Verbruggen, J. Meyerson, …., T. Patterson (Eds.), *15. International Conference on Digital Preservation*. Boston [ABD]: y.y. Retrived from http://osf.io/cxahf

Glassford, S. (2018). Black hole or brave new world? Archivists, historians and the challenges of the digital age. *Emerging Library & Information Perspectives*, *1*(1), 91-110. https://doi.org/10.5206/elip.v1i1.357

Guo, W., Fang, Y. Pan, W. ve Li, D. (2016). Archives as a trusted third party in maintaining and preserving digital records in the cloud environment. *Records Management Journal*, *26*(2), 170-184. https://doi.org/10.1108/RMJ-07-2015-0028

Han, Y. ve Chan, C.P. (2008). The modeling system reliability for digital preservation: Model modification and four-copy model study. In *5. Intirnational Conference on Preservation of Digital Objects: Joined UP and Working: Tools and Methods for Digital Preservation* (p. 281). London: The British Library, Retrieved from http://phaidra.univie.ac.at/detail_object/o:294190

Hasan, R., Winslett, M., Mitra, S., Hsu, W. ve Sion, R. (2008). Trustworthy records retention. In M. Gertz ve S. Jajodia (Eds.), *Handbook of Database Security* (pp. 357-381). New York [ABD]: Springer.

Hay-Gibson, N. (2011). *Risk and records management: ınvestigating risk and risk management in the context of records and information management in the electronic environment* (Doctoral Thesis). Retrieved from: https://nrl.northumbria.ac.uk/id/eprint/3308/2/hay-gibson.naomi_phd.pdf

International Organization of Standardization (ISO). (2005). *18492 Long-term preservation of electronic document-based ınformation*. Cenevre [İsviçre]: Author.

ISO. (2012). *14721 Open archival ınformation system (OAIS)*. Cenevre [İsviçre]: Author.

ISO. (2012). *16363 Audit and certification of trustworthy digital repositories*. Cenevre [İsviçre]: Author.

ISO. (2015). *27040 Security techniques: Storage security*. Cenevre [İsviçre]: Author.

INTERPARES. (2008). *INTERPARES 2: Experiential, interactive and dynamic records*. L. Duranti ve R. Preston (Eds.), Retrieved from http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf

INTERPARES. (2021). Terminology [Web Page]. Retrieved from https://interparestrust.org/terminology/term/trustworthiness

KAMU Sertifikasyon Merkezi. (2015). *Elektronik belgeleri açık anahtar altyapısı kullanarak güvenli işleme rehberi*, Sürüm 1.4. http://kamusm.bilgem.tubitak.gov.tr/dosyalar/rehberler/REHB-001.001_1.4.pdf adresinden erişildi.

Kirschenbaum, M. G., Ovenden, R. ve Redwine, G. (2010). *Digital forensics and born-digital content in cultural heritage collections*. Washington [ABD]: Council on Library and Information Resources.

Külcü, Ö., Çakmak, T. ve Özel, N. (2015). *Kamusal bilgi ve elektronik belge yönetimi: organizasyonlar ve üniversitelere yönelik koşulların analizi*. Ankara: Türk Kütüphaneciler Derneği.

Lemieux, V. L. ve Krumwied, E. D. (2011). Managing records risks in global financial ınstitutions. In L. Coleman, V. L. Lemieux, Stone, R. & Yeo, G. (Eds.), *Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk* (pp. 91-105). London [Birleşik Krallık]: Facet Publishing.

MacNeil, H. (2000). *Trusting records: Legal, historical and diplomatic perspectives*. y. y.: Springer.

McHugh, A., Ross, S., Ruusalep R. ve Hofman, H. (2007). *Digital Repository Audit Method Based on Risk Assessment*. Glasgow [İskoçya]: DCC.

Meehan, J. (2006). Towards an archival concept of evidence. *Archivaria*, 61, 127-146. Retrieved from https://archivaria.ca/index.php/archivaria/article/view/12538/13681

Minnesota Historical Society State Archives Department. (2002). *Trustworthy information systems handbook*. Minnesota [Amerika Birleşik Devletleri]: Author.

National Archives and Records Administration. (2010). Risk management plan**.** Washington [Amerika Birleşik Devletleri]: Author.

Niu, J. (2015). Original order in the digital world. *Archives and Manuscripts*, *43*(1), 61-72. https://doi.org/10.1080/01576895.2014.958863

Rogers, C. (2015). *Virtual authenticity: Authenticity of digital records from theory to practice* (Doctoral thesis) Retrieved from: https://dx.doi.org/10.14288/1.0166169.

Rosenthal, D. S., Robertson, T., Lipkins, T., Reich, V. ve Morabito S. (2005). Requirements for digital preservation systems: A bottom-up approach. *D-Lib Magazine*, *11*(1). Retrieved from http://www.dlib.org/dlib/november05/rosenthal/11rosenthal.html

Rosenthal, D.S. (2008). Bit preservation: A Solved problem?. In *5. Intirnational Conference on Preservation of Digital Objects: Joined UP and Working: Tools and Methods for Digital Preservation* (p. 277-279). London: The British Library, Retrieved from http://phaidra.univie.ac.at/detail_object/o:294190

The National Archives (TNA). (2017). *Risk assessment handbook*. Retrieved from https://www.nationalarchives.gov.uk/documents/information-management/risk-assessment-handbook.pdf

TNA. (2017a). *Migrating information between records management systems*. Retrieved from https://nationalarchives.gov.uk/documents/information-management/edrms.pdf

TNA. (2017b). *Managing digital contuinity*. Retrieved from https://nationalarchives.gov.uk/documents/information-management/managing-digital-continuity.pdf

TNA. (2017c). *Mapping the technical dependencies of information assets*. Retrieved from https://www.nationalarchives.gov.uk/documents/information-management/mapping-technical-dependencies.pdf

TNA. (2021). *The digital archiving graphical risk assessment model*. Retrieved from https://nationalarchives.shinyapps.io/DiAGRAM/

The National Electronic Commerce Coordinating Council. (2002). *Creating and maintaining proper systems for electronic record keeping*. Retrieved from http://www.pearcemoses.info/papers/creating_systems.pdf

Thibodeau, K. (2013). The perfect archival storm: The transfer of electronic records from the G. W. Bush White House to the National Archives of United States. In L. Duranti & E. Shaffer (Eds.), *The Memory of the World in the Digital Age: Digitization and Preservation* (pp. 724-733). Vancouver Kanada]: United Nations Educational, Scientific and Cultural Organization.

Yalçınkaya, B. (2014). Belge yönetim sistemlerinde ve süreçlerinde risk tanımları. *Arşiv Dünyası*, 16-17, 16-24.

Yalçınkaya, B. (2016). Elektronik belge yönetimi uygulamalarında başarıyı olumsuz etkileyen risk unsurları. *Bilgi ve Belge Araştırmaları*, 4, 20-40.

Yıldız, Ö. R. (2010). Elektronik belge yönetim sistemleri ve denetim. *Sayıştay Dergisi*, 78, 3-30.

Young, L.J. (2020). Data reawakening: The “File Not Found” series: Past 3 of 3. Retrieved from http://apps.sciencefriday.com/data/reawakening.html