Elektronik Belgelerin Arşivsel Güvenilirliğinin Başarıyla Korunmasında Üstverilerin Rolü

The Role of the Metadata in the Successfull Preservation of the Archival Trustworthiness of Electronic Records

Özhan Sağlık[1]

GİRİŞ

Elektronik devlet (e-devlet) uygulamalarının yaygınlaşmasıyla birlikte kurumlar faaliyetlerini elektronik ortama taşımış ve elektronik belge (e-belge) üretmeye başlamıştır. Üretilen bu belgeler kurumsal fonksiyonların nasıl gerçekleştiğini yansıttıklarından delil değerine sahiptir. Söz konusu değerin sürdürülebilmesi için belgelerin özniteliklerinin zaman içerisinde korunması gerekir. Bu öznitelikler, elektronik belge yönetim sistemlerinde (EBYS) üstverilerle kayıt altına alınırlar. Bu üstverilere belgenin düzenleyeni, sorumlusu ve arşivsel bağ örnek verilebilir. Hâliyle özniteliklerin korunmasında üstveriler oldukça önemlidir.

Delil değerinin sürdürülebilmesinde üstverileri kritik eden arşivsel güvenilirlik yaklaşımından yararlanıldığı bilinmektedir. Arşivsel güvenilirlik, belgelerin üretiminden imhasına kadar geçen süreçte özniteliklerinin nasıl korunabileceğini inceler. Durum böyle olunca delil değerinin arşivsel güvenilirliğin korunmasıyla sürdürülebileceği söylenebilir. Ancak Türkiye'de bunun için hangi üstverilerden yararlanılabileceği henüz yeteri kadar incelenmemiştir. Bundan dolayı çalışmanın sorusu "*e-belgelerin arşivsel güvenilirliğinin başarıyla korunmasında üstverilerden nasıl yararlanılabilir*" şeklindedir. Çalışma, "*yeterli üstveri oluşturulmazsa güvenilirlik korunamayabilir*" probleminden hareket edilerek hazırlanmıştır. Bu problemi çözümlemek için nitel araştırma yöntemleri kullanılarak farklı kurumlardaki belge yönetimi pratiklerini incelemiş saha uzmanlarıyla görüşmeler yapılmıştır.

Araştırmada incelenen konu üstveriler olduğundan nitel araştırma türlerinden olan durum çalışması benimsenmiş, bütüncül tek durum deseni tercih edilmiştir. 9 katılımcı ile görüşme yapılmıştır. Katılımcıların görüşleri rastgele numaralandırılarak aktarılmıştır. Görüşmeler yüz yüze, e-posta ve video-konferans aracılığıyla gerçekleştirilmiştir. Elde edilen cevaplar ve yapılan alanyazını araştırması sonucunda bir güvenilirlik üstverisinin önerilebileceği görülmüştür.

Alanyazını araştırması sırasında e-belgelerde kullanılacak üstverilerle ilgili pek çok çalışmayla karşılaşılmıştır (National Archives of Australia, 2015; Rogers, 2015a; Rolan, 2017). Ancak araştırmanın odak noktası bu üstverilerin güvenilirlik için nasıl kullanılabileceği olduğundan tarama yapılırken anahtar kelime olarak Türkçe'de "*elektronik belge*", "*üstveri*", "*güven*", "*güvenilirlik*" ve "*özgünlük*" sözcükleri seçilmiştir. İngilizce'de ise "*electronic*

[1] Dr., Bursa Uludağ Üniversitesi, ozhansaglik@uludag.edu.tr. Bu çalışma, yazarın İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalında gerçekleştirilen "Elektronik Belge Yönetimi Uygulamalarındaki Koşullar Işığında E-İmzalı Belgelerin Delil Değerinin Arşivsel Güvenilirlik Açısından İncelenmesi" adlı doktora tezine dayanılarak hazırlanmıştır. Bu çalışmada, tezde kullanılmayan kaynaklardan da faydalanılmıştır.

records", "*digital records*", "*metadata*", "*trust*", "*trustworthiness*" ve "*authenticity*" kelimeleriyle arama yapılmıştır.

Çalışma dört bölümden oluşmaktadır. Birinci bölümde elektronik belgelerin güvenilirlik unsurları açıklanmıştır. İkinci bölümde saha araştırmasının yöntemi ifade edilmektedir. Üçüncü bölümde saha araştırmasında elde edilen sonuçlar yorumlanmıştır. Dördüncü ve son bölümde ise arşivsel güvenilirlik üstverisine ilişkin öneriler dile getirilmektedir. Çalışma, kurumlarda oluşan e-belgelerin güvenilirliğinin korunmasında benimsenecek üstverilerle ilgili bir farkındalık oluşturursa amacına ulaşmış kabul edilecektir.

1. ELEKTRONİK BELGELERİN GÜVENİLİRLİĞİ

Belgelerin delil değerinin sürdürülebilmesi için taşıyıcı ortam, içerik, düzenleyen, kontekst gibi özniteliklerin muhafaza edilmesi gerekir. Bu özniteliklerin korunup güvenilirliğin devamlılığıyla alakalı olarak diğer alanlara göre belgeyle daha çok ilişkisi olduğu düşünülen hukuk, diplomatik ve tarih disiplinleri farklı yaklaşımlar geliştirmişlerdir. Güvenilirliğin bu disiplinlerde farklı tanımlandığı dikkat çekmektedir. Mesela, hukuki güvenilirlik, belgenin yaşam döngüsü içerisinde onu üreten yetkilinin otorite ve garantisini gösteren hukuki delillere sahip olmasını ifade etmektedir. Bir belgenin mevzuatta yer alan özellikleri haiz olup olmadığının incelendiği hukuki güvenilirlikte, belge üretmede yetki mekanizması ve belge yönetimi süreçlerinde prosedürlerin tesis edilip edilmediği kontrol edilmektedir (Sağlık, 2021, s. 58; Çiçek, 2009, s. 212; MacNeil, 2000, s. 53-56).

Hukuki güvenilirliğin yanı sıra belgelerin delil değeri incelemesinde kullanılabilecek diğer bir yaklaşım da diplomatik güvenilirliktir. Bu yaklaşımda 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; MacNeil, 2000, 73-75, 91, 96-97, 100-102).

Diplomatik güvenilirliğin yanı sıra karşılaşılan bir diğer güvenilirlik yaklaşımı ise tarihî güvenilirliktir. Burada, belgenin içerdiği bilgilerin, yer ve olayların doğru olarak verilip verilmediği kontrol edilmektedir. Özellikle belgede geçen bilgilerin, açıklanan tarih, yer, kişi ve dönemle uyuşması gerekir (Sağlık, 2021, s. 59; Çiçek, 2009, s. 212).

Ancak, e-belgelerin delil değerinin analizinde tek başına diplomatik güvenilirlik 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; International Research on Permanent Authentic Records [INTERPARES], 2008; Bushey, 2016). Diğer güvenilirlik anlayışlarında olduğu gibi arşivsel güvenilirlikte de delil değeri unsurlarından olan özgünlük, tamlık ve gerçeklik kritik edilmektedir (INTERPARES, 2008, s. 335, 816; Sağlık, 2021, s. 59). Ancak burada arşivcilik ve belge yönetimi, hukuk ve bilgisayar biliminin yaklaşımlarından yararlanarak belgelerin özgünlüğü, tamlığı ve gerçekliğinin korunması hedeflenir.

Belgenin özniteliklerinin üretildikten sonra işlem gördüğü ve dosyalanıp arşivlendiği dönem içerisinde değişmemesi olarak açıklanan özgünlük, tanımlanabilirlik ve bütünlük olmak üzere iki adımda incelenmektedir. Tanımlama, belgenin türüne göre karakteristik özelliklerini belirtmektir. Bu özellikler, belgenin diğer türlerden ayrılmasını sağlar. 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; Rogers, 2015, s. 26; Çiçek ve Sağlık, 2019, s. 150-151).

Bütünlüğün yanı sıra bir diğer güvenilirlik unsuru tamlıktır. Tamlık arz eden bir belgede kesin, doğru, hakikate uygun ve tahrifattan uzak olmak özellikleri aranmaktadır. Buna göre, tamlık, hukuki sonuç meydana getirebilmek için belgenin üreticisi ve idari-hukuki sistem tarafından ihtiyaç duyulan tüm elemanların varlığını ifade etmektedir. Çünkü belge, üretilme gerekçesi olan hukuki prosedüre ve görmesi gereken idari işlem türüne göre belge vasfı kazanmaktadır (Sağlık, 2021, s. 61; 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, 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).

Arşivsel güvenilirlik anlayışı benimsenerek e-belgelerin özgünlüğü, tamlığı ve gerçekliğinin nasıl korunabileceği incelenirken üstveriler oldukça önemlidir. Çünkü EBYS'lerde belgelerin öznitelikleri üstverilerle kayıt altına alınır. Durum böyle olunca, üstveriler e-belgelerin arşivsel güvenilirliğinin korunmasında incelenmesi gereken hususların başında gelmektedir. Güvenilirliği korumak için hangi üstverilerden yararlanılabileceği düşüncesiyle bir saha araştırması yapılmış ve uzmanların görüşlerinin alınmasına karar verilmiştir.

2. YÖNTEM

Bu çalışmada e-belgelerin güvenilirliğinin korunması problemine saha uzmanlarının atfettiği anlamları keşfetme ve anlamaya yönelik bir yaklaşım olması nedeniyle nitel araştırma yöntemleri kullanılmaktadır. Özelden genel temalara ulaşan tümevarımsal veri analizi yapılarak saha uzmanlarından elde edilen veriler yorumlanmıştır. Nitel araştırmalarda çalışmanın sorusu, deseni, örneklem, veri toplama teknikleri, verilerin analiz yöntemleri, araştırmacının rolü ve geçerlilik ile güvenirliğe ilişkin hususların belirtilmesi beklenmektedir.

Çalışmanın sorusu, "*e-belgelerin arşivsel güvenilirliğinin başarıyla korunmasında üstverilerden nasıl yararlanılabilir*" şeklindedir. Araştırma deseni olarak durum çalışması benimsenmiştir. Bu çalışmada üstverilerin güvenilirliğe etkisi incelendiğinden bütüncül tek durum deseni tercih edilmiştir. Örneklem ise Türkiye'de farklı kurumlardaki e-belge yönetimi

uygulamalarını incelemiş veya tatbik etmiş 9 saha uzmanından oluşmaktadır[2]. Katılımcıların görüşleri rastgele numaralandırılarak aktarılmıştır. Veri toplama tekniği olarak yüz yüze, e-posta ve video-konferans görüşmeleri yapılmıştır[3].

Bu görüşmelerin analizi için elde edilen veriler kod, kategori ve temalar altında bir araya getirilmiştir. Kodlama, verilerin etiketlenerek küçük bilgi kategorileri içinde toplanmasını ifade etmektedir (Creswell, 2016, s. 184-186). Tüm veriler değil, üstverilerle ilgili olduğu düşünülenler bir etiket hâline getirilip, kodlanmış ve Şekil 1'de gösterilmiştir. Çalışmada elde edilen cevaplar kodları, üstveri kategoriyi, güvenilirlik ise temayı oluşturmaktadır. Cevapların belirlenen temayla ilişkisinin kurulabilmesi için bu ilişkiyi kurmada sık kullanılan yazılımlardan biri olan MAXQDA tercih edilmiştir. Bu tercihin nedeni, söz konusu yazılımın nitel verileri kodlama aracılığıyla kategori ve temalarla ilişkilendirmede sağladığı yetkinliklerdir.

Nitel araştırmalarda araştırmacının rolü ve arka planının açıklanması beklenmektedir. Araştırmacı, lisans, yüksek lisans ve doktora eğitimini bilgi ve belge yönetimi alanında tamamlamıştır. Lisans döneminden itibaren çeşitli arşiv kurma ve e-belge yönetimi geliştirme çalışmalarında yer almıştır. İstanbul Üniversitesi ve Bursa Uludağ Üniversitesinde sayısallaştırma projeleri yürütmüştür. Bursa Uludağ Üniversitesinin senato ve yönetim kurulu kararlarının elektronik ortama aktarılması sürecinde arşiv yazılımının geliştirilmesi konusunda çalışmıştır. Araştırmacı, hem çalıştığı hem de sahada incelediği kurumlarda e-belge yönetimi sürecinin yeteri kadar başarılı yürütülemediğini, belgelerin arşivlenmesinden ziyade üretilip yığın oluşturulması şeklinde bir eğilimin mevcut olduğunu gözlemlemiştir. Ona göre bu eğilimin bir nedeni de yeteri kadar üstveri kullanılmamasıdır. Bu olumsuz durum neticesinde e-belgelerin güvenilirliği yeteri kadar korunamayabilir. Durum böyle olunca bu gözlemler saha araştırmasının yapılmasını gündeme getirmiştir. Fakat araştırmacı kendi gözlemlerinin bir sınırlılık arz ettiğini ve sorunu çözümlemek için yeterli nitelikte olmadığını düşünmektedir. Bu nedenle nitel araştırma örneklemi, kamudaki farklı belge yönetimi uygulamalarını incelemiş veya tatbik etmiş kişilerden seçilmiştir. 9 kişi ile görüşme yapılmıştır. Yapılan mülakatlar sadece sorular çerçevesinde gerçekleştirilmiş, katılımcıların belirli bir tarafa yönlendirilmemesine çalışılmıştır (Sağlık, 2021, s. 210).

Nitel araştırmalarda elde edilen verilerin alanyazınında daha sağlıklı bir zeminde konumlandırılabilmesi için geçerliliğinin tartışılmasına ihtiyaç duyulmaktadır. Bunun yöntemlerinden biri bulguların doğru olup olmadığının incelenmesi ve akran değerlendirmesidir (Creswell, 2017; s. 191, 201-203). Çalışmada elde edilen bulgular alanyazınındaki yerleri belirtilerek metne aktarılmıştır. Kullanılan bir diğer geçerlik yöntemi olan akran değerlendirmesinde ise araştırmacı dışında başka bir kişi, konu hakkında soru sormuş ve inceleme yapmıştır. Bu noktada, araştırmacının tez dönemi süresince altı ayda bir toplanan tez izleme kurulunun görüşleri dikkate alınmıştır.

---

2 Yazarın "Elektronik Belge Yönetimi Uygulamalarındaki Koşullar Işığında E-imzalı Belgelerin Delil Değerinin Arşivsel Güvenilirlik Açısından İncelenmesi" başlıklı doktora tezi çalışması kapsamında yapılan bu araştırmanın etik kurul onayı, İstanbul Üniversitesi Rektörlüğü, Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu Başkanlığının 10.07.2020 tarih ve 08 sayılı toplantısında 2020/16 sayılı karar no ile alınmıştır.

3 Katılımcıların görüşlerine http://acikerisim.istanbul.edu.tr/handle/20.500.12627/167875 adresindeki "Nitel_Araştırma_Verileri.pdf" adlı dosyadan erişilebilir.

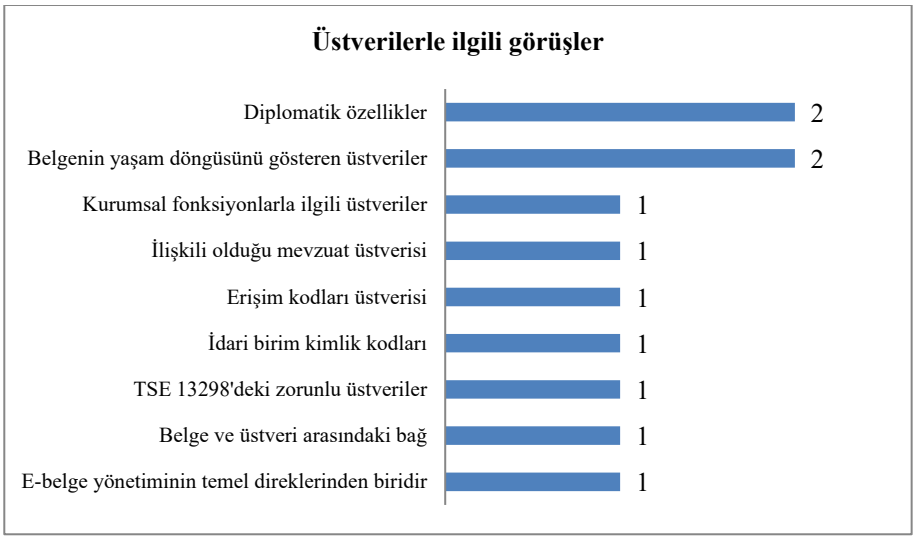
Nitel araştırmalarda elde edilen verilerin tartışılması sırasında uygulanan bir diğer safha güvenirliktir. Bu safhada farklı araştırmacılar tarafından geliştirilen kodların çapraz kontrolünün yapılması önerilmektedir (Creswell, 2017; s. 191, 203). Güvenirliği sağlamak için Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümünde araştırmanın temas ettiği konular hakkında çalışmaları bulunan araştırma görevlileri ve doktora öğrencilerinin görüşlerinden faydalanılmıştır. Dr. Varol Saydam, Emin Gedikli ve Oytun Cibaroğlu'na nitel veriler gönderilmiştir. Yaptıkları kodlamalarla araştırmacınınki kontrol edilmiştir.

3. SAHA ARAŞTIRMASI

Özgünlük, gerçeklik ve tamlık gibi güvenilirlik unsurları, aynı zamanda hukuk düzeninin belgede aradığı delil değeri kriterlerindendir (Duranti ve Rogers, 2012; Sağlık ve Çiçek, 2020). Söz konusu güvenilirlik unsurları korunduğu takdirde belgenin delil değerinin sürdürülebileceği söylenebilir (Sağlık, 2021). Bu unsurlar, EBYS'lerde üstverilerle kayıt altına alındığından üstveriler oldukça kritiktir. Saha uzmanları da "e-belgelerin delil değerinin korunmasında üstverilerin nasıl rol oynayacağı" sorusuna bu yönde görüş bildirmektedir. Bu görüşler şöyle açıklanabilir (Sağlık, 2021, s. 221-222):

"NİT09, "*üstverilerin e-belgelerin delil değerinin ortaya çıkarılmasında en kritik nokta*" olduğunu ifade ederek "*belgenin içeriğiyle birlikte kontekstini de açığa çıkardığını*" belirtmiştir. Üstverileri, "*e-belge yönetiminin temel direklerinden biri*" olarak değerlendirmektedir. Ayrıca, "*çok fazla sayıda üstveri oluşturmanın belge üretimindeki teknik süreçleri artıracağını ve fazla zaman harcanması nedeniyle insanların bir süre sonra bunları üretmeyebileceğini, çok az sayıda üretilirse de farklı sorunların ortaya çıkacağını*" dile getirmektedir. NİT01, "*belgenin diplomatik özelliklerinin*", NİT02 ise "*belgedeki açıklamaların bir üstveri olarak kurgulanabileceğini*" önermektedir. NİT02 aynı zamanda, "*olmazsa olmaz üstverilerin belirlenmesini*", "*belgenin hangi mevzuat kapsamında saklandığını gösteren bir üstveri alanının bulunmasını*" ve "*kurumsal iş ve fonksiyonlarla ilgili üstverilerin olması gerektiğine*" vurgu yapmıştır. NİT05, "*belgeyi oluşturan kurumun erişim kodlarını saklaması gerektiğini ifade ederek bu kodların üstverilerde yer aldığını*" dile getirmiştir. Aynı zamanda "*idari birim kimlik kodlarını ihtiva eden üstverilerin iyi bir şekilde saklanması gerektiğini*" ifade etmektedir".

"NİT03 ve NİT09, belgenin yaşam döngüsünü gösteren üstverilerin önemine dikkat çekmektedir. NİT03, "*üstverilerin belgenin oluşumundan nihai tasfiyesine kadar geçen süreçte belgelerin bütünsel gerçekliği açısından önemli verileri içerdiğini*" beyan etmiştir. NİT09, "*yaşam döngüsü ve belge süreklilik modelleriyle üstverilerin eşleştirilerek belgenin üretimi, yönetimi ve saklanması noktasında herhangi bir karanlık noktanın kalmamasını*" önermektedir. Bununla birlikte, NİT07, "*belge ve üstveri arasındaki bağın korunması gerektiğini*" ifade etmektedir. NİT06, "*belgenin görsel formunda yazılı olan bilgiler dışında birçok bilginin üstverilerde saklanabileceğini*" belirtmiş, "*e-imza ile korunmuş bir belgenin tüm üstverilerin de belgeyle birlikte korunabilmesi anlamına geldiğini*" dile getirmiştir. NİT08 ise "*TS 13298'deki üstverilerin yeterli olduğunu*" ileri sürmüştür" (INTERPARES, 2008; Yalçınkaya, 2014). Verilen cevaplar neticesinde aşağıdaki gibi bir grafik oluşturulabilir.



Şekil 1. Üstverilerle İlgili Görüşler

Üstverilerle ilgili katılımcılara yönetilen sorular neticesinde NİT02, NİT05, NİT07 ve NİT09 "*üstverilerin*" bir güvenilirlik mekanizması olarak ele alınabileceğini belirtmiştir (INTERPARES, 2008; Yalçınkaya, 2014). Durum böyle olunca, bir güvenilirlik üstverisinin önerilebileceği düşünülmüştür.

4. GÜVENİLİRLİK ÜSTVERİSİ

Sorumludan imzalayana tarihten belgenin amacı ve konusuna kadar başlıca tanımlama bilgileri olan üstveriler, belge, onu oluşturan işlem ve üreticisi arasındaki ilişkiyi yansıttığından özgünlüğün temel yapı taşlarından biridir. Belgeyle onu üreten ve kullanan birimler arasındaki ilişkiyi gösteren üstverilerin doğru oluşturulması, belgenin anlaşılabilirliğini sağlayarak güvenilirliğini artırır (Sağlık, 2021; s. 72; ISO, 2009, s. 3-4; ISO, 2017, s. 2-3).

E-belgelerin özgünlük, gerçeklik ve tamlık gibi özniteliklerinin zaman içerisinde bozulup değişmeden korunması böylece güvenilirliğin devam ettirilmesi için belgenin düzenleyeni, sorumlusu ve arşivsel bağı gibi üstveri araçları kullanılmaktadır (Sağlık, 2021, s. 158; Rogers, 2015a, s. 12; INTERPARES, 2008, s. 277). Kanada, Norveç, Malezya, Almanya, Litvanya, İtalya, Hindistan, Çin, Botsvana ve İsviçre gibi farklı ülkelerdeki çalışmalar incelendiğinde güvenilirlikle ilgili olarak bu üstverilerden yararlanılabileceği anlaşılmaktadır. Bunlar şöyle açıklanabilir (Sağlık, 2021, s. 158-161):

"Kanada merkezli INTERPARES çalışmaları kapsamında geliştirilen koruma zincirinde (preservation chain) üstveriler, belgelerin güncel, yarı güncel ve arşivdeki işlemleriyle alakalı olarak üç döneme ayrılarak ele alınmıştır (INTERPARES, 2008, s. 200-205). Belgelerin güncel döneminde kullanılabilecek üstveriler, form özellikleri, format, belgenin sayısı, konusu, dosya kodu ve saklama süresi, ekleri, belgedeki kişiler (sorumlu, düzenleyen, muhatap, oluşturan) ile imza, onaylama ve doğrulama gibi diğer tasdik araçları olarak belirtilmektedir. Yarı güncel dönemde ise belge yöneticisinin dosyalamayı onayladığı tarih, varsa eklediği dosya kodu gibi tanımlayıcı bilgiler, belge bileşenlerinin saklandığı konumlar,

meydana gelen teknolojik değişimler, açıklama notları, belgenin yarı güncel olup birim arşivine devir zamanı ve devri onaylayıp gerçekleştirenler üstveri olarak kullanılabilmektedir (INTERPARES, 2008, s. 209-211). Belge arşivlendikten sonra ise bu üstverilerle birlikte format, e-imza ve zaman damgası sertifikalarının güncellenmesi gibi hususlara yönelik üstverilerden yararlanılabildiği görülmektedir. Eski ve yeni dosya formatı, formatın ve imza sertifikalarının güncellenmesinin nedeni, bu değişikliklerden sonra güvenilirliğin kim tarafından onaylandığı gibi üstveriler benimsenebilmektedir (INTERPARES, 2008, s. 213)".

Güvenilirliğin başarıyla korunmasında benimsenen yöntemlerden biri de yedeklemedir. Hâliyle, kurumlarda yedeklemeyle ilgili üstveriler de oluşmaktadır. Bunlara, yedeklemenin türü, kapsamı, zamanı, referans numarası ve kim tarafından ne zaman onaylandığı gibi üstveriler örnek verilebilir (INTERPARES, 2008, s. 214-215).

Yedeklemenin yanı sıra, belgeler zaman içerisinde teknolojik eskimeye maruz kalabildiğinden teknolojik göç ettirme işlemlerinin yapılması gerekebilir. Bu işlemlerde teknolojik göçün nedeni, işlemin zamanı ve işlem referans numarası ile sorumlusu gibi üstveriler kullanılabilmektedir. Bununla birlikte, teknolojik göçten sonra belgenin form özellikleri ve özgünlüğünün korunup korunmadığı ile onaylanmasına ilişkin üstveriler benimsenebilir (INTERPARES, 2008, s. 214-215).

"Ancak, özgünlüğün korunması için sadece belgenin arşiv dönemini dikkate almak yeterli olmaz. Güncel kullanım safhasındaki süreciyle ilgili üstveriler de değerlendirilmelidir. Durum böyle olunca, bu safhada özgünlüğü onaylamak için kullanılan teknikler, özgünlüğü onaylayan kişi, özgünlük değerlendirme raporu referans numarası, özgünlüğü onaylanan belgelerin arşive devir zamanı, log kaydı gibi güncel belge döneminde yapılan dokümantasyonlar ile devir sırasında benimsenen güvenlik ve kontrol prosedürleri gibi hususlara yönelik üstverilerin kullanılabileceği anlaşılmaktadır (INTERPARES, 2008, s. 221, 226-228; Tennis, 2013, s. 935, 939)".

E-belgelerin kullanımının artmasıyla birlikte INTERPARES kapsamında geliştirilen bu üstverilere benzerlerinin çeşitli ülkelerde de kullanılmaya başlandığı görülmektedir. Belgelerin dosya ve serileriyle ilişkilendirilerek saklandığı Norveç'te müstakil olarak özgünlük üstverisinin geliştirildiği gözlenmektedir. Burada belgelerin özgünlüğü, erişim kontrolü ve bütünlüğü ayrı bir üstveri alanı olarak kurgulanmıştır (Long Term Records Management Project). Bununla birlikte, Malezya, Almanya, Litvanya, İtalya ve Hindistan gibi ülkelerde Open Archival Information System (OAIS - Açık Arşivsel Bilgi Sistemi) yapısında arşivlenen belgelerin tanımlanmasında (Bunawan vd., 2015; Stancic vd., 2015, s. 218-223) kullanılan üstverilerin güvenilirlik üstverisi olarak kullanılabileceği düşünülmektedir. Malezya'da kullanılan belgelerin referans numarası ve muhafaza sürecinde yapılan arşivcilik işlemleri gibi üstveriler bunlara örnek verilebilir (Bunawan vd., 2015, s. 29-34).

Bu örneklerle birlikte, İtalya'da uzun dönemli koruma sistemine aktarılacak hasta kayıtlarında hastanın kimlik numarası, doğum tarihi, cinsiyeti ve teşhisin yapıldığı tarih gibi üstverilerin kullanıldığı görülmektedir. Bu üstverilerle belgelerin özgünlüğünün doğrulanmasında kullanılabilecek bir özgünlük protokolü oluşturulmuştur. Bu protokolde belgenin türü ve yaşam döngüsündeki süreçler, protokolü uygulayan kişiler, protokol sonucu ortaya çıkan özgünlük doğrulama kaydı ve özgünlüğün doğrulanmasında uygulanacak adımlar yer almaktadır (Salza ve Guercio, 2012, s. 177-178).

İtalya'daki bu örnekle birlikte Hindistan Anayasa Mahkemesinde oluşan belgeler, belgenin delil değerine esas teşkil edecek bilgileri içeren, içerik ve uzun dönemli korumaya ilişkin bilgilerin mevcut olduğu arşiv bilgi paketi hâline getirilirken (International Organization for Standardization [ISO], 2012, s. 85-86) özet değeri, format, dizin ve belge sayısı gibi üstverilerin kullanıldığı görülmektedir. Ancak, Abichandani ve Prakash bu üstverilerin kullanılmasına rağmen uygulamada bir standartlaşma olmadığına dikkat çekmektedir. Bundan dolayı üstverilerin belirlenen standartlar çerçevesinde üretilmesine ve belgelerin özgünlüğünü tasdik edecek yöntemlerin tayin edilmesine duyulan ihtiyacı dile getirmektedirler (Abichandani ve Prakash, 2014, s. 220-227).

"Bu örneklerin yanı sıra, Çin'deki Beijing arşivlerinde gerçekleştirilen bir uygulama dikkat çekmektedir. Burada, belgeler özniteliklerinin korunup korunmadığı kontrol edilip, özgünlükleri doğrulanarak arşive transfer edilmektedir. Bunun için belge ve referans numarası, belgedeki kişiler, belgenin özet değeri, üstveriler ve e-imzadan oluşan kimlik bilgisi paketi, bu paketi barındıran merkezi otoriteden alınan kayıt ve belgenin kendisi olmak üzere elde edilen üç özet değer karşılaştırılmaktadır. Bu değerlerin eşleşmesinden sonra arşive transfer edilen belge sayısı otonom bir şekilde kontrol edilmektedir. Bu kontrolde de eşleşme sağlanırsa belgeler, özgünlüklerinin doğrulandığı onaylanmış bir şekilde arşive devredilmektedir (Zhang vd., 2013, s. 191-194)".

Belgelerin özgünlüklerinin doğrulanmasına yönelik bir başka öneride noter gibi bir otoriteden yararlanılabileceği ifade edilmektedir. Burada, özgünlüğün doğrulanması amacıyla e-belgelerin imzaları ve üstverileriyle birlikte bir paket hâline getirilerek bu paketin noter gibi bir otorite tarafından onaylanması önerilmektedir. Söz konusu paket, üstveri eklenmesi ya da e-imza sertifikasının yenilenmesi gibi güncellemelerde yeniden noter onayı alabilmektedir. Böylece, paketin yani belgenin özgünlüğünün doğrulanması talep edildiğinde, her zaman isteyen herkesin erişimine açılabilmektedir (Lekkas ve Gritzalis, 2007, s. 442-448).

Tüm bunlarla birlikte, Bostvana ve İsviçre'deki örnekler üzerinden yapılan çalışmalar da dikkat çekmektedir. Bostvana'daki uygulamalar özelinde elektronik ortamda oluşan muhasebe kayıtlarının arşivsel güvenilirliğine ilişkin bir çalışmada üretici ve sorumlu, muhatap, düzenleyen, arşivsel bağ, belgenin ait olduğu konu ya da vaka ile belgenin ekleri gibi üstverilerin hâlihazırda kullanıldığı gözlenmektedir (Mosweu, 2020, s. 68). Bu üstverilerin e-belgelerin güvenilirlik kriterlerinden olan tanımlanabilirlik için kullanılabileceği anlaşılmaktadır. İsviçre'de yapılan başka bir çalışmada ise e-belgelerle ilgili kullanılması önerilen özgünlük üstverilerinden format, log kayıtları ve zaman damgası ile bit sağlaması (checksum) bilgilerinin birer güvenilirlik üstverisi olarak kurgulanabileceği görülmektedir (Shabou, 2015, s. 75).

Yukarıda çeşitli çalışmalar ve ülkelerden verilen örneklerden de yararlanılarak Türkiye'de kullanılacak arşivsel güvenilirlik üstverisi alanlarının önerilmesine ihtiyaç duyulduğu düşünülmektedir. Türkiye'de Bahattin Yalçınkaya, 2014'te gerçekleştirdiği doktora tezinde e-belgelerin paylaşılması ve uzun dönemli arşivlenmesine ilişkin bir üstveri modeli geliştirmiştir. Bu nedenle modelde tabii olarak müstakil bir güvenilirlik üstverisi bulunmamaktadır. Söz konusu tezde belgelerin güvenilirliğiyle ilişkilendirilebilecek belgedeki kişiler, üretim tarihi, format, dosyalama, sayısal koruma gibi hususlar zorunlu ve seçmeli üstveriler olarak yer almaktadır (Yalçınkaya, 2014). Bununla birlikte, Gülten Alır,

2008'de gerçekleştirdiği doktora tezinde Adalet Bakanlığında oluşan e-belgeler için kullanılabilecek bir üstveri modeli önermiştir. Hâliyle bu modelde de müstakil bir güvenilirlik üstverisi kurgulanmamıştır. Ancak Bakanlık'ta oluşan e-belgeler için kullanılması önerilen belgedeki kişiler, belgenin türü, e-imza ve ekler gibi üstveriler, aynı zamanda güvenilirlik üstverisi olarak değerlendirilebilmektedir (Alır, 2008, s. 97-100).

Alanyazınında görülen bu çalışmalarda belirtilen üstveriler, kurumlarda oluşan e-belgelerin güvenilirliğiyle ilgili olarak bir çerçeve sunmaktadır. Ancak güvenilirliğin korunması için mevzuatsal bir dayanağa ihtiyaç duyulmaktadır. Böylece, politika ve prosedürleri hazırlanmış, gerekli teknik ve teknolojik altyapısı tesis edilmiş, ihtiyaç duyulan insan kaynağı istihdam edilmiş bir süreç yönetiminin uygulanması mümkün hâle gelecektir. Bu sürecin hangi niteliklerde yapılması gerektiğinin ise standartlarda açıklandığı görülmektedir. Aynı zamanda çeşitli kanun ve yönetmelikte bilgi güvenliği gibi uluslararası standartlardaki esasların uygulanabileceği ifade edilmektedir (Türk Ticaret Kanunu, 2011; Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği, 2014; Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik, 2015; Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik, 2020). Durum böyle olunca kurumlarda oluşan e-belgelerin güvenilirliğin korunması için geliştirilecek üstverilerde arşivcilik ve belge yönetimiyle ilgili uluslararası standartlardan özellikle de ISO'nun çıkarmış olduklarından yararlanmak mümkündür. Bunun yanı sıra, Türkiye'de EBYS geliştirirken esas alınması tavsiye edilen TS 13298 Elektronik Belge ve Arşiv Yönetimi Standardından da yararlanılmıştır (Elektronik Belge Standartları, 2008; Türk Standartları Enstitüsü [TSE], 2015). Ayrıca yirmi yıldan fazla bir süredir e-belgelerin güvenilirliğiyle ilgili metodolojiler geliştiren INTERPARES çıktılarından da faydalanılmıştır. İncelenen bu kaynaklarda bazı üstverilerin oldukça kritik olduğu söylenmektedir. Bu üstveriler, belgelerin güvenilirliğini korumak için yapılması gerekenler olarak değerlendirildiğinden zorunlu olarak benimsenmiştir. Güvenilirliği korumayı destekleyen ancak mevcut olmadığı takdirde ciddi bir eksiklik olarak değerlendirilemeyecekler ise seçmeli olarak kabul edilmektedir. Durum böyle olunca önerilen bazı üstveriler zorunlu, bazıları ise seçmeli olarak değerlendirilmiştir. Önerilen güvenilirlik üstverisi ve kaynakları çalışmanın ekinde sunulan tabloda belirtilmektedir.

SONUÇ

Kurumlarda oluşan e-belgeler, kurumsal fonksiyonların nasıl gerçekleştiğini yansıttıklarından delil değerine sahiptir. Bu değerin tabii olarak belgenin üretiminden imhasına kadar sürdürülmesi gerekir. Bunun için belgenin özniteliklerinin yani güvenilirliğinin korunmasına ihtiyaç duyulmaktadır. Bu öznitelikler, EBYS'lerde üstverilerle kayıt altına alındığından güvenilirliğin korunmasında üstveriler oldukça kritiktir. Bunlara belgenin düzenleyeni, sorumlusu ve arşivsel bağ örnek verilebilir. Ancak Türkiye'de güvenilirliğin korunması için hangi üstverilerden yararlanılabileceği henüz yeteri kadar incelenmediğinden bu çalışma kaleme alınmıştır.

Nitel araştırma yönteminin benimsendiği bu çalışmada, Türkiye'deki farklı belge yönetimi uygulamalarını incelemiş veya tatbik etmiş 9 saha uzmanıyla görüşme yapılmıştır. Saha uzmanlarına e-belgelerin delil değerinin korunmasında üstverilerin nasıl rol oynayacağı

sorulmuş ve üstverilerin oldukça kritik olduğu cevabı alınmıştır. Üstveriler, belge yönetiminin temel direği şeklinde ifade edilmekte; diplomatik özellikler ve belgenin üretilme gerekçesini teşkil eden mevzuatın bir üstveri olarak kurgulanabileceği dile getirilmiştir. Bununla birlikte, belgenin hangi faaliyet ve fonksiyonlar kapsamında üretildiğine dair bir üstverinin oluşturulabileceği de ifade edilmiştir. Katılımcılar, üstverilerin bir güvenilirlik mekanizması olarak değerlendirilebileceğini belirtmiştir. Durum böyle olunca, bir güvenilirlik üstverisinin geliştirilebileceği düşünülmüştür.

Güvenilirlik üstverisiyle ilgili alanyazını incelendiğinde Kanada, Norveç, Malezya, Almanya, Litvanya, İtalya, Hindistan, Çin, Botsvana ve İsviçre gibi farklı ülkelerdeki çalışmalarda güvenilirlikle ilgili olarak belgenin düzenleyeni, sorumlusu ve arşivsel bağı gibi üstverilerden yararlanılabileceği görülmektedir. Belgenin form özellikleri, formatı, sayısı, konusu, dosya kodu ve saklama süresi, ekleri ile belgedeki kişiler (sorumlu, düzenleyen, muhatap, oluşturan), imza, onaylama ve doğrulama gibi diğer tasdik araçları, belge yöneticisinin dosyalamayı onayladığı tarih, varsa eklediği dosya kodu gibi tanımlayıcı bilgiler, belge bileşenlerinin saklandığı konumlar, meydana gelen teknolojik değişimler, açıklama notları, belgenin yarı güncel olup birim arşivine devir zamanı ve devri onaylayıp gerçekleştirenler, yedekleme bilgileri ile teknolojik göç ettirme, özgünlüğün değerlendirilmesi ve e-imza ile zaman damgası sertifikalarının güncellenmesi gibi hususlara yönelik üstverilerin bu kapsamda değerlendirilebileceği anlaşılmaktadır.

Bu çalışmada, alanyazınında görülen bu üstverilerden hareketle bir arşivsel güvenilirlik üstverisinin önerilmesine çalışılmıştır. Ancak bunların sahada bir karşılığının olabilmesi için mevzuatsal bir dayanağa ihtiyaç duyulmaktadır. Çeşitli kanun ve yönetmelikte bilgi güvenliği gibi uluslararası standartlardaki esasların uygulanabileceği ifade edildiğinden bir sürecin hangi niteliklerde yapılması gerektiğinin açıklandığı standartlara başvurulabileceği düşünülmüştür. Böylece, güvenilirliğin korunmasıyla ilgili olarak politika ve prosedürleri hazırlanmış, gerekli teknik ve teknolojik altyapısı tesis edilmiş, ihtiyaç duyulan insan kaynağı istihdam edilmiş bir süreç yönetiminin uygulanması mümkün hâle gelecektir. Durum böyle olunca kurumlarda oluşan e-belgelerin güvenilirliğin korunması için geliştirilecek üstverilerde TSE ile ISO gibi ulusal ve uluslararası standartlardan, INTERPARES gibi yirmi yıldan fazla süredir metodolojiler geliştiren projelerin çıktılarından yararlanılmıştır. İncelenen bu kaynaklarda bazı üstverilerin oldukça kritik olduğu söylenmektedir. Bunlar, belgelerin güvenilirliğini korumak için yapılması gerekenler olarak değerlendirildiğinden zorunlu olarak benimsenmiştir. Güvenilirliği korumayı destekleyen ancak mevcut olmadığı takdirde ciddi bir eksiklik olarak değerlendirilemeyecekler ise seçmeli olarak kabul edilmiştir.

Çalışma, kurumlarda oluşan e-belgelerin güvenilirliğinin korunmasında benimsenecek üstverilerle ilgili bir farkındalık oluşturursa amacına ulaşmış kabul edilecektir. Bununla birlikte çalışmadan yeni araştırmalara kaynaklık etmesi beklenmektedir. Belirlenen güvenilirlik üstverisinin kurumlarda nasıl oluşturulabileceği, bu üstverilerin uzun dönemde hangi yöntemlerle korunabileceğinin incelenmesine ihtiyaç duyulmaktadır. Böylece arşivsel güvenilirliğin başarıyla korunmasına katkı sunulabilir.

KAYNAKÇA

Abichandani, P. ve Prakash, R. (2014). Digital preservation of court's disposed case records - A case study from Indian Judicial System's Perspective. D. Katre ve D. Giaretta (Yay. Haz.). *APA/C-DAC International Conference on Digital Preservation and Development Trusted Digital Repositories* içinde (ss. 220-227). Yeni Delhi[Hindistan]: yayıncı yok.

Alır, G. (2008). *E-Türkiye uygulamaları: Elektronik belge yönetimi ve üst veri*. Yayımlanmamış doktora tezi, Hacettepe Üniversitesi, Ankara.

Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik, *Resmî Gazete [R.G.]* (31069, 15 Mart 2020). 14 Şubat 2023 tarihinde https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm adresinden erişildi.

Bunawan, A. vd. (2015). Model for preserving the electronic records event history metadata in Malaysia government agencies. D. Dabass vd. (Yay. Haz.). *Seventh International Conference on Computational Intelligence, Modelling and Simulation* içinde (ss. 29-34). Yayın yeri yok: yayıncı yok.

Bushey, J. (2016). *The archival trustworthiness of digital photographs in social media platforms*. Yayımlanmamış doktora tezi, University of British Columbia, Vancouver[Kanada]. 14 Şubat 2023 tarihinde http://hdl.handle.net/2429/57606 adresinden erişildi.

Creswell, J. W. (2016). *Nitel araştırma yöntemleri: Beş yaklaşıma göre nitel araştırma ve araştırma deseni* (M. Bütün vd. Çev.). 3. bs., Ankara: Siyasal Kitabevi. (Orijinali 2013'te yayımlanmıştır).

Creswell, J. W. (2017). *Araştırma deseni: Nitel, nicel ve karma yöntem yaklaşımları* (S. B. Demir vd. Çev.). 3. bs., Ankara: Eğiten Kitap.

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

Çiçek, N. ve Sağlık, Ö. (2019). Blokzincir teknolojisinin elektronik belgelerin güvenilirliğinin korunmasında başarıya katkısı. B. Yalçınkaya (Yay. Haz.). *Bilgi yönetimi ve bilgi güvenliği: eBelge-eArşiv-eDevlet-Bulut bilişim-Büyük veri-Yapay zekâ* içinde (ss. 141-170). Ankara: Ankara Üniversitesi.

Duranti, L. ve Rogers, C. (2012). Trust in digital records: An increasingly cloudy legal area. *Computer Law & Security Review*, 28, 522-531.

Elektronik Belge Standartları. *R.G.* (26938, 16 Temmuz 2008). 14 Şubat 2023 tarihinde https://www.resmigazete.gov.tr/eskiler/2008/07/20080716-7.htm adresinden erişildi.

Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği. *R.G.* (29059, 13 Temmuz 2014). 14 Şubat 2023 tarihinde https://www.resmigazete.gov.tr/eskiler/2014/07/20140713-4.htm adresinden erişildi.

Heather, MacNeil vd. Authenticity task force report. *The long-term preservation of authentic electronic records: Findings of the INTERPARES Project* içinde. 14 Şubat 2023 tarihinde http://www.interpares.org/book/interpares_book_d_part1.pdf adresinden erişildi.

Heather, MacNeil vd. Requirements for assessing and maintaining the authenticity of electronic records. *The long-term preservation of authentic electronic records: Findings of the INTERPARES Project* içinde. 14 Şubat 2023 tarihinde http://www.interpares.org/book/interpares_book_d_part1.pdf adresinden erişildi.

INTERPARES. (2008). *INTERPARES 2: Experential, Interactive and Dynamic Records*, L. Duranti ve R. Preston (Yay. Haz.). 14 Şubat 2023 tarihinde http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf adresinden erişildi.

ISO. (2008). *26122 Work Process Analysis for Records.* Cenevre[İsviçre]: ISO.

ISO. (2009). *12033 Guidance for the Selection of Document Image Compression Methods.* Cenevre[İsviçre]: ISO.

ISO. (2012). *13008 Digital Records Conversion and Migration Process.* Cenevre[İsviçre]: ISO.

ISO. (2012). *27037 Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence.* Cenevre[İsviçre]: ISO.

ISO. (2015). *27040 Security Techniques: Storage Security*. Cenevre[İsviçre]: ISO.

ISO. (2016). *15489 Records Management Part 1: Concepts and Principles*. Cenevre[İsviçre]: ISO.

ISO. (2017). *15801 Electronically Stored Information: Recommendations for Trusworthiness and Reliability.* Cenevre[İsviçre]: ISO.

ISO. (2017). *18829 Assessing ECM/EDRM Implementations : Trustworthiness.* Cenevre[İsviçre]: ISO.

ISO. (2017). *23081-1 Managing Metadata for Records Part 1: Principles*. Cenevre[İsviçre]: ISO.

ISO. (2018). *14641 Design and Operation of An Information System for the Preservation of Electronic Documents: Specifications.* Cenevre[İsviçre]: ISO.

ISO. (2018). *21496 Appraisal for Managing Records.* Cenevre[İsviçre]: ISO.

ISO. (2019). *27050-1 Electronic Discovery Part 1: Overview and Concepts.* Cenevre[İsviçre]: ISO.

ISO. (2020). *16175-1 Processes and Functional Requirements for Software for Managing Records Part 1: Functional Requirements and Associated Guidance for any Applications that Manage Digital Records:* Cenevre[İsviçre]: ISO.

Lekkas, D. ve Gritzalis, D. (2007). Long-term verifiability of electronic healthcare records authenticity. *International Journal of Medical Informatics*, 76, 442-448.

Long Term Records Management Project. *Recommended Practices*. 14 Şubat 2023 tarihinde http://research.dnv.com/LongRec/ResearchResults/Pages/RecommendedPractices.html adresinden erişildi.

Macneil, H. (2000). *Trusting records: Legal, historical and diplomatic perspectives.* yayın yeri yok: Springer.

Mosweu, O. (2020). Assessing digital records authenticity in a Botswana government accounting system: An archival diplomatics perspective. *South African Journal of Libraries & Information Science, 86*(1), 64-72.

National Archives of Australia (2015). *Australian Government Recordkeeping Metadata Standart*. 14 Şubat 2023 tarihinde https://www.naa.gov.au/sites/default/files/2019-09/AGRkMS-Version-2.2-June-2015_tcm16-93990_1.pdf adresinden erişildi.

National Archives. *Digital Record Object Identification [DROID]*. 14 Şubat 2023 tarihinde https://www.nationalarchives.gov.uk/information-management/manage-information/preserving-digital-records/droid adresinden erişildi.

Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik. *R. G.* (29413, 11 Temmuz 2015). 14 Şubat 2023 tarihinde http://www.resmigazete.gov.tr/eskiler/2015/07/20150711-19.htm adresinden erişildi.

Open Preservation Foundation [OPF]. *JSTOR/Harvard Object Validation Environment [JHOVE]*. 14 Şubat 2023 tarihinde https://jhove.openpreservation.org adresinden erişildi.

Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik. *R. G.* (31151, 10 Haziran 2020).14 Şubat 2023 tarihinde https://www.resmigazete.gov.tr/eskiler/2020/06/20200610-8.pdf adresinden erişildi.

Rogers, C. (2015). *Virtual authenticity: Authenticity of digital records from theory to practice*. Yayımlanmamış doktora tezi, University of British Columbia, Vancouver[Kanada]. 14 Şubat 2023 tarihinde http://hdl.handle.net/2429/52722 adresinden erişildi.

Rogers, C. (2015a). Diplomatics of born digital documents: Considering documentary form in a digital environment. *Records Management Journal*, *25*(1), 6-20.

Rolan, G. (2017). Towards interoperable recordkeeping systems: A meta-model for recordkeeping metadata. *Records Management Journal, 27*(2), 125-148.

Sağlık, Ö. (2021). *Elektronik belge yönetimi uygulamalarındaki koşullar ışığında e-imzalı belgelerin delil değerinin arşivsel güvenilirlik açısından incelenmesi*. Yayımlanmamış doktora tezi, İstanbul Üniversitesi: İstanbul. 14 Şubat 2023 tarihinde http://hdl.handle.net/20.500.12627/167875 adresinden erişildi.

Sağlık, Ö. ve Çiçek, N. (2020). Elektronik imzalı belgelerin delil değerinin korunmasında mevzuatta öngörülen delil özelliklerinin incelenmesi. *Bilgi Yönetimi*, *3*(2), 120-142.

Salza, S. ve Guercio, M. (2012). Authenticity management in long term digital preservation of medical records. R. Moore vd. (Yay. Haz.). *9. International Conference on the Preservation of Digital Objects* içinde (ss. 172-179). Toronto[Kanada]: University of Toronto.

Shabou, B. M. (2015). Digital diplomatics and measurement of electronic public data qualities: What lessons should be learned? *Records Management Journal*, *25*(1), 56-77.

Stancic, H. vd. (2015). Archival cloud services: Portability, continuity and sustainability aspects of long-term preservation of electronically signed records. *The Canadian Journal of Information and Library Science*, *39*(2), 210-227.

Tennis, J. (2013). Data, documents and memory: A taxonomy of sources in relation to digital preservation and authenticity metadata. L. Duranti ve E. Shaffer (Yay. Haz.). *The memory of the world in the digital age: Digitization and preservation* içinde (ss. 933-940). Vancouver[Kanada]: United Nations Educational, Scientific and Cultural Organization [UNESCO].

TSE. (2015). *13298 Elektronik Belge Yönetim Sistemi Standardı*. Ankara: TSE.

Türk Ticaret Kanunu. *R. G.* (27846, 14 Şubat 2011). 14 Şubat 2023 tarihinde http://www.resmigazete.gov.tr/eskiler/2011/02/20110214.htm adresinden erişildi.

UNESCO. *Software Heritage Web Sitesi*. 14 Şubat 2023 tarihinde https://www.softwareheritage.org adresinden erişildi.

Yalçınkaya, B. (2014). *E-devlet üstveri standardının oluşturulması ve Türkiye için modellenmesi*. Yayımlanmamış doktora tezi. Marmara Üniversitesi: İstanbul. 14 Şubat 2023 tarihinde http://hdl.handle.net/11424/198695 adresinden erişildi.

Zhang, G. (2013). *A new electronic records security model for long-term preservation*. B. Li vd. (Yay. Haz.). *10th Web Information System and Application Conference* içinde (ss. 191-194). Yangzhou[Çin]: yayıncı yok.

EK 1. Güvenilirlik Üstverisi

Tablo 1. Güvenilirlik Üstverisi

Üstveri	Kaynak	Seçmeli/Zorunlu
E-belge yönetimi politika ve prosedürleri	TSE, 13298 (s. 42)	Zorunlu
E-arşiv yönetimi politika ve prosedürleri	TSE, 13298 (s. 42)	Zorunlu
İş süreçlerine dair dokümantasyonlar	ISO, 14641 (s. 30)	Seçmeli
Form ve şablonlar	TSE, 13298 (s. 41)	Zorunlu
Belge türü şablonları kontrol numaraları	TSE, 13298 (s. 7)	Seçmeli
Spesifik üstveri şemaları	ISO, 15489 (s. 6)	Zorunlu
Dosya tasnif ve saklama planları	ISO, 15489 (s. 14)	Zorunlu
Kontrollü terminolojiler	ISO, 26122 (s. V)	Seçmeli
Felaket kurtarma ve yedekleme planları	ISO, 27050-1 (s. 20) ve ISO, 14641 (s. 7)	Zorunlu
Dokümanın belgeye dönüşme tarih ve zamanı (Log kayıtlarında)	TSE, 13298 (s. 23)	Zorunlu
Belgeye erişim istekleri (Log kayıtlarında)	TSE, 13298 (s. 23)	Zorunlu
Belgenin iletim geçmişi (Log kayıtlarında)	TSE, 13298 (s. 23)	Zorunlu
Belgeye yapılan açıklamalar (Log kayıtlarında)	INTERPARES, 2008 (s. 692)	Zorunlu
Belgede yapılan işlemler ve bu işlemleri yapan kullanıcılar (Log kayıtlarında)	TSE, 13298 (s. 23)	Zorunlu
Üstverilerde yapılan değişiklikler (Log kayıtlarında)	TSE, 13298 (s. 24)	Zorunlu
Saklama planı ve saklama sürelerinde yapılan değişiklikler (Log kayıtlarında)	TSE, 13298 (s. 23)	Zorunlu
Belgede yaşanan teknolojik değişimler (Log kayıtlarında)	ISO 23081-1 (s. 6)	Zorunlu
Sistem arıza ve bakımları (Log kayıtlarında)	ISO 15801 (s. 26)	Zorunlu
Paraf bilgileri ve paraflayanın yaptığı işlemler (Log kayıtlarında)	TSE, 13298 (s. 24)	Zorunlu
Belgelerin taşıyıcı ortamının değiştirilip değiştirilmemesi hususunda düzenli aralıklarla yapılan incelemelerin sonuçları	ISO, 27040 (s. 48)	Seçmeli
Teknolojik göç sonrası belgenin erişilebilirliği ve okunabilirliğinin kontrol edilmesi	ISO, 13008 (s. 13-14)	Zorunlu
Yeni taşıyıcı ortamın oluşturulması ve göçün gerçekleştiği tarih	ISO, 13008 (s. 8)	Zorunlu
Teknolojik göç konusunda risk analiz raporları	INTERPARES, 2002 (s. 30)[4]	Zorunlu
Yedeklemenin tarihi ve zamanı	INTERPARES, 2008 (s. 214)	Zorunlu
Yedeklemeyi onaylayan	INTERPARES, 2008 (s. 214)	Zorunlu
Yedeklemenin konumu	INTERPARES, 2008 (s. 214)	Seçmeli
Yedekleme referans numarası	INTERPARES, 2008 (s. 214)	Zorunlu
Yedeklemenin başarılı olup olmadığı (Log kayıtlarında)	INTERPARES, 2002 (s. 163)[5]	Seçmeli
Yazılım algoritması	UNESCO, Software Heritage	Zorunlu
Veri tabanı formatı	ISO, 15801 (s. 20)	Seçmeli
Belgelerin saklama konumu	ISO, 27037 (s. 10)	Seçmeli
Belgelerin üretildiği araçlardaki donanım ve yazılım özellikleri	TSE, 13298 (s. 30)	Zorunlu

[4] INTERPARES'in ilk safhasındaki projenin ürünü olan bu kitaba erişmek mümkün olmamıştır. Luciana Duranti ile yapılan görüşmede doğru atıf şeklinin kitaptaki bölümlerin yazarlarına yapılması gerektiği kararlaştırılmıştır. Durum böyle olunca, kaynakçada Heather MacNeil'in editörlüğünü yaptığı Authenticity Task Force Report'a atıf yapılmıştır. Ancak tablodaki üstverilerin kaynağı, INTERPARES çıktıları ve standartlar gibi metinler olduğundan söz konusu atıf INTERPARES şeklinde bırakılmıştır.

[5] Kaynakçada Heather MacNeil'in editörlüğünü yaptığı Requirements for Assessing and Maintaining the Authenticity of Electronic Records'a atıf yapılmıştır.

Log kayıtlarının zaman damgası ile damgalanması	ISO, 18829 (s. 6)	Zorunlu
Üstveri dosyası formatı	INTERPARES, 2008 (s. 277)	Zorunlu
Yapılan işlemlerin tarih ve zamanı (Log kayıtlarında)	ISO, 27040 (s. 58)	
Denetim günlüklerine erişimde sorun yaşanıp yaşanmadığı hususunda düzenli aralıklarla yapılan otomatik incelemelerin sonuçları	ISO, 15801 (s. 39)	Zorunlu
Sorumlu (Belgeyi üreten kurum)	TSE, 13298 (s. 52)	Zorunlu
Düzenleyen (Belgedeki irade beyanı sahibi)	TSE, 13298 (s. 57)	Zorunlu
Muhatap/Alıcı	TSE, 13298 (s. 57)	Zorunlu
Konu	TSE, 13298 (s. 57)	Zorunlu
Belge formatı	TSE, 13298 (s. 58)	Zorunlu
Belgenin üretim tarihi	TSE, 13298 (s. 57)	Zorunlu
KEP aracılığıyla belgenin gönderim/alma tarihi	TSE, 13298 (s. 57)	Zorunlu
Belge tarihi (Son imzalayıcının imza attığı tarih)	TSE, 13298 (s. 59)	Zorunlu
Belgenin dosyasına kaldırıldığı zaman	INTERPARES, 2002 (s. 28)[6]	Zorunlu
Belgenin ait olduğu işlem-dosya-seri-birim	INTERPARES, 2002 (s. 147)[7]	Zorunlu
Dosya kodu	TSE, 13298 (s. 57)	Zorunlu
Belge referans numarası	TSE, 13298 (s. 56)	Zorunlu
Belgeye erişmek için asgari gereksinimler	ISO, 23081-1 (s. 13)	Zorunlu
Belgenin üretildiği EBYS yazılımı ve versiyon numarası	TSE, 13298 (s. 58)	Zorunlu
Belge yönetimi için kullanılacak algoritmalar	ISO, 12033 (s. 42) ve ISO, 27040 (s. 49)	Zorunlu
Belge bileşenleri	TSE, 13298 (s. 60)	Zorunlu
E-imza ve zaman damgası bilgileri	TSE, 13298 (s. 59)	Zorunlu
Saklama süresi	TSE, 13298 (s. 7)	Zorunlu
Belgeye erişim profilleri	ISO, 16175-1 (s. 12)	Zorunlu
Belgenin konumu	ISO, 27037 (s. 10)	Seçmeli
Belgeye yapılan açıklama notları	INTERPARES, 2008, (s. 210-211)	Zorunlu
Sayısal koruma için yapılan işlemler	ISO, 15801 (s. 25)	Zorunlu
Belgenin sayısı	TSE, 13298 (s. 56)	Zorunlu
Belgenin gizlilik derecesi	TSE, 13298 (s. 58)	Zorunlu
Belgedeki ilgilerin referans numarası	TSE, 13298 (s. 60)	Zorunlu
Belgenin özet değeri	ISO, 13008 (s. 22)	Zorunlu
Şifreleme bilgisi	TSE, 13298 (s. 59)	Zorunlu
Belgedeki eklerin referans numaraları	TSE, 13298 (s. 60)	Zorunlu
Belgenin ait olduğu dosya türü	ISO 16175-1 (s. 16)	Zorunlu
Fiziksel ortamda saklanan belgelerin yeri	TSE, 13298 (s. 50)	Zorunlu
Saklama süresi sonunda yapılacak tasfiye işlemleri	ISO, 16175-1 (s. 9) ve TSE, 13298 (s. 62)	Seçmeli
Belgenin arşive devir zamanı	INTERPARES, 2008 (s. 211)	Zorunlu
Belgenin özgünlüğünü onaylayan teknikler	INTERPARES, 2008 (s. 226)	Zorunlu
Belgenin özgünlüğünü onaylayan kişiler	INTERPARES, 2008 (s. 226)	Zorunlu
Özgünlük değerlendirme raporu	INTERPARES, 2008 (s. 226)	Seçmeli
Belgenin tanımlama bilgileri	INTERPARES, 2008 (s. 226)	Seçmeli

[6] Kaynakçada Heather MacNeil'in editörlüğünü yaptığı Authenticity Task Force Report'a atıf yapılmıştır.

[7] Kaynakçada Heather MacNeil'in editörlüğünü yaptığı Requirements for Assessing and Maintaining the Authenticity of Electronic Records'a atıf yapılmıştır.

Kurumsal mühür bilgileri	Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik	Seçmeli
EYP bilgileri	TSE, 13298 (s. 17)	Zorunlu
Bütünlük analizinin düzenli kontrolünün sonuçları	ISO, 27040 (s. 17)	Zorunlu
Bütünlük bozulması riskine karşı risk değerlendirmesi ve riskten kaçınma raporları	ISO, 21496 (s. V)	Seçmeli
Kullanılan dosya tanımlayıcılar	The National Archives, Open Preservation Foundation	Zorunlu
Log kayıtlarına erişimde sorun yaşanıp yaşanmadığı hususunda düzenli aralıklarla yapılan otomatik incelemelerin sonuçları	TSE, 13298 (s. 23)	Zorunlu