T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

DOKTORA TEZİ

ELEKTRONİK BELGE YÖNETİMİ UYGULAMALARINDAKİ KOŞULLAR IŞIĞINDA E-İMZALI BELGELERİN DELİL DEĞERİNİN ARŞİVSEL GÜVENİLİRLİK AÇISINDAN İNCELENMESİ

Özhan SAĞLIK
2502150019

TEZ DANIŞMANI
PROF. DR. Niyazi ÇİÇEK

İSTANBUL - 2021

ÖZ

ELEKTRONİK BELGE YÖNETİMİ UYGULAMALARINDAKİ KOŞULLAR IŞIĞINDA E-İMZALI BELGELERİN DELİL DEĞERİNİN ARŞİVSEL GÜVENİLİRLİK AÇISINDAN İNCELENMESİ

ÖZHAN SAĞLIK

Bu tezde elektronik imzalı (e-imzalı) belgelerin delil değeri arşivsel güvenilirlik açısından incelenmektedir. Problem, kurumların elektronik belge yönetim sistemlerinde (EBYS) üretilip arşivlenen bu belgelerin zaman içerisinde özgünlüğünü koruyamama riskidir. Bu durum, özellikle uzun süre saklanacak e-imzalı belgelerin delil değerini tehdit edip güvenilirliklerinden şüphe duyulmasına neden olabilir. Hipotez, "e-imza, zaman damgası ve e-mühür gibi yapıların kırılganlıkları ve kurumların gerekli denetimleri uygulamamasından dolayı arşivlenen e-imzalı belgelerin uzun süre saklanmaları sürecinde delil değerinde kayıplar yaşanabilir" şeklindedir. Tezde karma yöntem benimsenmiş, nitel ve nicel araştırma yapılmıştır.

Saha araştırmasının nitel kısmında örneklem olarak Türkiye'de farklı kurumlardaki e-belge yönetimi uygulamalarını değerlendirmiş uzmanlar seçilmiştir. Dokuz (9) kişi ile görüşme yapılmıştır. Nicel kısımda ise Türkiye'de en çok kamu personeli çalıştıran organizasyonların kümesi olan bakanlıklar örnekleminden altı (6) kurum incelenmiştir. Nitel araştırmada literatür okumaları neticesinde oluşan kanaatlerin saha uzmanları tarafından da benimsenip benimsenmediği sorulmuş ve bu kanaatlerin biri hariç hepsi kabul görmüştür. Nicel araştırmada ise arşivsel bağın muhafazası, gerekli teknolojik koşulların sağlanması ve belgelerin güvenilirliğinin korunmasına yönelik politika ve prosedürlerin çıkarılmasına ilişkin uygulamalar değerlendirilmiştir.

Kurumların bu alanlarda yeteri kadar pratiğinin olmadığı tespit edilmiştir. Teknolojik koşulların sağlanmasında ise diğerlerine göre daha başarılı oldukları gözlenmiştir. Sahada e-belge yönetiminin süreç olarak değerlendirilmeyip, uygulama yazılımından ibaretmiş gibi görüldüğü anlaşılmıştır. Tezde e-imzalı belgelerin güvenilirliğinin korunup delil değerinin riske girmemesi için uzun dönemli korumaya

yönelik politikaların geliştirilmesi, gerekli teknolojik koşulların sağlanması ve belge hiyerarşisi koparılmadan arşivsel bağın muhafaza edilmesi gerektiği sonucuna varılmıştır.

Anahtar Kelimeler: e-belge yönetimi, e-belge, e-arşiv, e-imza, e-imzalı belgelerin delil değeri, arşivsel güvenilirlik, arşivsel bağ, organik bağ, e-belgelerin dosyalanması, diplomatik analiz, blokzincir teknolojisi, yapay zekâ, yapay öğrenme, derin öğrenme, elektronik delil elde etme

ABSTRACT

SURVEYING THE EVIDENTIAL VALUE OF E-SIGNED RECORDS IN THE LIGHT OF THE CONDITIONS AT ELECTRONIC RECORDS MANAGEMENT APPLICATIONS IN TERMS OF THE ARCHIVAL TRUSTWORTHINESS

ÖZHAN SAĞLIK

In this thesis, the evidential value of electronic signed (e-signed) records is examined in terms of archival trustworthiness. The problem is that the risk of these records generated and archived in organizations' electronic records management systems can not preserve their authenticity over time. Therefore it may threaten the evidential value of the particularly e-signed records that will be stored for a long time and cause doubts about their trustworthiness. The hypothesis is as follows: "Due to the fragility of structures such as e-signature, timestamp and e-seal and the failure of institutions to adopt necessary controls, the evidential value of archived e-signed records may be lost over time in the process of long term preservation." A mixed method was adopted in the thesis, qualitative and quantitative research was conducted.

In the qualitative part of the field research, experts who have evaluated e-records management practices in different organizations in Turkey were selected as a sample. Nine (9) people were interviewed. In the quantitative part, six (6) institutions from the ministries sample, which are the cluster of organizations that employ the most public personnel in Turkey, were examined. In the qualitative research, it was asked whether the experts also adopted the opinions that emerged from the literature readings, and it was understood that all of these opinions were accepted, except for one. In the quantitative research, practices of the institutions regarding the maintenance of the archival bond, provision of the necessary technological conditions and enacting of policies and procedures for the preservation of trusworthiness of the records were criticized.

In the light of the answers given to the questions, it has been seen that the institutions do not have enough successful practices in these areas. Institutions are

more successful in providing technological conditions. It has been understood that e-records management is not considered as a process, but adopted just as a software in the field. In order to preserve the trustworthiness of e-signed records and prevent their evidential value from risking, it has been conducted that policies and procedures for long-term preservation should be enacted, the necessary technological conditions should be provided, and the archival bond should be maintained without breaking the record hierarchy.

Keywords: e-records management, e-records, e-archive, e-signature, evidential value of e-signed records, archival trustworthiness, archival bond, organic bond, filing of e-records, diplomatic analysis, blockchain technology, artificial intelligence, machine learning, deep learning, digital forensics

ÖNSÖZ

Bu doktora tezi, kurumlarda oluşan e-imzalı belgelerin delil değerinin mevcut EBYS'lerde hangi oranda korunduğunu ve arşivsel güvenilirlik yaklaşımıyla nasıl incelenebileceğini araştırmaktadır. Türkiye'de en çok personel çalıştıran kurum öbeği olması nedeniyle bakanlıklar özelinde bir inceleme yapılmış, örneklem olarak 6 (altı) kurum araştırmaya dâhil olmuştur. Belgelerin delil değerinin arşivsel güvenilirlik bakımından incelenmesi konusunda uzmanlarla da görüşülmüştür.

E-imzalı belgelerin arşivlenip uzun dönemli korunmaları sürecinde delil değerini muhafaza edip edemeyecekleriyle ilgili şüpheler bulunmaktadır. Bu şüpheler, daha çok sayısal ortamın kırılganlığı ve e-imzaların uzun yıllar geçerliliğini muhafaza edemeyeceği endişesinden kaynaklanmaktadır. Bununla birlikte, arşivsel bağın kurulamaması, yeterli teknolojik koşulların sağlanamaması ile kurumsal politika ve prosedürlerin tesis edilememesi sonucunda e-imzalı belgelerin delil değerinin zayıflayabileceği düşünülmektedir. Bu kanaati sınamak için uluslararası standart ve projelerde geliştirilen çıktılar ışığında belirlenen sorularla Türkiye'deki e-imzalı belgelerin delil değerinin hangi oranda korunduğu incelenmiştir. Gerekli önlemler alınmazsa bu belgelerin delil değerinde kayıplar yaşanacağı söylenebilir.

Saha çalışması sırasında bazı kurumlar, adlarının yayınlanmaması şartıyla araştırmaya dâhil olabileceklerini belirtmiş, bir kısmından ise olumlu bir cevap alınamamıştır. Bu nedenle araştırmaya 6 kurum katkı sağlamıştır. Görüşme gerçekleştirip anket sorularını cevaplayan çalışanlara teşekkür borçluyum.

Tez konusunu belirlememde yardımcı olan, tezin ortaya çıkışında değerli katkılarını esirgemeyen danışmanım Prof. Dr. Niyazi Çiçek'e içtenlikle teşekkür etmek isterim. Tez izleme komitesinde yer alarak değerli görüşleriyle beni yönlendiren Prof. Dr. Oğuz İcimsoy ve Prof. Dr. İshak Keskin'e şükranlarımı arz ediyorum.

Saha araştırmasındaki bulguları yorumlamada katkıda bulunan Doç. Dr. Bahattin Yalçınkaya'ya, nitel ve nicel anket sorularını cevaplayan katılımcılara, saha araştırmasındaki desteklerinden dolayı Türkiye Cumhuriyeti Cumhurbaşkanlığı Bilgi ve Belge Yönetimi Daire Başkanı Serkan Menteş'e, aynı birimde uzman olarak çalışan Mutlu Uysal'a, görüşleriyle teze katkıda bulunan Prof. Dr. Fahrettin Özdemirci,

uzman arşivci Mehmet Torunlar ve Kızılay Arşiv Müdürü Mevlüt Kuş'a teşekkür etmek isterim.

Tezin istatistiksel kurgusunun geliştirilmesinde görüşlerine başvurduğum Bursa Uludağ Üniversitesi Psikoloji Bölümünde araştırma görevlisi Deniz Bilger ve Bursa Teknik Üniversitesinde öğretim görevlisi Oytun Cibaroğlu'na teşekkür borçluyum. Bununla birlikte, elektronik delil elde etme yöntemlerinin belge yönetiminde uygulanması hususundaki görüşleriyle beni yönlendiren Bursa Uludağ Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyesi Prof. Dr. Ahmet Emir Dirik'e, mevzuattaki hükümlerin yorumlanmasında yardımcı olan hâkim Cansu Çamur ve Kültür Bakanlığı müfettişi Emre İlhan'a teşekkür ederim. Tezi baştan sona okuyarak önemli değerlendirmelerde bulunan Yasemin Genç Sağlık ve Emine Pınar Gevheroğlu'na müteşekkirim.

Elektronik belgelerin özgünlüğü hakkında görüş ortaya koyup teze katkıda bulunan İskoçya Milli Arşivinden Tim Gollins'e teşekkür borçluyum. Bununla birlikte, elektronik belgelerin güvenilirliği, blokzincir teknolojisi ve sayısal koruma konularında fikirleriyle beni yönlendiren International Research on Permanent Authentic Records in Electronic Systems (INTERPARES - Elektronik Sistemlerde Belgelerin Özgünlüğünün Korunması Üzerine Uluslararası Araştırma) Direktörü Prof. Dr. Luciana Duranti ve British Columbia Üniversitesi öğretim üyesi Prof. Dr. Victoria Lemieux'e teşekkür etmek isterim.

ÖZHAN SAĞLIK
İSTANBUL, 2021

İÇİNDEKİLER

İKİNCİ BÖLÜM
E-BELGELERİN GÜVENİLİRLİK UNSURLARI VE TEHDİTLER

ÜÇÜNCÜ BÖLÜM
E-BELGELERİN GÜVENİLİRLİĞİNİN KORUNMASI YÖNTEMLERİ

DÖRDÜNCÜ BÖLÜM
SAHA ARAŞTIRMASI

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

a.e. : Aynı eser
a.g.e. : Adı geçen eser
AB : Avrupa Birliği
ABD : Amerika Birleşik Devletleri
ACID : Atomicity, consistency, isolation, durability (Bölünmezlik, tutarlılık, diğer nesnelerden ayrılabilme ve süreklilik)
ACM : Association for Computing Machinery (Bilgisayar Derneği)
AFF : Advanced Forensics Format (İleri Seviye Delil Formatı)
AFFBOM : Advanced Forensics Format Bill of Material (İleri Seviye Delil Formatı Listesi)
AIP : Archival Information Package (Arşiv Bilgi Paketi)
APARSEN : Alliance Permanent Access to the Records of Science in Europe Network (Avrupa'daki Bilim Kayıtlarına Kalıcı Erişim Birliği Ağı)
API : Application Programming Interface (Uygulama Programlama Arayüzü)
ASCII : American Standard Code for Information Interchange (Bilgi Değişimi için Amerikan Standart Kodlama Sistemi)
BES : Basic Electronic Signature (Basit/Temel Elektronik İmza)
BİLGEM : Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BM : Birleşmiş Milletler
BS : British Standard (İngiliz Standardı)
bs. : Basım
BTK : Bilgi Teknolojileri ve İletişim Kurumu
C. : Cilt
CADES : Cryptographic Message Syntax (CMS) Electronic Signature (CMS Elektronik İmza)
CADES-A : Cryptographic Message Syntax Archival Electronic Signature (CMS Arşiv Elektronik İmza)
CASPAR : Cultural, Artistic and Scientific Knowledge for Preservation, Access and Retrieval (Koruma, Erişim ve Bulup Getirme için Kültürel, Sanatsal ve Bilimsel Bilgi)
CBDDO : Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
CD : Compact Disk
CERN : Conseil Européen pour la Recherche Nucléaire (Avrupa Nükleer Araştırma Merkezi)
CMK : Ceza Muhakemesi Kanunu
CMS : Cryptographic Message Syntax (Kriptografik Mesaj Sözdizimi)
CRC : Cyclic Redundancy Check (Döngüsel Artıklık Denetimi)
Çev. : Çeviren
ÇiSDuP : Çevrimiçi Sertifika Durum Protokolü (Online Certificate Status Protocol, OCSP)

DAVID : Flaman Kurum ve Kuruluşlarında Elektronik Arşivleme (Digitale Archivering in/voor Vlaamse Instellingen en Diensten)
DDT : Dağıtık Defter Teknolojisi
DFXML : Digital Forensics eXtended Markup Language (Elektronik Delil Elde Etme Genişletilebilir İşaretleme Dili)
DIP : Dissemination Information Package (Dağıtım Bilgi Paketi)
DPC : Digital Preservation Coalition (Sayısal Koruma Koalisyonu)
DROID : Digital Record Object Identification (Sayısal Belge Nesnesi Kimliklendirme)
EAD : Encoded Archival Description (Kodlanmış Arşivsel Tanımlama)
EBYS : Elektronik Belge Yönetim Sistemi
ECC : Error Correcting Code (Hata Düzeltme Kodu)
EIDAS : Electronic Identification, Authentication and Trust Services (Elektronik Kimlik Belirleme ve Güven Hizmetleri)
EİK : Elektronik İmza Kanunu
ERPANET : Electronic Resource Preservation and Access Network (Elektronik Kaynak Koruma ve Erişim Ağı)
ES-A : Archival Electronic Signature (Arşiv Elektronik İmza)
ETSI : European Telecommunications Standards Institute (Avrupa Telekomünikasyon Standartlar Enstitüsü)
EYP : Elektronik Yazışma Paketi
E-ARK : European Archival Records and Knowledge Preservation (Avrupa Arşiv Bilgi ve Belgelerinin Korunması)
FAT 32 : File Allocation Table 32 (Dosya Yerleşim Tablosu)
FRED : Forensic Recovery of Evidence Device (Delil Elde Etme Aracı)
FTK : Forensic Toolkit Imager (Delil Elde Etme Araç Seti)
GDPR : General Data Protection Regulation (Genel Veri Koruma Yönetmeliği)
GIF : Graphics Interchange Format (Grafik Değiştirme Formatı)
GİB : Gelir İdaresi Başkanlığı
GPO : Government Publishing Office (Resmî Gazete Ofisi)
HEYS : Hizmet Envanteri Yönetim Sistemi
HFS : Hierarchical File System (Hiyerarşik Dosya Sistemi)
HMK : Hukuk Muhakemeleri Kanunu
IBM : International Business Machines (Uluslararası İş Makineleri)
ICA : International Council of Archives (Uluslararası Arşivler Konseyi)
IEEE : The Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)
IFRS : International financial reporting standards (Uluslararası finansal raporlama standartları)
IMF : International Monetary Fund (Uluslararası Para Fonu)

INTERPARES : International Research on Permanent Authentic Records in Electronic Systems (Elektronik Sistemlerde Belgelerin Özgünlüğünün Korunması Üzerine Uluslararası Araştırma)
ISO : International Organization for Standardization (Uluslararası Standartlar Teşkilatı)
İÜMK : İstanbul Üniversitesi Merkez Kütüphanesi
JHOVE : JSTOR/Harvard Object Validation Environment (JSTOR/Harvard Nesne Doğrulama Ortamı)
JORF : Journal Officiel de la Republique Française (Fransa Cumhuriyeti Resmî Gazetesi)
JPEG : Joint Photographic Experts Group (Birleşik Fotoğraf Uzmanları Grubu)
JSON : Javascript Object Notation (Javascript Nesne Gösterimi)
KAMU SM : Kamu Sertifikasyon Merkezi
KAYSİS : Devlet Teşkilatı Merkezi Kayıt Sistemi
KEP : Kayıtlı Elektronik Posta
KEPHS : Kayıtlı Elektronik Posta Hizmet Sağlayıcısı
MERSİS : Merkezi Sicil Kayıt Sistemi
METS : Metadata Encoding and Transmission Standard (Üstveri Kodlama ve İletim Standardı)
MONK : Metadata Offer New Knowledge (Yeni Bilgi Sunan Üstveri)
NARA : The National Archives and Records Administration (Amerika Milli Arşivi ve Belge Yönetimi İdaresi)
NDSA : National Digital Stewardship Alliance (Ulusal Sayısal Savunuculuk Birliği)
No : Numara
NTFS : New Technology File System (Yeni Teknoloji Dosya Sistemi)
OAIS : Open Archival Information Systems (Açık Arşivsel Bilgi Sistemi)
OCFL : Oxford Common File Layout (Oxford Müşterek Dosya Düzeni)
OECD : Organisation for Economic Co-operation and Development (Ekonomik Kalkınma ve İşbirliği Örgütü)
OJ : Officiel Journal (Avrupa Birliği Resmî Gazetesi)
OPC : Open Packaging Conventions (Açık Paketleme Kuralları)
OPF : Open Preservation Foundation (Açık Koruma Vakfı)
QR : Quick Response (Karekod)
PADES : Portable Document Format (PDF) Advanced Electronic Signature (Taşınabilir Doküman Formatı Gelişmiş Elektronik İmza)
PDF : Portable Document Format (Taşınabilir Doküman Formatı)
PDF/A : Portable Document Format Archive (Arşiv Taşınabilir Doküman Formatı)

PLANETS : Preservation and Long-Term Access Through Networked Services (Ağ Bağlantılı Hizmetler Aracılığıyla Koruma ve Uzun Dönemli Erişim)
PREMIS : Preservation Metadata Implementation Strategies (Koruma Üstverisi Uygulama Stratejileri)
PTT : Posta Telgraf Teşkilatı
RAID : Redundant Array of Independent Disks (Bağımsız Disklerin Artıklık Dizisi)
R.G. : Resmî Gazete
RYY : Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik
S : Sayı
s. : Sayfa/Sayfalar
SDP : Standart Dosya Planı
SHA : Secure Hashing Algorithm (Güvenli Özet Değeri Algoritması)
SIP : Submission Information Package (Gönderim Bilgi Paketi)
SİL : Sertifika İptal Listeleri
SSD : Solid State Disk (Katı Hâl Sürücüleri)
tar. : Tarih
TBMM : Türkiye Büyük Millet Meclisi
TDK : Türk Dil Kurumu
TIFF : Tagged Image File Format (Etiketlenmiş Görüntülü Dosya Formatı)
TNB : Türkiye Noterler Birliği
TNBSS : Türkiye Noterler Birliği Bilişim Sistemi
TRT : Türkiye Radyo Televizyon Kurumu
TS : Technical Specification (Teknik Özellikler)
TSE : Türk Standartları Enstitüsü
TBK : Türk Borçlar Kanunu
TMK : Türk Medeni Kanunu
TTK : Türk Ticaret Kanunu
TÜBA : Türkiye Bilimler Akademisi
TÜBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UBC : University of British Columbia
UBL : Universal Business Language (Evrensel İş Dili)
UETS : Ulusal Elektronik Tebligat Sistemi
UNCITRAL : United Nations Commission on International Trade Law (Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu)
UNESCO : United Nations Educational, Scientific and Cultural Organization (Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü)
URL : Unique Resource Locator (Tekbiçim Kaynak Tanımlayıcı)
UTF-8 : Unicode Transformation Format-8 (Unicode Dönüşüm Formatı-8)
UYAP : Ulusal Yargı Ağı Bilişim Sistemi

VUK : Vergi Usul Kanunu
WORM : Write Once Read Many (Bir Kez Yazılabilir Çok Kez Okunabilir)
XADES : Extended Markup Language (XML) Advanced Electronic Signature (Genişletilebilir İşaretleme Dili Gelişmiş Elektronik İmza)
XADES-A : XML Archival Electronic Signature (XML Arşiv İmza)
XADES-Bes : XML Basic Electronic Signature (XML Basit İmza)
XBRL : eXtensible Business Reporting Language (Genişletilebilir İşletme Raporlama Dili)
XML : eXtended Markup Language (Genişletilebilir İşaretleme Dili)
XSD : XML Schema Definition (XML Şema Tanımı)
YÖK : Yükseköğretim Kurulu

GİRİŞ

Tüm dünyada bilgi toplumunun etkisi ve bilişim teknolojisinin hızlı gelişmesiyle benimsenen e-Devlet anlayışı, Türkiye'de 2000'li yıllardan itibaren belge yönetiminde paradigma değişikliğine neden olmuştur. Hazırlanan uygulama yazılımlarıyla kurulan EBYS'ler, örgütlerdeki idari iş ve işlemleri bilinen kâğıt ortamdan elektroniğe taşımıştır. Elektronik İmza Kanunu'nun (EİK) ardından yürürlüğe giren güvenli e-imza ile elektronik belgeler (e-belge), hukukun tanıdığı delil ve ispat değerine sahip evrak olarak tanımlanmış ve ıslak imzalı belgelerle aynı ispat kuvvetinde olduğu kabul edilmiştir[1]. E-imza, her ne kadar belgeye güncel dönemde delil vasfı kazandırsa da zaman içerisinde bu değerin nasıl muhafaza edileceği uzmanlar tarafından tartışılmaktadır[2].

Uzun dönem korumak için arşivlenen e-belgelerin teknolojik eskime ve sayısal kırılganlık gibi durumlardan dolayı akıbetlerinin ne olacağı konusu henüz yeteri kadar cevap bulamadığından şüpheler de giderilememiştir. Bu şüphelerden biri, e-imzalı belgelerin özniteliklerinin zaman içerisinde korunup korunamayacağı sorusudur. Çünkü, belge bileşenlerinin muhafaza edilememesi, taşındığı formatın güncellenememesi, e-imzanın doğrulanamaması ve arşivsel bağın bozulması gibi nedenlerden dolayı arşivlenen e-imzalı belgelerin zaman içerisinde özgünlüğünü koruyamama riski bulunmaktadır. Bu durum, belgelerin delil değerini tehdit edip güvenilirliğinden şüphe duyulmasına neden olabilmekte; özgünlük, bütünlük ve kullanılabilirlik gibi birtakım karakteristik özelliklerin bozulabileceği tartışmalarını gündeme getirmektedir[3]. Bu tartışmalar, belgelerin üretildikleri dönemde yürütülen

---

1 "Elektronik İmza Kanunu", Kanun No: 5070, **Resmî Gazete**[**R.G.**], S 25355, tar. 23.01.2004, (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2004/01/20040123.htm#1, 5 Aralık 2020. Tezde kullanılan e-imzalı belgeler kavramı, güvenli e-imzalı belgeleri ifade etmektedir.

2 Luciana Duranti ve Allison Stanfield, "Authenticating Electronic Evidence", **Electronic Evidence and Electronic Signatures**, 5. bs., ed.: Stephen Mason ve Daniel Seng, Londra[Birleşik Krallık], University of London Press, 2021, s. 263. ; Stephen Mason, "Electronic Signature", **Electronic Evidence and Electronic Signatures**, 5. bs., ed.: Stephen Mason ve Daniel Seng, Londra[Birleşik Krallık], University of London Press, 2021, s. 285-288, 356-358, 368-370.

3 Niyazi Çiçek, "Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme", **Bilgi Dünyası**, C. 12, No: 1, 2011. ; Laura Millar, **A Matter of Facts: The Value of Evidence in an Information Age**, Chicago[Amerika Birleşik Devletleri(ABD)], American Library Association, 2019. ; Corinne Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice", Yayınlanmamış Doktora Tezi, University of British Columbia[Kanada], 2015. ; Anne Thurston, "Records as Evidence for Measuring Sustainable Development in Africa", **A Matter of Trust:**

fonksiyonlara ait idari işlemlerin delili olma niteliğini (delil değeri) kaybetme riskinden kaynaklanmaktadır. İdari ve hukuki bakımdan geçerli olabilmeleri için belgeler var olduğu sürece bu nitelikler korunmalıdır.

Güncel idari işlemler sırasında bir sorun yaşanmıyorken, arşiv malzemesi olduklarında üretildikleri dönemdeki özniteliklerini muhafaza edebilecekler mi, hukuki geçerliliklerini koruyabilecekler mi gibi sorular akla gelmektedir. Bu bağlamda hukuki kriterlerle birlikte arşivcilik teori ve uygulamaları, delil değerinin korunmasında kullanılabilir mi sorusu ortaya çıkmıştır. Bir zan olarak şekillenen bu soru, birtakım ön araştırmalarla kanaate dönüşünce, geçerliliği bu doktora teziyle sınanmaya çalışılmıştır. Tezin hipotezi şöyle belirlenmiştir: "E-imza, zaman damgası ve e-mühür gibi yapıların kırılganlıkları ve kurumların gerekli denetimleri uygulamamasından dolayı arşivlenen e-imzalı belgelerin uzun süre saklanmaları sürecinde delil değerinde kayıplar yaşanabilir". Tezin sorusu ise "Kurumlarda oluşan e-imzalı belgelerin delil değeri, mevcut e-belge yönetimi uygulamalarında hangi oranda korunmaktadır ve bu değer arşivsel güvenilirlik yaklaşımıyla nasıl incelenebilir?" şeklindedir.

Dünyada elektronik ortamda tutulan bilgi malzemelerinin güvenilirliğine ilişkin Electronic Resource Preservation and Access Network (ERPANET - Elektronik Kaynak Koruma ve Erişim Ağı)[4], Cultural, Artistic and Scientific Knowledge for Preservation, Access and Retrieval (CASPAR - Koruma, Erişim ve Bulup Getirme için Kültürel, Sanatsal ve Bilimsel Bilgi)[5], Preservation and Long-Term Access Through Networked Services (PLANETS - Ağ Bağlantılı Hizmetler Aracılığıyla Koruma ve Uzun Dönemli Erişim)[6], Alliance Permanent Access to the Records of Science in Europe Network (APARSEN - Avrupa'daki Bilim Kayıtlarına Kalıcı Erişim Birliği Ağı)[7] ve

---

Building Integrity into Data, Statistics and Records to Support the Sustainable Development Goals, ed.: Anne Thurston, Londra[Birleşik Krallık], University of London Press, 2020, s. 15.

4 **Electronic Resource Preservation and Access Network [ERPANET] Web Sitesi**, (Çevrimiçi) https://www.erpanet.org, 26 Temmuz 2020.

5 **Cultural, Artistic and Scientific Knowledge for Preservation, Access and Retrieval [CASPAR] Web Sitesi**, (Çevrimiçi) http://casparpreserves.digitalpreserve.info, 26 Temmuz 2020.

6 **Preservation and Long-Term Access Through Networked Services [PLANETS] Web Sitesi**, (Çevrimiçi) https://www.planets-project.eu, 26 Temmuz 2020.

7 **Alliance Permanent Access to the Records of Science in Europe Network [APARSEN] Web Sitesi**, (Çevrimiçi) http://www.alliancepermanentaccess.org, 26 Temmuz 2020.

INTERPARES gibi saha çalışmalarının yapıldığı bilinmektedir. Bunlar içerisinde kurumsal belgelerle alakalı olanı daha çok INTERPARES'dir. 1999 yılında başlayan INTERPARES çalışmalarına Türkiye, 2007 yılında 3. safhasından itibaren katılmıştır. Türkiye takımı'nın Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) projesi olarak yaptığı çalışma[8], kamu üniversitelerindeki e-belgelerin özgünlüğünün korunmasına ilişkin bir yaklaşımın mevcut olup olmadığını sorgulaması bakımından dikkat çekmektedir. Araştırmaya katılan üniversitelerde bu hususlarla ilgili yeterli prosedürün bulunmadığı anlaşılmış, e-belgelerin bütünlüğünün ve özgünlüğünün yeteri kadar korunamadığı sonucu ortaya çıkmıştır.

Bu çalışmaların yanı sıra çeşitli araştırmacıların da konu hakkında incelemeler yaptığı gözlenmektedir. Basma Makhlouf Shabou, yaptığı bir çalışmada, İsviçre'deki bazı kurumlarda üretilen e-belgelerin güvenilirlik niteliğini belgenin formatı, üreticisi ve düzenleyeni gibi özgünlük kriterleri açısından sorgulamıştır. Böylece, kurumlarda oluşan e-belgelerin güvenilirlik açısından niteliklerinin analiz edilebileceği görülmüştür[9]. Shabou'nun bu araştırmasının yanı sıra Güney Afrika'daki bir kurum özelinde e-belgelerin güvenilirliğinin analizi için bir kontrol listesinin hazırlandığı görülmektedir. Tezde de incelenen bu hususların daha ayrıntılı bir şekilde ele alındığı söz konusu çalışmada, kurumsal belge yönetimi politikası içerdiği maddeler bakımından incelenmiş ve bilgi teknolojileri yoğun süreçlerin e-belgelerin güvenilirliğinin korunmasındaki rolü analiz edilmiştir[10].

Bu konuyla alakalı Türkiye'de de farklı bilim insanlarının yayınları bulunmaktadır. E-belgelerin diplomatik analiz alanları ve dosyalamayla ilgili çalışmalardan tezde faydalanılmıştır[11]. Bununla birlikte, Hamza Kandur'un belgenin özniteliklerinin korunması

---

8 Bu takım, "INTERPARES 3 Kurumsal Bilgi Sistemleri İçerisinde Belge Yönetimi: Türkiye'deki Kamu Üniversitelerinde Gerçekleştirilen Uygulamalara Yönelik Bir Durum Analizi" adıyla bir Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Projesi gerçekleştirilmiştir (Özgür Külcü, **INTERPARES 3 Kurumsal Bilgi Sistemleri İçerisinde Belge Yönetimi: Türkiye'deki Kamu Üniversitelerinde Gerçekleştirilen Uygulamalara Yönelik Bir Durum Analizi**, 1011 TÜBİTAK Projesi, Proje No: 109K518, 2014, Ankara).

9 Basma Makhlouf Shabou, "Digital Diplomatics and Measurement of Electronic Public Data Qualities What Lessons Should be Learned?", **Records Management Journal**, C. 25, No: 1, 2015.

10 Mpho Ngoeepe ve Jonathan Mukwevho, **Ensuring Authenticity and Reliability of Digital Records to Support the Audit Process**, yayım yeri yok, yayımcı yok, 2018.

11 Niyazi Çiçek, "Özel Diplomatik Analiz Metodu: Sağlık Bakanlığında Üretilen İki Yazışma Üzerinde Uygulama", **Bilgi Dünyası**, C. 7, No: 2, 2006. ; Niyazi Çiçek, "Elektronik Belge Yönetimi Uygulamalarında Bir Alt Sistem Olarak Dosya Yönetimi", **Türk Kütüphaneciliği**, C. 30, No: 3, 2016. ; Niyazi Çiçek, "Elektronik Belge Yönetimi Uygulamalarında Dosya Bütünlüğü

için birim-seri-dosya-belge hiyerarşisinde bir tasnif sistemi oluşturulması, saklama planlarının hazırlanması, belgelerin sistem içerisinde tanımlanması ve üstverilerin oluşturulmasının temel bir gereklilik olarak benimsenmesi önerisinden yararlanılmıştır[12].

Bu önerilerin yanı sıra Ken Chasse, e-belgelerin delil değerinin sorgulanması için bir sertifikasyon sisteminin kurulmasını tavsiye etmektedir[13]. Bununla birlikte Aydın ve Özdemirci'nin çalışmasında Chasse'nin dile getirdiklerine benzer öneriler görülmektedir. Bu çalışma, e-belgelerle bileşenleri arasındaki bağın korunması gerektiğini ifade etmesi bakımından dikkate değerdir[14].

Resul Göksoy'un yüksek lisans tezine dayanarak yayınladığı anlaşılan "Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğin Sağlanması" adlı kitabı, sayısal delilin geçirdiği tüm sürecin şüpheden uzak bir şekilde kayıt altına alınarak üstveriler aracılığıyla izlenebilirliğinin sağlanmasını önermesi bakımından dikkat çekmektedir[15]. Göksoy'un bu çalışmasının yanı sıra Gamze Gümüşkaya'nın vergi mevzuatı açısından e-belgelerin delil değerini incelediği doktora tezinde, delillerin gerçeklik, akılcılık, güvenilirlik, olayı temsil edicilik ve hukuka uygunluk gibi niteliklerine dikkat edilerek olayı aydınlatma gücüne göre değerlendirilmesi önerilmektedir[16]. Hukuk disiplinin öğretileri ışığında şekillenen bu araştırmalarda delil değeri nitelemelerinin arşivsel güvenilirlik yaklaşımının dışında ele alındığı görülmüştür.

Türk mevzuatında idari işlemler sırasında temel güvenilirlik aracı olarak e-imza kullanılmaktadır. E-imzanın başlıca amacı belgenin düzenleyenini belirtmektir. Hâliyle belgelerin yaşam döngüsünde geçirdiği aşamaları göstermek gibi bir işlevi yoktur.

Problemi", **e-Beyas 2015 Sempozyumu Kurumsal Belleklerin Geleceği: Dijitalleştirme-Elektronik Arşiv-Elektronik Belge Yönetimi**, 21-22 Ekim 2015, ed.: Fahrettin Özdemirci vd., Ankara, Ankara Üniversitesi, 2016. ; Niyazi Çiçek, "Belediyelerdeki Elektronik Belge Yönetim Sistemlerinde Dijital Devamlılığı Tehdit Eden Yazılıma Dayalı Sorunlar", **Belediyelerin Kütüphane ve Arşiv Hizmetleri Uluslararası Sempozyumu**, 12-14 Mayıs 2016, ed.: Bülent Yılmaz vd., Nilüfer Belediyesi, Bursa, 2016.

12 Hamza Kandur, "Elektronik Belgelerin Özniteliklerinin Elektronik Belge Yönetimi Açısından İncelenmesi", **Aysel Yontar Armağanı**, ed.: Bekir Kemal Ataman ve Mesut Yalvaç, İstanbul, Türk Kütüphaneciler Derneği İstanbul Şubesi, 2004.

13 Ken Chasse, **Electronic Records as Evidence**, (Çevrimiçi) http://ssrn.com/abstract=2438350, 28 Kasım 2019.

14 Cengiz Aydın ve Fahrettin Özdemirci, "Elektronik Belgelerin Arşivlenmesinde Gerçekliğin ve Bütünlüğün Korunması", **Bilgi Dünyası**, C. 12, No: 1, 2011, s. 107-110, 122.

15 Resul Göksoy, **Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması**, Ankara, Seçkin Yayınevi, 2019, s. 113-115, 119.

16 Gamze Gümüşkaya, "Vergi Hukukunda İspat", Yayınlanmamış Doktora Tezi, İstanbul, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Mali Hukuk Anabilim Dalı, 2015, s. 266-267, 292.

Bundan dolayı, e-imza geliştiricilerinin arşivsel bağ örneğinde olduğu gibi yaşam döngüsündeki süreçleri gösteren unsurları dikkate almaması tabii kabul edilebilir. Her ne kadar güncel idari işlemlerde güvenilirlik aracı olarak tek başına e-imzanın kullanılması güvenilirliğin korunmasında yeteri kadar başarı sağlayabilse de belgelerin uzun süre saklanması durumunda güvenilirliğin ilk günkü gibi muhafaza edilip edilemeyeceği konusunda şüpheler henüz giderilememiştir. Durum böyle olunca, e-imzanın yanı sıra yeni elektronik güvenilirlik araçlarının da kullanılabileceği düşünülmektedir. Elektronik Yazışma Paketi (EYP) ve Kayıtlı Elektronik Posta (KEP) delili gibi bu güvenilirlik araçları, belgenin yaşam döngüsünde geçirdiği aşamaları göstermeleri, e-imza barındırmaları ve mevzuatta yer bulmaları nedeniyle öne çıkmaktadır.

E-imzalı belgelerde imza doğrulanamadığı takdirde hâkim, imzayı tetkik edip bir karara varamazsa bilirkişi incelemesine başvurabilmektedir. Bilirkişinin, e-imza analizi yaparken imza atıldığında oluşan özet değeriyle sonradan hesaplanan özet değerinin örtüşüp örtüşmediğini inceleyebildiği ifade edilmektedir[17]. Fakat yapılan inceleme, her zaman sağlıklı sonuçlar veremeyebilir. Örneğin, imza oluşturma ve doğrulama verileri kontrol edilemeyebilir, zaman damgası sunucusunda gecikmeler yaşanabilir ya da merkezi otoriteler imza verilerini arşivlememiş olabilir[18]. Bu durumda delil değeri unsurlarından olan "aidiyeti belli olmak" kriteri sağlanamayacaktır. Hâl böyle iken, doğru koşullarda üretilmiş fakat teknik ve teknolojik nedenlerle e-imza doğrulaması yapılamamış belgeler geçersiz mi kabul edilecektir? Oysa delil değerini korumak için benimsenen arşivsel bağın açığa çıkarılmasına ilişkin yöntemlerden olan dosyalama ve diplomatik analiz ile teknolojik yaklaşımlardan e-delil elde etme yöntemleri, blokzincir teknolojisi ve yapay zekâ ile yapay öğrenme gibi araçlardan

---

17 Mustafa Serdar Özbek, "Elektronik Ortamda Düzenlenen Noter Senetleri", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 22, No: 3, 2016. Özet değeri, verilerin bütünlüğünün kontrolü için şifreleme algoritmalarıyla yeni bir bit dizisine dönüştürülmesi işlemidir. Bit, verinin en küçük yapıtaşıdır. 0 ve 1'den meydana gelir. 8 bit bir araya gelerek 1 baytı oluşturur. Bir bayt ise bit akışlarının oluşumuna kaynaklık eder.

18 Vladamir Bralic, Magdelena Kules ve Hrvoje Stancic, "A Model for Long-term Preservation of Digital Signature Validity: TrustChain", **InFuture 2017**, 8-10 Kasım 2017, ed.: Iana Atassova v.d., Zagrep, yayımcı yok, 2017. ; Jorge L. Hernandez-Ardieta v.d., "A Taxonomy and Survey of Attacks on Digital Signatures", **Computers&Security**, No: 34, 2013. ; Murat Özbek, "Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları", **1. International Symposium on Digital Forensics and Security**, 20-21 Mayıs 2013, ed.: Asaf Varol vd., Elazığ, yayımcı yok, 2013. ; Ross Spencer, "Binary Trees? Automatically Identifying the Links between Born-digital Records", **Archives and Manuscripts**, C. 45, No: 2, 2017.

faydalanılabileceği düşünülmektedir[19]. Burada, e-imzanın doğrulama süreçlerine alternatif geliştirmek değil, arşivsel güvenilirlik yaklaşımı benimsenerek delil değerinin korunmasına yardımcı olacak mekanizmalar önerilmektedir.

Ancak, KEP, dosyalama ve yapay zekâ gibi araçların kullanılması güvenilirliğin korunması için her zaman yeterli olmayabilir. Çünkü, taşıyıcı ortamın kırılganlığı ve teknolojik eskime nedeniyle bit akışının bozulması, belge ile üstveriler arasındaki ilişkinin kopması, dosyalamanın layıkıyla yapılamayıp belge yığınlarının oluşması ve gerekli kurumsal politika ve prosedürlerin çıkarılmaması gibi nedenlerle güvenilirlik teyidi riske girebilmektedir[20]. Hâliyle, güvenilirlik araçlarının belirlenip kullanılmasının yanı sıra bunu tehdit edecek risklerin de açıklanmasına ihtiyaç duyulmaktadır. Bunlar, tezde güncel belge sürecinde format yapısından kaynaklanan, gerekli teknolojik koşulların sağlanamamasında ortaya çıkan ve sürdürülebilirlikle ilgili riskler şeklinde değerlendirilmiştir.

Kurumlardaki EBYS'lerde oluşturulan e-imzalı belgelerin delil değerinin hangi oranda korunduğunun incelenmesinin amaçlandığı bu tezde arşivsel güvenilirlik bakış açısıyla hareket edilmiştir. "Karma yöntem" benimsenmiş, nitel ve nicel araştırma yapılmıştır. Saha araştırması bölümünde yöntemle ilgili hususlar belirtilmiştir. Nitel araştırmada örneklem olarak Türkiye'de farklı kurumlardaki e-belge yönetimi uygulamalarını değerlendirmiş uzmanlar seçilmiştir. Dokuz (9) kişi ile görüşme yapılmıştır. Katılımcılardan bazıları görüşlerinin çalıştıkları kurumları da bağlayabileceği endişesinden dolayı adlarının verilmesini istememiştir. Durum böyle olunca, katılımcıların verdikleri cevaplar rastgele numaralandırılarak aktarılmıştır. Ayrıca, literatürde karşılığı bulunan uzmanların görüşleri dipnotta "Görüş A", karşılığı bulunmayanlar ise "Görüş B" şeklinde kısaltılarak verilmiştir.

Nicel araştırmada ise tezin evrenini kamu kurumları oluşturmuştur. Örneklem seçilerek evren hakkında çıkarımlar yapılmıştır. Bunun için küme örnekleme yoluna

---

19 Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice", **a.g.e.** ; Sekie Amanuel Majore, Hyunguk Yoo ve Taeshik Shon, "Secure and Reliable Electronic Record Management System Using Digital Forensic Technologies", **The Journal of Supercomputing**, No: 70, 2014.

20 David Bearman, "Moments of Risk: Identifying Threats to Electronic Records", **Archivaria**, No: 62, Fall 2006. ; The National Archives, **Managing Digital Contunity Loss**, 2017, s. 7, (Çevrimiçi) https :// www. nationalarchives. gov. uk/ documents/ information-management/ managing-digital-continuity-los.pdf, 4 Mart 2020.

gidilmiş ve Türkiye'de en çok kamu personeli çalıştıran kurumların kümesi olan bakanlıklar, örneklemi oluşturmuştur. Saha araştırmasında 6 (altı) kurum incelenmiştir. Diğer bakanlıklar, araştırma yapılması teklifine olumlu ya da olumsuz bir cevap vermemiştir. Ancak, araştırmaya katılanlar sonuçların olumsuz etki doğurabileceği endişesi nedeniyle adlarının açıklanmasını istememişlerdir. Kurumlar numaralandırılarak verdikleri cevaplar aktarılmıştır.

Literatürdeki eserler incelenirken İstanbul Üniversitesi Merkez Kütüphanesi (İÜMK) ve Bursa Uludağ Üniversitesi Prof. Dr. Fuat Sezgin Merkez Kütüphanesinin abone olduğu elektronik kaynaklar taranmıştır. Türkiye'deki tezler için Yükseköğretim Kurulu (YÖK) Tez Kataloğu, yabancı dildeki tezler için ise Proquest Dissertations & Theses veri tabanları incelenmiştir. Resmî Gazete ve konuyla ilgili tartışmaların yapıldığı sosyal medya platformları (Twitter, Facebook) ve web siteleri de başvurulan kaynaklar arasında yer almaktadır. Literatür taraması yapılırken, Türkçe kaynaklarda "delil", "belge", "arşiv", "özgünlük", "güvenilirlik", "arşivsel bağ", "elektronik belge yönetimi" ve "dosyalama"; yabancı dil kaynaklarda ise "evidence", "records", "archive", "authenticity", "trustworthiness", "archival bond", "electronic records management" ve "filing" gibi anahtar kelimeler kullanılmıştır. Tez yazılırken Türk Dil Kurumu (TDK) ve İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Kılavuzu'na[21] göre hareket edilmiştir.

Tezin birinci bölümünde Türkiye'de ve çeşitli ülkelerde, e-belgelerin delil değeriyle ilgili hükümler içeren mevzuat araştırılmıştır. Burada Metin Turan ve Özgür Külcü'nün birlikte kaleme aldıkları makalelerinden yararlanılmıştır[22]. Bu çalışma, delil değeriyle ilgili hükümlerin olduğu tüm mevzuatı belirtmese de yönlendirici olmuştur. Aynı zamanda Ayşe Ece Acar'ın e-imzalı belgelerin delil niteliklerini

---

21 Tez yazım kurallarına göre tablo ve şekiller, yer aldığı bölüm numaralarıyla birlikte adlandırılmaktadır. Fakat tezde çoğu tablo ve şekil EK'de verildiğinden tablo ve şekiller ait olduğu bölümlere (Tablo 1.1, Tablo 2.2, Tablo 3.1 gibi) göre değil, ardışık numaralarla (Tablo 1, Tablo 2, Tablo 3 gibi) isimlendirilmiştir (İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, **Tez Hazırlama Yönergesi**, İstanbul, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, tarih yok, (Çevrimiçi) https:// cdn. istanbul. edu. tr/ FileHandler2. ashx?f= tez. hazirlama. yonergesi. pdf, 4 Ekim 2020).

22 Özgür Külcü ve Metin Turan, "Kamu Hukukunda Geleneksel ve Elektronik İletişim, Bilgi ve Belge Yönetimi Uygulamaları", **Türk Kütüphaneciliği**, C. 27, No: 2, 2013.

araştırdığı kitabından istifade edilmiştir[23]. Ayrıca, e-belgelerin delil değeri üzerine çalışmalar yapan hukukçuların[24] eserleri incelenmiştir. Bununla birlikte, arşivcilik açısından delil değeri sorgulanmış; bununla ilişkili standartlar incelenmiştir. Tüm bunların yanı sıra, delillerin güvenilirliğiyle ilgili olduğu düşünülen hukuk kaynaklı standartlar da analiz edilmiştir.

İkinci bölümde e-imzalı belgelerin güvenilirlik araçları incelenmiştir. E-imza, EYP ve KEP'in güvenilirliğe katkısı analiz edilmiş, mevcut sorunların dile getirilmesine çalışılmıştır. Aynı zamanda, güvenilirliği tehdit eden unsurların ifade edilmesi yönünde çaba gösterilmiştir.

Üçüncü bölümde güvenilirliğin başarıyla korunmasında kullanılabileceği düşünülen arşivcilik ve teknolojik yöntemlerin açıklanmasına gayret edilmiştir. Arşivcilik kaynaklı olanlar, arşivsel bağı korumaya yönelik dosyalama, diplomatik analiz ve güvenilirlik üstverisidir. Teknolojik yaklaşımlardan ise e-delil elde etme yöntemleri, blokzincir teknolojisi, yapay zekâ, yapay öğrenme ve derin öğrenmenin güvenilirliğin korunmasına katkısının değerlendirilmesine çalışılmıştır.

Dördüncü bölümde saha araştırmasının sonuçları aktarılmıştır. Burada sonuçlar, nitel ve nicel olmak üzere iki kısımda açıklanmaktadır. Nitel araştırmada uzmanların görüşleri tartışılmış; nicel araştırmada ise kurumların verdikleri cevaplar değerlendirilmiştir.

Saha araştırmasının yapılması sırasında çeşitli zorluklarla karşılaşılmıştır. Araştırmanın gerçekleştirileceği dönemde tüm dünyayı etkileyen COVID-19 salgını[25] nedeniyle kamu kurumlarında alınan tedbirler gereği kurumlar yerinde ziyaret edilememiştir. Bu sorun, uzaktan video-konferans görüşmeleri yapılarak çözülmüştür.

Teze dayanılarak üç makale hazırlanmıştır. Bunlardan ilki, "e-Belgelerin

---

23 Ayşe Ece Acar, **Medeni Muhakeme Hukukunda Elektronik İmzalı Belgelerin Delil Niteliği**, İstanbul, On İki Levha Yayıncılık, 2012.

24 Mine Erturgut, "Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi", Yayınlanmamış Doktora Tezi, İzmir, Dokuz Eylül Üniversitesi, 2004. ; Mustafa Göksu, "Hukuk Yargılamasında Elektronik Delil", Yayınlanmamış Doktora Tezi, Ankara, Ankara Üniversitesi, 2010. ; Hakan Pekcanıtez vd., **Hukuk Muhakemeleri Kanunu Hükümlerine Göre Medeni Usul Hukuku**, 11. bs., Ankara, Yetkin Yayınları, 2011. ; Mustafa Serdar Özbek, **a.g.e.** ; Ertan Yardım, "Medeni Usul Hukuku Çerçevesinde Güvenli Elektronik İmzalı Belgelerin Delil Niteliği ve Unsurları", **Prof.Dr. Mustafa Dural'a Armağan**, ed.: Tufan Öğüz, İstanbul, Seçkin Yayıncılık, 2013.

25 COVID-19 salgını, 2019 yılının sonlarında Çin'in Vuhan eyaletinde ortaya çıkarak 2020 yılında tüm dünyayı etkilemiş ve milyonlarca insanın ölümüne neden olmuştur. Dünya genelinde seyahat yasakları uygulanmış, insanlar bir araya gelmemek için uzaktan çalışmışlardır. Tezin gerçekleştirildiği 2021 yılında da salgının etkileri devam etmektedir.

Arşivsel Bağının Elektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme"[26] adıyla 2017'de; ikincisi "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı",[27] adıyla 2019'da; son makale ise "Elektronik İmzalı Belgelerin Delil Değerinin Korunmasında Mevzuatta Öngörülen Delil Özelliklerinin İncelenmesi" adıyla 2020 yılında yayınlanmıştır[28].

Tezde kurumların e-imzalı belgelerin arşivsel bağının korunması, gerekli teknolojik koşulların sağlanması ve bu belgelerin güvenilirliğine yönelik politika ile prosedürlerin çıkarılmasına ilişkin uygulamaları kritik edilmiştir. Saha araştırması neticesinde elde edilen sonuçlara göre kurumların bu alandaki uygulamalarının yeterli olmadığı görülmüştür. Bu yüzden ilerleyen yıllarda arşivlenen e-imzalı belgelerin delil değerinin korunamaması riskiyle karşılaşılabileceğini ileri sürmek mümkündür.

Bu doktora tezi, kurumlarda oluşan e-imzalı belgelerin delil değerinin arşivsel güvenilirlik yaklaşımıyla nasıl korunabileceğini inceleyen ilk örneklerden biridir. Tez, yeni araştırmalara kaynaklık eder ve Türkiye'de oluşan e-imzalı belgelerin delil değerinin güçlenmesine ortam oluşturabilirse görevini yerine getirmiş sayılacaktır.

---

26 Niyazi Çiçek ve Özhan Sağlık, "e-Belgelerin Arşivsel Bağının Elektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme, **Bilgi Sistemleri ve Bilişim Yöntemi: Beklentiler ve Yeni Yaklaşımlar**, ed.: Fahrettin Özdemirci ve Zeynep Akdoğan, Ankara, Ankara Üniversitesi, 2017.

27 Niyazi Çiçek ve Özhan Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ**, ed.: Bahattin Yalçınkaya vd., Ankara, Ankara Üniversitesi, 2019.

28 Özhan Sağlık ve Niyazi Çiçek, "Elektronik İmzalı Belgelerin Delil Değerinin Korunmasında Mevzuatta Öngörülen Delil Özelliklerinin İncelenmesi", **Bilgi Yönetimi**, C. 3, No: 2, 2020.

BİRİNCİ BÖLÜM

HUKUK, ARŞİVCİLİK VE STANDARTLARDA E-BELGELERİN DELİL DEĞERİ

1.1. E-Belgelerin Delil Değeri

1.1.1. E-Belge

Örgütlerde kurumsal fonksiyonların yürütülmesi sırasında tabii olarak ortaya çıkan belgeler, hukuki açıdan işlemlerin delilini oluşturur. Önceden beri kâğıt belge üretmek yaygın bir yolken bilgi teknolojilerinin gelişmesi ve hukuki altyapının da oluşmasıyla taşıyıcı ortam, kâğıttan elektroniğe kaymaktadır. Özellikle E-İmza Kanunu gibi prosedürlerin çıkarılmasıyla hukukun kabul ettiği delil değerine sahip e-belgeler üretilmeye başlanmıştır.

Bu gelişmelerin ardından birçok kanun, yönetmelik ve standartta e-belgenin ne olduğuyla alakalı açıklamaların yanı sıra resmî tanımlar da yapılmıştır. Yapılan tanımlamalar ve açıklamalar ışığında "e-belge, elektronik ortamda bir işlemin yerine getirilmesi için oluşmuş[1]; içerik, ilişki ve formatı ile ait olduğu işlem için delil teşkil ederek aidiyet zincirini muhafaza eden, imzalanmış[2] ve kayıt altına alınmış uyuşmazlık konusu vakıaları ispata elverişli olan her türlü bilgi"[3] biçiminde ifade edilebilir. Bu özelliklere sahip e-belgelerde güvenli bir e-imzanın bulunması ön plana çıkmaktadır[4].

---

1 Kurumsal faaliyetlerle ilişkili olarak kurumda üretilen ve dışarıdan gelip dosyasına kaldırılanlar "oluşan belgeler" şeklinde nitelendirilmiştir. Tezde "üretilen belgeler" kavramı ise kurumun kendi ürettiklerini ifade edecek şekilde kullanılmaktadır (Niyazi Çiçek, **Kurumsal Bilgi ve Belge Yönetimi**, İstanbul, Marmara Belediyeler Birliği, 2018, s. 66).

2 E-belge kavramı, e-imzalı olanlarla e-imzalı olmayan fakat elektronik ortamda oluşmuş belgeleri de ifade etmektedir. E-imzalı belgelerin delil değerinin korunması için gerekli olan özellikleri araştırmak e-belgelerin de incelenmesini gerekli kılmaktadır. Bu nedenle e-belgelerin delil değeri hususiyetleri üzerinden gidilerek e-imzalı belgelerin sahip olabileceği özelliklerin incelenebileceği düşünülmüştür. Fakat bu özellikler incelenirken tek bir kanundaki belge tanımı üzerinden hareket etmenin yeteri kadar sağlıklı sonuçlar oluşturamayacağı değerlendirilmiştir. Çünkü, kanunlar ait olduğu sektöre göre tanımlamalar yapmaktadır. Mesela, Türk Ticaret Kanunu (TTK) ticari faaliyetler, Ceza Muhakemesi Kanunu (CMK) ise ceza muhakemesi bağlamında belgeleri tanımlamaktadır. Hâl böyle olunca, farklı kanunlardaki tanımların birleştirilmesi tercih edilmiştir.

3 "Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (RYY)", **R.G.**, S 31151, tar. 10.06.2020, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2020/06/20200610-8.pdf, 5 Aralık 2020. ; "Hukuk Muhakemeleri Kanunu" [HMK], Kanun No: 6100, **R.G.**, S 28736, tar. 04.02.2011, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2011/02/20110204-2.htm, 27 Nisan 2018.

4 "RYY", **a.g.e.**

E-belgeler[5], elektronik ortamdaki en küçük veri parçaları olan 0 ve 1'lerden oluşan sayı karakterlerinin karşılığı olan bitlerin bir araya gelmesiyle üretilir. Bu karakterlerin bilgisayarlar tarafından anlaşılabilmesi için American Standard Code for Information Interchange (ASCII - Bilgi Değişimi için Amerikan Standart Kodlama Sistemi) kodlarının kullanılması gerekir[6]. ASCII'de her karakterin bir bit olarak karşılığı bulunur[7]. E-belgeler, bu bitlerin ASCII kodları aracılığıyla temsil edilmesi sonucunda okunup anlaşılabilir. Mesela, "e-belge" kelimesini gösteren bit yapısı "01100101001011010110001001100101011011000110011101100101" şeklindedir. Bu kodlar, bit yapısının ekranda e-belge olarak görünmesini sağlar. Bir e-belgenin varlığı için vazgeçilmez olan bu yapı, temel delil değeri unsurlarındandır.

1.1.2. Delil Değeri

Delil kavramı, bilimden sosyal ilişkilere, kriminolojiden günlük işlemlere kadar birçok alanda kullanılmaktadır. Bir suç mahallindeki parmak izi, saç teli veya kan lekesi başlıca deliller olarak kabul edilir ve suça karışmış fail/lerin izlerini taşıdığı için sonuca ulaşma imkânı verir. Bir belgenin varlığı, gerçekliği ve özgünlüğü için de delillere ihtiyaç vardır. Örneğin belgeyi düzenleyenin ismi, kimlik tespiti aracı olarak e-imza veya elle attığı imzası, içeriği oluşturduğu yazısı başlıca delil unsurlarıdır.

Belgelerdeki delil unsurları, idari işlemlerin kim tarafından ne zaman ve nasıl yürütüldüğünü ispatlayan vasıtalar olarak karşımıza çıkmaktadır[8]. Deliller, geçmişte yürütüldüğü iddia edilen herhangi bir işlemin gerçekten meydana gelip gelmediğini tespit etmek için kullanılır[9]. Bu işlemin varlığı ya da yokluğu yazı, ses ve görüntü

---

5 Türkçe dışındaki kaynaklarda "digital records" (sayısal belge) ve "electronic records" (elektronik belge) kavramlarıyla karşılaşılmaktadır. Bu noktada, sayısal ve elektronik arasındaki ayrımı ifade etmek gerekli görülmektedir. Sayısal ortamda en küçük yapı taşı 0 ve 1'lerden oluşan ikili yapılar (bit) söz konusudur (Türkiye Bilimler Akademisi [TÜBA], **Türkçe Bilim Terimleri Sözlüğü**, (Çevrimiçi) www.tubaterim.gov.tr, 6 Haziran 2020). Bu bitler işlenerek ekranda metin veya görüntü gibi karakterler oluşmaktadır. Elektronik kavramı ise sayısal nesneleri de içermektedir. Mesela elektrik sinyalleri yoluyla üretilen radyo yayınları gibi analog kayıtlar, sayısal belge olmayıp e-belge olarak kabul edilebilir. Türkiye'de de sayısal yerine e-imza, e-devlet örneklerinde olduğu gibi elektronik kavramı daha çok benimsenmiştir. Bu nedenle İngilizce kaynaklarda digital records olarak geçen ifadeler tezde e-belge olarak kullanılmıştır.

6 Corinne Rogers, "Diplomatics of Born-digital Documents: Considering Documentary Form in a Digital Environment", **Records Management Journal**, C. 25, No: 1, 2015, s. 10-11.

7 Vint Cerf, **ASCII Format for Network Interchange**, yayım yeri yok, 1969, (Çevrimiçi) https://www.rfc-editor.org/rfc/rfc20.pdf, 29 Mart 2020.

8 Acar, **a.g.e.**, s. 4.

9 Nur Centel, **Ceza Muhakemesi Hukuku**, 9. bs., İstanbul, Beta Basım Yayınları, 2012, s. 196.

dosyası ya da güvenli e-imza ile düzenlenmiş bir kayıt ile ispat edilirken bu kaydın da gerçekten hukukun geçerli kabul ettiği belge özelliklerini barındırması gerekir. Hâliyle işlemlerin nasıl yürütüldüğünü gösteren kayıtları belge olarak değerlendirebilmek için birtakım delil hususiyetleri aranır. Bu hususiyetler, belgelerin delil değerine kaynaklık etmektedir[10].

Mevzuat hükümleri, belgelerin delil değeriyle alakalı bazı şartlar belirlemiş ve çeşitli hukuki özellikler atfetmiştir. Bu hükümler ışığında belgelerin delil değeri, irade beyanı içermek, yazılılık, gerçeklik ve sonucunda oluştuğu idari işlemin ispatını sağlamaya yönelik ilişkiyi gösterebilmek gibi özellikleri muhafaza etme kabiliyeti olarak tanımlanmaktadır[11]. Bu özellikler, kâğıt ya da elektronik taşıyıcı ortam fark etmeksizin her formattaki belge için geçerlidir. Her ne kadar, belgelerin delil değeri konusu kâğıt belgeler için çözümlenmişken elektronik ortamın kırılgan yapısı ve hızla değişmesi sebebiyle e-belgeler için tartışmalar devam etmektedir[12].

1.1.3. E-Belgelerin Delil Değeri

Kâğıt belgelerin delil değeri taşıması için gerekli olan yazılılık, hukuki sonuç doğurmaya elverişli bir içeriğin bulunması ve düzenleyenin belli olması gibi özellikler[13], e-belgeler için de geçerlidir. Bu özelliklerle birlikte, e-belgenin üretildiği teknik ve teknolojik ortam yanı sıra kullanıldığı ticaret, vergi ve noterlik gibi sahaların kendi iç düzenlemelerinden kaynaklanan nedenlerden dolayı yeni hususiyetler aranabildiği görülmektedir. Mesela e-imzalı resmî belgelerde delil değeri özellikleri güvenli e-imza ile imzalanmak; EBYS'de kayıt altına alınmış olmak, alıcı kişi ya da kuruma KEP vb. gibi bir protokol ile gönderilmek gibi hususlardır[14].

Ayrıca çeşitli sektörler, bu temel unsurlarla birlikte belgelerin ait olduğu fonksiyonları daha iyi yansıtabilmesi amacıyla farklı koşullar oluşturmuştur. Örneğin

---

10 Sağlık ve Çiçek, **a.g.e.**, s. 121.

11 Çiçek ve Sağlık, "e-Belgelerin Arşivsel Bağının Elektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme, **a.g.e.**

12 Olefhile Mosweu ve Mpho Ngoepe, "Trustworthiness of Digital Records in Government Accounting System to Support the Audit Process in Botswana", **Records Management Journal**, C. 31, No: 1, 2021. ; Rimkus, Kyle R. vd. : " Preservation and Access for Born-digital Electronic Records: The Case for an Institutional Digital Content Format Registry", **American Archivist**, C. 83, No: 2, 2020.

13 "Yargıtay Ceza Genel Kurulu Kararı", Esas No: 2016/1065, Karar No: 2017/27.

14 "RYY", **a.g.e.**

e-defter ve e-faturaları düzenleyen kanun, genelge ve tebliğ gibi mevzuatta e-belgelerin delil değeri taşıması için üstveri, form özellikleri ve kontekst gibi birtakım unsurlar aranmaktadır[15]. Bununla birlikte, Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği'nde zaman içerisinde belgenin içeriğinin bir değişime uğrayıp uğramadığının tespiti için log kayıtları gibi araçlardan yararlanılması gerektiği belirtilmektedir[16]. Adı geçen Yönetmelik ile Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik hükümlerinde ise e-belgelerin bilgi güvenliğine ilişkin uluslararası standartlara uygun olarak saklanması; risk analizi yapılarak kategorilendirilmesi ve yedeklemelerinin yapılması gibi hususiyetlere sahip olması gerektiği açıklanmaktadır[17].

Ancak, elektronik ortamda delil değeri özellikleri ilk bakışta doğrudan ve açıkça görünmeyebilir. Diğer taraftan KEP gibi birtakım farklı bileşenler de gerektirir. Mesela üniversitedeki bir personelin atama belgesini ve e-imzaları doğrulamak için belgenin üretilmiş olduğu sistemdeki doğrulama kodu üzerinden inceleme yapmak başvurulan yöntemlerden biridir. Bu belge, KEP ile gönderilmiş ise belgenin delil değerini kritik etmek için kullanılan KEP sistemi ve bu sistemin oluşturduğu kayıtların incelenmesi gerekir. Bununla birlikte, Vergi Usul Kanunu (VUK) kapsamında üretilmesi gereken bir e-belge, Kanun'un belirttiği eXtended Markup Language (XML - Genişletilebilir İşaretleme Dili) formatında olmak XML Archival Electronic Signature (XADES-A - XML Arşiv İmza) imza türü ile imzalanmak gibi özelliklere de sahip olmalıdır. Bu gibi durumlar, belgelerin delil değeri kritik unsurlarını belirlemeye çalışırken içerdiği hükümler açısından farklı kanunların araştırılması gerektiğini gündeme getirmektedir.

---

15 "Türk Ticaret Kanunu" [TTK], Kanun No: 6102, **R.G.**, S 27846, tar. 14.02.2011, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2011/02/20110214.htm, 11 Aralık 2018. ; Sağlık ve Çiçek, **a.g.e.**, s. 133-135.

16 "Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği", **R.G.**, S 29059, tar. 13.07.2014, (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2014/07/20140713-4.htm, 22 Şubat 2020.

17 Sağlık ve Çiçek, **a.g.e.**, s. 133-135. "Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği", **a.g.e.** ; "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik", **R.G.**, S 31069, tar. 15.03.2020, (Çevrimiçi) https:// www. resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm, 9 Nisan 2020. ; "Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik", **R.G.**, S 29413, tar. 11.07.2015, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2015/07/20150711-19.htm, 10 Mart 2019.

1.2. Hukuki Açıdan Belgelerin Delil Değeri

1.2.1. Türk Hukuku

Günlük işlemlerin nasıl yürütüldüğünü gösteren belgeler, hukuki bakımdan da birtakım delil değeri hususiyetlerine sahip olmalıdır. Çünkü yönetim kurulu kararlarından diplomalara, yazışmalardan yevmiye defterleri ve faturalara kadar farklı işlemler sonucunda oluşan kayıtların belge olarak nitelendirilmesi için delil değeri taşımaları gerekir. Çeşitli kanunlarda belge tanımı yapılırken delil değeri özellikleri de açıklanmıştır.

Her ne kadar Yargıtay kararlarıyla bir belgenin temel özellikleri belirlenmiş olsa da özellikle e-belgeler için kullanıldığı sahaya göre farklı nitelemeler yapılmıştır. Örneğin Hukuk Muhakemeleri Kanunu (HMK) ile Bilgi Edinme Hakkı Kanunu'nda belge, uyuşmazlık konusu vakıaları ispata elverişli bilgi taşıyıcıları olarak tanımlanmıştır[18]. Bunun yanı sıra, Damga Vergisi Kanunu'nda yazılı olmaları ve imza içermeleri gerektiği de ifade edilmektedir[19]. Türk Ceza Kanunu'na göre, usulüne uygun olarak düzenlenen, gerçeklik ve güvenilirlik içerip doğrulanabilen her türlü yazı, belge olarak kabul edilmektedir[20]. Belge, Yargıtay'ın 2017'deki bir kararında belirli bir düşünce, hukuki ilişki veya vakayı yansıtan, başka bir deyişle hukuki sonuç doğurmaya elverişli bir irade beyanını içeren ve düzenleyicisinin kim olduğunu gösteren yazılı evrak olarak tanımlanmıştır. Aynı kararda belgenin unsurları da açıklanmıştır[21]:

- Yazılı olmak
    - Bir dil ve alfabenin kullanılması,
    - Yazının bir taşıyıcı ortama kaydedilmesi,
    - Yazının elverişli bir cisme kaydedilerek taşınabilir olması
    - Yazının okunabilir olması
- Hukuki sonuç doğurmaya elverişli bir içeriğinin bulunması
- Düzenleyenin belli olması

---

18 "HMK", **a.g.e.** ; Türkiye Büyük Millet Meclisi [TBMM], **HMK Gerekçesi**, 2008, s. 63, (Çevrimiçi) https://www.tbmm.gov.tr/sirasayi/donem23/yil01/ss393.pdf, 1 Mayıs 2018. ; "Bilgi Edinme Hakkı Kanunu", Kanun No: 4982, **R.G.**, S 25269, tar. 24.10.2003, (Çevrimiçi) http:// www.mevzuat.gov.tr/MevzuatMetin/1.5.4982.pdf, 1 Mayıs 2018.

19 "Damga Vergisi Kanunu", Kanun No: 488, **R.G.**, S 11751, tar. 11.07.1964 (Çevrimiçi) http:// www.mevzuat.gov.tr/MevzuatMetin/1.5.488.pdf, 2 Mayıs 2018.

20 TBMM, **Türk Ceza Kanunu Gerekçesi**, 2003, s. 172, (Çevrimiçi) http :// www2. tbmm. gov. tr/d22/1/1-0593.pdf, 1 Mayıs 2018 ; "Türk Ceza Kanunu", Kanun No: 5237, **R.G.**, S 25611, tar. 12.10.2004, (Çevrimiçi) http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf, 1 Mayıs 2018.

21 "Yargıtay Ceza Genel Kurulu Kararı", Esas No: 2016/1065, **a.g.e.**

Yukarıdaki maddeler ışığında belirli bir düşünce veya olayın aktarımını ya da bir hukuki ilişkinin varlığını veya yokluğunu göstermek gibi hukuki sonuç doğurmaya elverişli bir irade beyanı bulunmasının belgenin delil niteliği bakımından öne çıktığı görülmektedir. O hâlde, bir yazılı kaydın belge olabilmesi için hukuki sonuç doğuracak içeriğin bulunması ve düzenleyenin belli olması gerekmektedir[22]. Hukuk açısından bakıldığında bu iki unsurun delil değeri açısından önkoşul olduğu anlaşılmaktadır[23]. Her türlü taşıyıcı ortam için aranan bu delil değeri özellikleri, e-belgeler için de geçerlidir.

Mevzuatta e-belgenin müstakil olarak açıklanması yerine, elektronik taşıyıcıların form ve format özellikleri göz önünde bulundurularak belge kavramının daha geniş tanımlanma yoluna gidildiği görülmektedir. Mesela, HMK'ya göre "uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları belgedir"[24]. Aynı şekilde, Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'te (RYY) belge, "herhangi bir bireysel işlemin, kurumsal fonksiyonun veya kurumsal işlemin yerine getirilmesi için alınmış ya da idare tarafından hazırlanmış; içerik, ilişki ve formatı ile ait olduğu fonksiyon veya işlem için delil teşkil ederek aidiyet zincirini muhafaza eden, güvenli elektronik imza ya da el yazısıyla imzalanmış ve kayıt altına alınmış her türlü bilgiyi" ifade etmektedir[25]. Bu açıklamalar ışığında elektronik ortamda üretilen kayıtlar, kâğıt ortamdaki belgelerin sahip olduğu delil değeri özellikleriyle beraber aidiyet zincirini muhafaza ettiği sürece belge olarak değerlendirilmektedir.

E-belgelerin delil değerinin incelenmesi, taşıyıcı ortam farklılığı ve hızlı teknolojik değişmelerden dolayı kâğıt belgelerden başka usulleri gündeme getirmektedir. Taşıyıcı ortam sebebiyle en başta teknik ve teknolojik niteleme ve değerlendirmeler yapılması gerektiği açıktır. Bununla birlikte, e-belgelerin üretilmesine sebep olan fonksiyonların hukuki kaynağını teşkil eden mevzuat da incelenebilir. EİK dışında E-belge Kanunu gibi müstakil bir prosedür olmadığından,

---

22 **a.e.**

23 Çiçek ve Sağlık, e-Belgelerin Arşivsel Bağının Elektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme, **a.g.e.**

24 TBMM, **HMK Gerekçesi**, **a.g.e.** ; "HMK"**, a.g.e.**

25 "RYY", **a.g.e.**

bir kanunda kapsamlı bir açıklama bulmak oldukça güçtür. Çünkü vergiden ticarete, medeni kanundan ceza kanununa kadar farklı prosedürlerde e-belgelerle ilgili çeşitli nitelemeler yapıldığı görülmüştür. Bundan dolayı, Türk hukukunda e-belgelerin delil değeriyle ilgili hükümler içerdiği düşünülen her türlü mevzuat incelemeye dâhil edilmiştir.

Bunun için özellikle EİK ardından belge, kimlik tespiti araçları ve kayıtların delil değeri bakımından güncellenen mevzuat dikkate alınmıştır. Bu bağlamda delil değeri, belgelerin şekil özellikleri, dosyalama, e-tebligat, arşivsel bağ ve risk değerlendirmesi, taşıyıcı ortamdaki form ve format değişikliğini barındıran hükümlerin olduğu mevzuat öne çıkmıştır. HMK e-belgelerin delil değeriyle, Ceza Muhakemesi Kanunu (CMK) ise delillerin özellikleriyle ilgili hükümler ihtiva ettiği için incelenmiştir. Türk Borçlar Kanunu (TBK) belgelerin şekil özellikleriyle ilgili hükümler barındırmaktadır. Türk Ticaret Kanunu (TTK) ve VUK'da ticari faaliyetler sonucunda oluşan belgelerin yapılan faaliyete göre dosyalanması gerektiği belirtilmektedir. Noterlik Kanunu, e-imza ile düzenlenecek belgelere ilişkin hükümler içerdiğinden; Tebligat Kanunu ise kurumlara yapılacak elektronik tebligatlara ilişkin hükümlerin yer alması nedeniyle analiz edilmiştir. Bankacılık Kanunu, belgelerin arşivsel bağının korunmasına; Elektronik Haberleşme Kanunu ise kurumların risk değerlendirmesine ilişkin hükümlere yer vermektedir. Sigortacılık Kanunu'nda belgelerin sahip olması gereken özellikler açıklanmıştır. Son olarak e-imzayı elle atılan imza ile aynı hukuki sonucu doğurduğunu ifade etmesi nedeniyle EİK özellikle değerlendirilmiştir.

1.2.1.1. Hukuk Muhakemeleri Kanunu

HMK, Türkiye'deki özel hukukun yargılama usûlünü belirlemekte olup medeni muhakeme hukukun temel mevzuatından biridir. Burada deliller, kesin ve takdiri olmak üzere ikiye ayrılmıştır. Kesin deliller, senet, yemin ve kesin hüküm; takdiri deliller ise bilirkişi, tanık, keşif, uzman görüşü ve kanunda düzenlenmemiş diğer delillerdir[26].

HMK'da belgeler, senet niteliğinde değerlendirilmektedir. Aynı şekilde, e-imza ile oluşturulan verilerin de senet hükmünde olduğu kabul edilmiştir[27]. O hâlde

---

26 "HMK", **a.g.e.**; Acar, **a.g.e.**, s. 8-12.

27 "HMK", **a.g.e.** Kanun'da verinin geniş anlamıyla kullanıldığı görülmektedir. Veri, bilim terimleri sözlüğünde "olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli

belgeler, senetlerin sahip olması gereken özellikleri ihtiva etmelidir. Her ne kadar HMK'da senedin delil değerine ilişkin hükümler bulunsa da bu konuda çalışma yapan hukukçuların çeşitli görüşler ileri sürdüğü bilinmektedir. Berkin'e göre senette aranan özellikler, somutluluk, yazılılık, bir irade beyanı içermek ve irade beyanının kimlik tespiti için bir imzanın bulunmasıdır[28]. Murat Yavaş ise Berkin'in görüşlerine ek olarak senetlerin Latin harfleriyle yazılmasının gerektiğini belirtmektedir[29]. Yavaş, resmî senetler söz konusu olduğunda, senedin, resmî makam veya memur tarafından düzenlenmesi; düzenlemenin, düzenleyen makam veya memurun yetkisi dâhilinde olması ve usulüne uygun olarak meydana getirilmesi gerektiğini ifade etmektedir[30]. Erturgut, elektronik ortamda üretilmiş senetler için bu özelliklere veri bütünlüğünün yani verilerin değiştirilemezliğinin sağlanmasını da eklemektedir[31].

E-belgelerde arşivsel bağın kurulamaması, teknolojik koşulların değişmesi ve yeterli kurumsal politika ve prosedürlerin tesis edilememesi nedeniyle zaman içerisinde özgünlüklerini kaybedebilme ve içeriğe ulaşamama gibi sorunlar ortaya çıkabilir. Bu ihtimal gerçekleşirse HMK'nın 203. maddesine göre tanık dinlenebilecek ya da 210. maddesi gereği bilirkişiye danışılabilecektir. Kanun'da meselenin tanık ve bilirkişi yönü bu şekilde ele alınsa da belgenin üretiminden imhasına kadar geçen süreçte korunmasında sorumlulardan biri olan arşivci ve belge yöneticileriyle ilgili bir hüküm görülememektedir.

1.2.1.2. Ceza Muhakemesi Kanunu

Ceza ile ilgili yargılamaları ve buna ilişkin mevzuat ile hukuki görüş ve mütalaaları kapsayan ceza muhakemesi, ceza konusu vakıayla alakalı somut olayların

---

biçimsel ve standart bir gösterimi" olarak geçerken, EİK'de "elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar" olarak tanımlanmaktadır (TÜBA, **a.g.e.** ; Elektronik İmza Kanunu, **a.g.e**.). Belge yönetiminde ise veriler, belgeyi meydana getiren bileşenler olarak değerlendirilmektedir (Duranti, "Structural and Formal Analysis: The Contribution of Diplomatics to Archival Appraisal in the Digital Environment", **The Future of Archives and Recordkeeping: A Reader**, ed.: Jennie Hill, Londra[Birleşik Krallık], Facet Publishing, 2011).

28 Necmettin Berkin, "İspat Hukukunda Senet Delili ve Yazılı Şekil", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. 12, No: 4, 1946. ; Acar, **a.g.e.**, s. 24-25.

29 Murat Yavaş, **Senetle İspat ve Senede Karşı İspat Kuralları ile Bu Kuralların İstisnaları**, Ankara, Seçkin Yayıncılık, 2009, s. 117.

30 **a.e.**, s. 150.

31 Erturgut, **a.g.e.**, s. 138.

delillerle temsil edilmiş şekli olan "maddi gerçeği" araştırıp bulmayı hedefler. Ceza muhakemesinde maddi gerçeğin aranmasına karşılık, medeni muhakemede kural olarak vakıanın kanunda belirtilen usuller ışığında ispatlanması anlamına gelen "biçimsel gerçeğin" tespitiyle yetinilir. Bu farklılıktan dolayı ceza muhakemesinde delil serbestîsi vardır[32]. Bu nedenle olsa gerek, CMK'da kesin ve takdiri delil şeklinde bir ayrım benimsenmemiştir. Ancak, ceza muhakemesinin bu özelliğinden kaynaklanan delil serbestîsinin sınırsız bir serbestlik olduğu düşünülmemelidir[33]. Delil olarak kullanılacak araçların bazı özelliklere sahip olması gerekir[34]:

- Deliller, uyuşmazlığı oluşturan olayın bir parçasını ispat edebilecek nitelikte ve beş duyu organımızla algılanabilecek maddi yapıya sahip olmalı,
- Deliller, hukuka uygun yollardan elde edilmeli,
- Delil, sağlam ve güvenilir olmalı, uydurulmamalı ve değiştirilmemeli,
- Mahkeme taraflarınca deliller bilinmeli (müştereklik) ve
- Delilin oluştuğu andan imhasına kadar geçen süreçte doğruluğu ve bütünlüğü sağlanmalı.

CMK'da herhangi bir delille alakalı geçerlilik kriterleri bunlar olurken, belge niteliğindeki bir elektronik kayıt (e-kayıt) için öncelikle e-imza koşulu aranmaktadır. Bundan dolayı, Kanun'un elektronik işlemler bölümünde e-imza ile ilgili hükümler bulunduğu görülmektedir. Buna göre, Kanun'da gösterilen istisnalar hariç olmak üzere e-imza ile Ulusal Yargı Ağı Bilişim Sistemi (UYAP) üzerinden her türlü ceza muhakemesi işlemi yapılabilmektedir. Fiziki olarak hazırlanması öngörülen her türlü belge, elektronik ortamda düzenlenip e-imza ile imzalanabilir ve e-imzalı bu belgeler, muhatabına elektronik ortamda gönderilir; gerekmedikçe fiziki olarak düzenlenmez. En dikkat çeken hüküm ise UYAP'taki e-imzalı belgenin elle atılan imzayla çelişmesi hâlinde UYAP'ta kayıtlı olan belgenin geçerli kabul edilmesidir[35]. Ayrıca, e-imzalı

---

32 Hamide Zafer ve Nur Centel, **Ceza Muhakemesi Hukuku**, 9. bs., İstanbul, Beta Basım Yayım, 2012, s. 7.

33 **a.e.**, s. 196-197.

34 "Ceza Muhakemesi Kanunu" [CMK], Kanun No: 5271, **R.G.**, S 25673, tar. 17.12.2004, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2004/12/20041217.htm#1, 28 Nisan 2018. ; "Yargıtay Ceza Genel Kurulu Kararı", Esas No: 1993/10, Karar No: 1993/6-79. ; "Yargıtay 9. Ceza Dairesi Kararı". Esas No: 2013/9110, Karar No: 2013/12351.

35 CMK, **a.g.e.**

belgelerde mühürleme işlemi ile kanunlarda birden fazla nüshanın düzenlenmesini öngören hükümler uygulanmamakta; zorunlu nedenlerle fiziki olarak düzenlenmiş belgeler ise yetkili kişilerce taranıp güvenli e-imza ile imzalanarak UYAP'a aktarılıp gerektiğinde ilgili birimlere elektronik ortamda gönderilmektedir[36]. Bu hükümler, Bölge Adliye ve Adlî Yargı İlk Derece Mahkemeleri ile Cumhuriyet Başsavcılıkları İdarî ve Yazı İşleri Hizmetlerinin Yürütülmesine dair Yönetmelik'te de yer almaktadır. Ayrıca, mezkûr Yönetmelik'e göre zorunluluktan dolayı fizikî olarak düzenlenmek durumunda kalınan belgeler, bu engel ortadan kalktıktan sonra derhâl elektronik ortama aktarılmalıdır[37].

1.2.1.3. Türk Borçlar Kanunu

Ekonomik ve sosyal yaşamı düzenleyen ticaret ve vergi mevzuatıyla birlikte öne çıkan bir diğer prosedür de TBK'dır. Bu Kanun, toplum içerisindeki alacak ve verecek gibi edimleri düzenlemektedir[38]. Aynı zamanda burada belgelerin sahip olması gereken niteliklere ilişkin hükümler de yer almaktadır.

Bu hükümler, daha çok sözleşmeler üzerinden açıklanmıştır. Adı geçen Kanun'da taraflar, hukuk tabiriyle "edinim" olarak tarif edilen mal mülk edinmekle alakalı işlemlerin hukuki geçerliliği için sözleşme düzenler[39]. Bu sözleşmelerden bazılarının yasal olması Kanun'da belirlenen şekil şartlarına bağlanmıştır. "Kanuni şekil" olarak adlandırılan bu koşullar, sözleşmenin yapılış biçimine göre beş başlıkta açıklanmıştır. Bunlar, sözlü, nitelikli yazılı, resmî, tescil ve ilan şeklindedir[40].

Sözlü şekilde bir hukuki işlemin ya da akdin kurulabilmesi için sözlü olarak irade beyanına ihtiyaç duyulur. Buna evlilik akdi örnek verilebilir. Yazılı şekilde ise Kanun, bazı sözleşmelerin geçerliliğini yazılı olarak yapılmaları şartına bağlamıştır. Sözleşmede bir irade beyanı bulunması ve bu irade beyanını ortaya koyanların

---

36 **a.g.e.**

37 "Bölge Adliye ve Adlî Yargı İlk Derece Mahkemeleri ile Cumhuriyet Başsavcılıkları İdarî ve Yazı İşleri Hizmetlerinin Yürütülmesine dair Yönetmelik", **R.G.**, S 29437, tar. 06.08.2015, (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2015/08/20150806-3.htm, 28 Nisan 2018.

38 Erol Cansel ve Çağlar Özel, **Borçlar Hukuku Genel Hükümler Cilt: 1**, 2. bs., Ankara, Seçkin Yayıncılık, 2017, s. 26, 37.

39 **a.g.e.**, s. 53.

40 Yalçın Kavak, "Borçlar Hukukunda Yazılı Şekil", Yayınlanmamış Doktora Tezi, İstanbul, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, 2015, s. 33.

imzasının varlığı gereklidir. Yazılı şekil, metin ve imzadan oluşmaktadır. Metin, sözleşmenin mahiyetini göstermelidir[41].

Ayrıca, TBK'da şirketlerin düzenleyeceği belgelerin diline ilişkin hükümler de yer almaktadır. Türk şirketlerin her türlü hukuki işlem, sözleşme ve ticari defterlerini Türkçe olarak düzenlemeleri zorunludur. Türkiye'de faaliyet gösteren yurt dışı kaynaklı şirketlerin de Türkiye'deki resmî makamlara ibraz edecekleri ve hukuki işlemlerde kullanacakları belgelerin Türkçe olması gerekir[42]. O hâlde, bu Kanun'a göre bir belgenin delil değerinden bahsedebilmek için belge Türkçe olmalı ve irade beyanı sahibi, kimliğini bir şekilde göstermelidir. Sözleşmelerde kimlik tespiti araçlarının en yaygın olanı ise hiç şüphesiz imzadır.

Kanun'da e-imzalı sözleşmelerin de yazılı şekil şartını taşıdığı belirtilmektedir[43]. Bunun için yazılı irade beyanına ihtiyaç duyulmaktadır. Bir irade beyanının yazılı kabul edilebilmesi için istenildiğinde ibraz edilmesi ve değiştirilemezliğinin temin edilmesi gerekir. E-imza, elektronik ortamda yapılacak sözleşmelerde kimliklerin doğruluğunu ve sözleşmenin bütünlüğünü sağladığından TBK'da e-imzalı belgelerin yazılı şekil şartını taşıdığı kabul edilmiştir[44].

Bununla birlikte, bazı hukuki işlem ve sözleşmelerin resmî şekilde yapılmaları gerektiği anlaşılmaktadır. Resmî şeklin unsurlarıyla yazılı şekil unsurları aynıdır. Mahiyet açısından bir fark bulunmayıp resmî şekilde bir kamu görevlisinin irade beyanı söz konusudur. O hâlde, aradaki fark, içerikten ziyade belgeyi düzenleyenlerden kaynaklanmaktadır. Resmî şekilde bir işlem ya da irade beyanının yetkili bir makam veya şahıs önünde, kanunların öngördüğü usul ve koşullara uyularak yapılması ya da bu makamlarca onaylanması söz konusudur. Mesela, tapu sözleşmeleri veya tapuyla ilgili değişiklikler tapu sicil memuru ve müdürü tarafından

---

41 Murat Doğan, Gökhan Şahan ve İsmail Atamulu, **Borçlar Hukuku Genel Hükümler Ders Kitabı**, Ankara, Seçkin Yayıncılık, 2019, s. 117-118.

42 Kavak, **a.g.e.**, s. 84.

43 TBK'nın "sözleşmelerin şekliyle" ilgili 15. maddesinde şu hüküm yer almaktadır: "İmzanın, borç altına girenin el yazısıyla atılması zorunludur. Güvenli elektronik imza da el yazısıyla atılmış imzanın bütün hukuki sonuçlarını doğurur". Bu maddeye göre sözleşmeler, e-imza ile imzalanabilmektedir ve ıslak imzalı sözleşmelerle aynı hukuki değere sahiptir ("Türk Borçlar Kanunu", Kanun No: 6098, **R.G.**, S 27836, tar. 04.02.2011, (Çevrimiçi) http:// www. resmigazete.gov.tr/eskiler/2011/02/20110204-1.htm, 23 Mayıs 2019).

44 "Türk Borçlar Kanunu", **a.g.e.** ; Ahmet Said Ber, **Elektronik Konişmento**, Ankara, Seçkin Yayınları, 2018, s. 64.

yapılacak düzenlemelere bağlıdır. Bunun haricinde, noterler, sulh hâkimleri ve köy ihtiyar heyetleri de tapuyla ilgili işlemlerde resmî şekil düzenleyecek makamlardandır[45].

Ayrıca, Kanun'un noterler tarafından düzenlenmesi ve onaylanmasını öngördüğü senetler de mevcuttur. Mesela, 241. maddede "satıcı veya alıcı, satış sözleşmesinin yapıldığını ve içeriğini önalım hakkı sahibine noter aracılığıyla bildirmek zorundadır" hükmü yer almaktadır[46]. Buna göre sözleşmenin noter tarafından onaylanması durumu söz konusu olmaktadır. Böylece, noterin onayı sözleşmenin resmî şekil şartlarından biri olarak karşımıza çıkmaktadır. Düzenleme şeklindeki senetler ise içerik de dâhil olmak üzere sahteliği sabit oluncaya kadar geçerlidir ve kesin delil hükmündedir[47]. Çünkü Türk Medeni Kanunu'nda (TMK) "resmî sicil ve senetlerin belgeledikleri olguların doğruluğuna kanıt oluşturduğu" belirtilmektedir[48]. Onaylama şeklindeki senetlerde ise noter onayı belge içeriğini kapsamayıp belgenin tarihi ve aidiyetini belirlemektedir. Bu onay, tarih ve imza sahteliği sabit oluncaya kadar geçerlidir[49]. Görüldüğü gibi, kanunlardan kaynaklanan gerekçelerden dolayı bazı senetlerin noterler tarafından düzenleme ve onaylama biçiminde resmî şekil şartını taşımaları gerekmektedir.

Noterler dışında da senetleri düzenleme ve onaylama şeklinde tanzim eden kurumlar mevcuttur. Mesela, sulh hâkimlikleri vasiyetname düzenlemeye yetkili kılınmıştır. Bununla birlikte, köy ihtiyar heyetine tevdi edilen bazı durumlar da söz konusudur. İmza atmaya muktedir olmayan kişilerin kullandığı işaretlerin köy ihtiyar heyeti tarafından tasdik edilmesi buna örnek verilebilir[50].

Bir diğer kanuni şekil ise tescildir. TBK, bazı hukuki işlemlerin geçerliliğini, yasa gereği tutulan resmî sicillere kayıt düşürülmesine bağlamıştır. Vakıfların vakıf

---

45 Ömer Ergün ve Coşkun Çaldağ, **Borçlar Hukuku Genel Hükümler Ders Notları**, Ankara, Seçkin Yayınları, 2019, s. 108. ; Tapu ve Kadastro Genel Müdürlüğü, **Tapu Sicili Uygulamaları**, 2014, (Çevrimiçi) https:// www. tkgm. gov. tr/ sites/ default/ files/ icerik/ ekleri/ tapu_sicili_uygulamari_2014_0_0.pdf, 9 Nisan 2020.

46 "Türk Borçlar Kanunu", **a.g.e.**

47 "Noterlik Kanunu", Kanun No: 15152, **R.G.**, S. 14090, tar. 05.02.1972, (Çevrimiçi) http :// www.mevzuat.gov.tr/MevzuatMetin/1.5.1512.pdf, 10 Mart 2019.

48 "Türk Medeni Kanunu", Kanun No: 4721, **R.G.**, S 24607, tar. 08.12.2001, (Çevrimiçi) https :// www.mevzuat.gov.tr/MevzuatMetin/1.5.4721.pdf, 23 Mayıs 2019.

49 "Noterlik Kanunu", **a.g.e.**

50 Sema Taşpınar Ayvaz, "Türk Borçlar Kanunu ve Hukuk Muhakemeleri Kanunu'nun İmza Atamayanlarla İlgili Yeni Düzenlemesine Eleştirel Bir Bakış", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C. 61, No: 1, 2012, s. 335.

siciline, şirketlerin de ticaret siciline kaydedilmesi tescil şartına örnek verilebilir. Bununla birlikte, Kanun, bazı hukuki işlemlerin ilan edilmesini öngörmüş ve işlemin geçerliliğini bu ilana bağlamıştır. Örneğin Vakıflar Genel Müdürlüğü tarafından merkezi sicile kaydedilen bir vakıf, Resmî Gazete ile ilan olunur. Bunların dışında TMK'ya göre ise vasi tayini, gaiplik, hacir ve kazai rüşt kararları da ilan edilmelidir[51]. O hâlde bu işlemler elektronik ortamda yapıldığında, belgelerin delil değerinin korunması için Ticaret Odaları ve Borsalar Birliği ile Vakıflar Genel Müdürlüğünün oluşturduğu şekil özelliklerinin incelenmesi gerekmektedir.

Görüldüğü üzere farklı sektörlere ait mevzuatta belgelerin şekil özellikleri birbirinin aynısı değildir. Bu özellikler, belge türü, yapılan iş ve mevzuata göre farklılık göstermektedir. Durum böyle olunca, e-imzalı belgelerin yazılı ve resmî şeklin şartlarını zaman içerisinde koruyup koruyamayacağı sorusu akla gelmektedir. E-belgeler üretildikten belirli bir süre sonra da şekil özelliklerini koruyabilecek mi, metin ve e-imza, belgenin mahiyetini gösterir bir biçimde muhafaza edilebilecek mi, yönetmeliklerle belirlenen resmî şeklin özellikleri korunabilecek mi gibi soruların tartışılmasına ciddi olarak ihtiyaç duyulmaktadır. Çünkü şekil şartı korunmadığı takdirde bunun müeyyidesinin butlan yani kesin hükümsüzlük şeklinde ifade edilen geçersizlik durumu olduğu ileri sürülmektedir[52].

E-imzalı belgelerin delil değeri incelemesinde kullanılan şimdilik en geçerli mekanizma e-imza kontrolüdür. E-imzada bir tereddüt oluşursa bilirkişiye başvurulabilmektedir. Bilirkişi, teknik, teknolojik ve hukuki usul ve yöntemlerle inceleme yapmaktadır[53].

1.2.1.4. Türk Ticaret Kanunu

İnsanların mal ve hizmet üretip neticesinde ekonomik sermaye oluşturdukları ticari faaliyetler, ticaret hukuku kapsamında olup TTK hükümlerine göre gerçekleştirilir[54]. Kanun kapsamındaki tüm ticari faaliyetler, birtakım işlemlerle yürütülüp, delili niteliğinde de belgeler üretildiğinden TTK'da belgelerin delil

---

51 Kavak, **a.g.e.**, s. 39, 43-44.
52 Cansel ve Özel, **a.g.e.**, s. 211.
53 Mustafa Serdar Özbek, **a.g.e.**, s. 2237.
54 İsmail Kayar, **6102 Sayılı Türk Ticaret Kanunu'na göre Ticaret Hukuku**, 5. bs., Ankara, Seçkin Yayıncılık, 2018, s. 45.

değerine ilişkin hükümler yer almaktadır. Birçok iş sürecinin e-ortama taşınmasıyla beraber ticari işlemler sonucunda oluşan belgeler de artık elektronik ortamda üretilmektedir.

Bugün e-faturadan e-irsaliyeye, elektronik ortamda hazırlanmış yevmiye defterinden icmale kadar birçok e-belge türü bulunmaktadır. TTK'da ticari defterlerde oluşturulan kayıtların eksiksiz, doğru, zamanında ve düzenli yapılması gerektiği belirtilmiştir. Kanun'un gerekçesinde geçen bilgiye göre belgede tamlık, iş ve işlemlerin eksiksiz biçimde muhasebeleştirilmesi olarak açıklanmaktadır. Tamlık kadar öne çıkan bir özellik de kayıtların doğruluğudur. Kaydın gerçeğe uygun bir biçimde iş ve işlemi yansıtması, işlemin gerçeğe uygun şekilde muhasebeleştirilmesi doğruluk anlamında kullanılmaktadır. Bunun yanı sıra, zamanındalık ve düzenlilik ilkeleri ile karşılaşılmaktadır. Zamanındalık ilkesi, muhasebe kayıtlarının en geç on (10) gün içerisinde kaydedilmesini, düzenlilik ise kayıtların zaman akışına göre tarih ve belge numarası esas alınarak yapılmasını ifade etmektedir[55].

TTK'nın 82. maddesinde tacirlerin, ticari faaliyetler sonucu oluşan belgeleri sınıflandırarak saklaması gerektiği belirtilmiş; e-belgelerin her an erişilebilir olması istenmiştir[56]. Adı geçen Kanun'a göre belgeleri düzenli bir şekilde oluşturmak kadar sınıflandırarak saklamak da önemlidir. O hâlde, belgeler, tasnif edilip ait oldukları faaliyetle ilişki kurularak dosyalanmalıdır.

Doğru, tam ve düzenli bir şekilde hazırlanıp tasnif edilerek dosyasında saklanan ve e-imza ile imzalanan ticari belgelerin kurum içi ve kurumlar arası transferi de delil değeri için önemli bir faktör olan resmî bir elektronik posta (e-posta) ile gerçekleştirilmektedir. TTK ile "tacirler arasında, diğer tarafı temerrüde düşürmeye, sözleşmeyi feshe, sözleşmeden dönmeye ilişkin ihbarlar veya ihtarlar, noter aracılığıyla, taahhütlü mektupla, telgrafla veya güvenli elektronik imza kullanılarak kayıtlı elektronik posta sistemi ile yapılabilmektedir"[57]. KEP sistemi hakkındaki hususların düzenlenmesi Bilgi Teknolojileri ve İletişim Kurumunun (BTK) uhdesine

---

55 Bumin Doğrusöz, Öznur Onat ve Funda Tunçel Toralp, **Gerekçe, Karşılaştırmalı Maddeler, Komisyon Raporları, Önergeler ve Karşılaştırmalı Tabloları ile Türk Ticaret Kanunu (Ticari İşletme, Ticaret Şirketleri Kıymetli Evrak Hükümleri): Cilt: I (Madde 1-849)**, Ankara, Türkiye Odalar ve Borsalar Birliği, 2011, s. 186-188.

56 "TTK", **a.g.e.**

57 **a.g.e.**

verilmiştir. Kayıtlı elektronik posta hizmet sağlayıcıların (KEPHS) KEP ile ilgili ürettiği kayıtlar, aksi ispat edilmedikçe kesin delil kabul edilmektedir[58].

Bu noktada e-imza mekanizması dışında KEP iletilerinin anlaşılabilirliğinin nasıl sağlanacağı merak edilmektedir. İmzalama algoritmasındaki bir güncelleme esnasında, belgedeki imza doğrulanamazsa KEP iletisinin gerçekten ilgili taraflar tarafından alındığı/gönderildiği nasıl gösterilecektir? Aynı zamanda, varlığı bilinen ancak teknik sebepler veya afet gibi olağanüstü durumlardan dolayı açılıp kullanılamayan, zayi olup olmadığından emin olunamayan e-ticari belgelerin durumu ne olacaktır?

Kanun'da kâğıt ya da elektronik ayrımı yapılmaksızın belgelerin hangi koşullarda zayi kabul edilebileceği hükme bağlanmıştır. Ancak bu hükmün donanım ve yazılım gibi e-belgeleri ilgilendiren koşullara atıf yapmadığından daha çok kâğıt belgeler için benimsendiği düşünülmektedir. Söz konusu hüküm şöyle belirtilebilir: "Tacirin saklamakla yükümlü olduğu defter ve belgeler yangın, su baskını, yer sarsıntısı gibi bir afet veya hırsızlık sebebi ile kanuni saklama süresi içinde zayi olursa tacir, zararı öğrendiği tarihten itibaren on beş gün içinde ticari işletmesinin bulunduğu yerin yetkili mahkemesinden kendisine bir belge verilmesini isteyebilmektedir"[59]. Talep edilen bu belgeye, zayi belgesi denilmektedir. Tacirin zayi belgesi alabilmesi için defter ve belgelerin, tacirin basiretli bir iş adamı gibi davranarak gerekli tüm önlemleri almasına rağmen önceden öngöremediği, engelleyemediği, olağan dışı olaylar sonucunda zayi olması gerekmektedir. Tacir, bu belgeyi alabilmek için kayıtlarını saklamak noktasında oldukça özenli olmalı ve söz konusu zayilik, tacirin kendi iradesi dışında gerçekleşmelidir. Bununla birlikte, ticari defter ve belgeler, zayiliğe söz konusu olmak için kanuni saklama süreleri olan on yıl içerisinde zayi olmalıdır[60]. Benzer etkenlerden dolayı e-ticari belgeler, zayi kabul edilebilir mi sorusu akla gelmektedir. E-imzalı belgelerin zayiliği ile ilgili bir uygulama henüz görülmemektedir.

---

58 "Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik", **R.G.**, S 28036, tar. 25.08.2011, (Çevrimiçi) http :// www. resmigazete.gov.tr/eskiler/2011/08/20110825-7.htm, 10 Mart 2019.

59 **a.e.**

60 Mehmet Ali Aksoy, "Türk Ticaret Kanunu Bağlamında Defter Tutma Yükümlülüğü", **Hacettepe Hukuk Fakültesi Dergisi**, C. 6, No: 2, 2016, s. 154-156.

1.2.1.5. Vergi Usul Kanunu

Ticari faaliyetler sonucunda oluşan ekonomik sermayeden ayrılan paylar ile devletin gerçekleştirdiği hizmetlerin finansmanı, vergi hukukunun alanını oluşturur[61]. Ticaret hukukunda olduğu gibi vergi hukukunda da işlemler, belgelere dayalı yürütülür. Bu yüzden Türkiye'deki vergi hukukunu düzenleyen VUK'da belgelerin delil değerine ilişkin çeşitli hükümler görülmektedir.

Kanun, bir hakkın ispatında delil olarak kullanılabilecek belgelerin işlerinin icabına göre dosyasında muhafaza edilmesini gerekli kılmaktadır[62]. Bu hükme göre, belgelerin delil değerinin korunması için sağlıklı bir dosyalama yapılıp arşivsel bağın kurulması gerektiği anlaşılmaktadır.

VUK'da olduğu gibi bu Kanun'a ilişkin farklı zamanlarda çıkan tebliğlerde de e-belgelerle ilgili birtakım hükümler görülmektedir. 509 nolu Genel Tebliğ'de, elektronik ortamda oluşturulacak belgelerin "mali mühür veya nitelikli elektronik sertifika taşımaya, belge üzerinde doğrulamaya, görüntülemeye ve kâğıt baskı almaya imkân veren genel bir tanınırlığa sahip bir formata sahip olması" gerektiği belirtilmiştir. Yine aynı Tebliğ'e göre, e-Arşiv Uygulamasını kendi sistemi üzerinden yönetenler, belgelere ait "elektronik kayıtların bozulması, silinmesi, zarar görmesi, işlem görememesi hâlleri ile olağanüstü durumların meydana gelmesi hâlinde, durumu Başkanlığa üç iş günü içinde bildirerek bu kayıtları nasıl tamamlayacağına ilişkin ayrıntılı bir plan sunmak zorundadır"[63]. Adı geçen Tebliğ'de e-fatura mükellefi olmayan kuruluşlara faturalar, e-fatura format ve standartları kullanılarak ve faturanın basılabilir görüntüsü eklenerek elektronik ortamda gönderilebilmektedir[64]. Tebliğ'de belirtilen e-fatura format ve standartları, Gelir İdaresi Başkanlığı (GİB) tarafından çıkarılan Elektronik Arşiv Kılavuzu ve E-Fatura Entegrasyon Kılavuzundan öğrenilmektedir. Bu kılavuzlara göre e-arşiv raporlarının XADES-A standardı

---

61 Erdoğan Öner, **Vergi Hukuku**, 11. bs., Ankara, Seçkin Yayıncılık, 2019, s. 27.

62 "Vergi Usul Kanunu" [VUK], Kanun No: 213, **R.G.**, S 10703-10705, tar. 10.01.1961-12.01.1961, (Çevrimiçi) http://www.mevzuat.gov.tr/MevzuatMetin/1.4.213.pdf, 11 Aralık 2018. 241. maddede "… gönderilen ve gelen muhabere evrakının, işlerinin icabına göre dosyada muhafaza edilmesi mecburidir" hükmü yer almaktadır. Bu hüküm, her ne kadar doğrudan arşivsel bağı ifade etmese de belgelerin ait olduğu fonksiyon ve işe göre dosyalanması arşivsel bağın gereklerinden biri olarak kabul edilmektedir (Çiçek, **Kurumsal Bilgi ve Belge Yönetimi**, **a.g.e.**).

63 "509 Sıra No'lu VUK Genel Tebliği", **R.G.**, S 30923, tar. 19.10.2019, (Çevrimiçi) https :// www. resmigazete.gov.tr/eskiler/2019/10/20191019-5.pdf, 5 Nisan 2020.

64 **a.g.e.**

kullanılarak e-arşiv uygulaması üzerinden GİB'e iletilmesi gerekmektedir[65]. Aynı idarenin yayınladığı Elektronik Arşiv Başvuru Kılavuzu'nda Bakanlığın geliştirdiği uygulama yerine kendi sistemlerini kullanmak isteyen kurumların International Organization for Standardization (ISO – Uluslararası Standartlar Teşkilatı) 27001, ISO 22301 ve ISO 2000 Standartları'na sahip olmaları gerektiği açıklanmıştır[66]. Başka bir kılavuzda, oluşturulacak e-faturaların Universal Business Language (UBL – Evrensel İş Dili) - Türkçe (TR) olarak XML dilinde, Unicode Transformation Format-8 (UTF-8 - Unicode Dönüşüm Formatı-8) biçiminde, Standart Business Document Header (Standart İş Dokümanları Başlığı) formatındaki bir zarfta ve XML Schema Definition (XSD - XML Şema Tanımı)'a uygun olarak üretilmesi hususu ifade edilmiştir. UBL dilindeki faturalar, mali mühür ile onaylanmalıdır[67]. O hâlde, mali belgelerin belirlenen format ve standartlarda üretilmesi ile çıktısı ve elektronik ortamdaki görüntüsünün aynı olması gerektiği anlaşılmaktadır. Ayrıca, e-belgeler için bir risk planı oluşturulmalıdır.

Bakanlığın geliştirdiği uygulama yerine e-faturasını kendi uygulama yazılımlarında oluşturmak isteyen kurumlar, Portable Document Format (PDF - Taşınabilir Doküman Formatı) kullanıyorsa faturayı PDF Advanced Electronic Signature (PADES - PDF Gelişmiş Elektronik İmza) standardını kullanarak mali mühürle imzalamalıdır. Fatura ekine, XML yapısındaki UBL-TR ve XSD eklenmelidir[68]. Mali mühür, verinin bütünlüğü, içeriği ve düzenleyeni gösteren ve koruma altına alan nitelikli elektronik sertifika alt yapısını ifade etmektedir[69].

VUK'da ve TTK'da bir hakkın ispatında delil olarak kullanılabilecek belgelerin işlerinin icabına göre dosyasında muhafaza edilmesi hükmü bulunmaktadır. Ancak, 509 nolu Genel Tebliğ'de her ne kadar e-faturaların delil değeriyle alakalı

---

65 Gelir İdaresi Başkanlığı [GİB], **Elektronik Arşiv Kılavuzu**, Ankara, 2021, (Çevrimiçi) https :// ebelge.gib.gov.tr/dosyalar/kilavuzlar/e-Arsiv_Teknik_Kilavuzu_V.1.12.pdf, 3 Ağustos 2021.

66 GİB, **Elektronik Arşiv Başvuru Kılavuzu**, Ankara, 2021, (Çevrimiçi) https :// ebelge. gib. gov. tr/dosyalar/kilavuzlar/e-ArsivBasvuruKilavuzu.1.5.Versiyon.pdf, 3 Ağustos 2021.

67 GİB, **E-Fatura Uygulaması Entegrasyon Kılavuzu**, Ankara, 2018, (Çevrimiçi) http :// ebelge. gib.gov.tr/dosyalar/kilavuzlar/e-FaturaUygulamasiEntegrasyonKilavuzu-v1.10.pdf, 10 Mart 2019. ; GİB, **E-Fatura Uygulaması Test Planı**, Ankara, 2017, (Çevrimiçi) http:/ ebelge. gib. gov.tr/dosyalar/kilavuzlar/e-FaturaTestPlani.pdf, 10 Mart 2019.

68 GİB, **Elektronik Arşiv Kılavuzu**, a.g.e.

69 GİB, **E-Fatura Portalı Kullanım Kılavuzu**, Ankara, 2013, (Çevrimiçi) http :// ebelge. gib. gov. tr/dosyalar/kilavuzlar/e-FaturaPortaliKullanimKilavuzu-v1.5.pdf, 10 Mart 2019.

olabilecek mali mühür ve nitelikli elektronik sertifika gibi araçlara işaret edilse de bu belgelerin belge hiyerarşisinde önemli bir basamak olan fonksiyon ve dosya konusuna pek işaret edilmemiştir. E-Fatura Portalı Kullanım Kılavuzu'nda verilen örneklerden faturaların üretim aşamasında vergi mükelleflerinin faaliyetleriyle ilişkilendirilmediği anlaşılmaktadır. Oluşturulan bir belgenin, hangi faaliyet ya da fonksiyon kapsamında üretildiği bilgisinin zorunlu bir alan olarak ele alınmadığı gözlenmektedir[70]. Aynı husus XSD şemalarında da görülmektedir[71].

E-faturalarda olduğu gibi e-biletler için de birtakım teknik gereksinimler olduğu mevzuatta belirtilmiştir. 446 nolu Genel Tebliğ[72] doğrultusunda hazırlanan kılavuzlarda e-biletlerde de XML ve XSD yapısının kullanıldığı, e-imzanın benimsendiği gözlenmektedir. Elektronik bilet ve elektronik yolcu listesinde mali mühür ya da e-imzanın XML Basic Electronic Signature (XADES-Bes - XML Basit İmza) ile havayolu ve etkinliklerde kullanılacak e-biletlerin ise XADES-A ile imzalanması gerekmektedir[73]. E-biletlerde biletin hangi üstverilere sahip olması gerektiği açıklanmıştır. Bu üstverilerden mali mühür ve e-imzanın özet değeri üstverisinde özet değerin Secure Hash Algorithms (SHA - Güvenli Özet Değeri Algoritması) 256[74] ile oluşturulması gerektiği ifade edilmektedir[75]. Ancak BTK'nın, mevcut e-imza özet değerlerini güncellediği dikkate alındığında[76], ilerleyen zamanlarda SHA 256 ile imzalanan belgelerin doğrulanmasıyla ilgili yaşanabilecek muhtemel sorunlar göz ardı edilmemelidir. E-biletlerle ilgili teknik kılavuzun bu

---

70 **a.e.**

71 GİB, **E-Fatura Uygulaması Sistem Yanıtı Şema Yapısı**, Ankara, 2017, (Çevrimiçi) http:// ebelge.gib.gov.tr/dosyalar/kilavuzlar/Ek-2e-FaturaUygulamasiSistemYanitiSemaYapisi-v1.5.pdf, 10 Mart 2019.

72 "446 Sıra No'lu VUK Genel Tebliği", **R.G.**, S 29316, tar. 04.04.2015, (Çevrimiçi) http:// www. resmigazete.gov.tr/eskiler/2015/04/20150404.htm, 10 Mart 2019.

73 GİB, **Elektronik Yolcu Listesi Raporu**, Ankara, 2020, (Çevrimiçi) https :// ebelge. gib. gov. tr/ dosyalar/ebilet/e-Yolcu_Listesi_Raporu_Teknik_Kilavuzu.pdf, 7 Ocak 2021; GİB, **E-Bilet Raporu Teknik Kılavuzu (Havayolu)**, Ankara, 2020, (Çevrimiçi) https :// ebelge. gib. gov. tr/ dosyalar/ebilet/e-Bilet_Raporu_Teknik_Kilavuzu(Havayolu).pdf, 7 Ocak 2021.

74 Verileri 256 bitlik boyutlarda özet değerlerine dönüştüren kriptografik algoritma.

75 GİB, **E-Bilet Raporu Teknik Kılavuzu (Etkinlik)**, Ankara, 2020, (Çevrimiçi) https :// ebelge. gib.gov.tr/dosyalar/ebilet/e-Bilet_Raporu_Teknik_Kilavuzu(Etkinlik).pdf, 7 Ocak 2021.

76 "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliğ", **R.G.**, S 30123, tar. 13.07.2017, (Çevrimiçi) https :// www. resmigazete.gov.tr/eskiler/2017/07/20170713-9.htm, 5 Nisan 2020. ; "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliğ", **R.G.**, S 31078, tar. 24.03.2020, (Çevrimiçi) https ://www.resmigazete.gov.tr/eskiler/2020/03/20200324-7.htm, 5 Nisan 2020.

güncellemelerin gerisinde kaldığı görülmektedir. Ayrıca, e-biletlerde hizmetin nevi kısmının zorunlu bir alan olarak benimsenmesinin biletin aidiyetinin belirlenmesine kolaylık sağlayacağı düşünülmektedir[77].

509 ve 446 nolu tebliğlerde e-biletlerde ve e-yolcu listelerinde bulunması gereken bilgiler açıklanmaktadır. Bununla birlikte, 509 nolu Tebliğ'de e-bilet ve raporlarının Türkiye'de saklanması gerektiği belirtilmiş; etkinlik biletlerinde bulunması gereken bilgiler ifade edilmiştir. 509 nolu Genel Tebliğ, sadece e-biletlerle ilgili hükümler içermemektedir. Tebliğ'de, sevk irsaliyesi, müstahsil makbuzu ve serbest meslek makbuzunun elektronik ortamda düzenlenebileceği belirtilmiş; bu belge türlerinde hangi bilgilerin bulunması gerektiği açıklanmıştır[78]. O hâlde, üretilen e-belgelerin delil değerinin korunması için Türkiye'de saklanmaları gerektiği anlaşılmaktadır.

Vergi uygulamaları kapsamında kurumların elektronik ortamda hazırladığı diğer belge türleri e-defter ve e-beratlardır[79]. Bu belgelerin bütünlüğü ve gerçekliği, e-imza ve mali mühür ile sağlanmaktadır. Ayrıca, e-defter ve e-beratlar, eksiksiz, okunabilir, anlaşılabilir ve kâğıt çıktısı alınabilir olmalı; Türkiye'de muhafaza edilmelidir[80]. 509 nolu Tebliğ, özel entegratör olarak ifade edilen GİB dışındaki kuruluşların da e-defter düzenlemek için sistemler geliştirmesini mümkün kılmıştır. Fakat bu durumda, entagratörün donanım ve yazılımının Türkiye'de bulunması zorunluluğu getirilmiştir[81].

Bununla birlikte e-defterlerle alakalı yazılımların uyumluluk onayı kılavuzunda, eXtensible Business Reporting Language (XBRL - Genişletilebilir İşletme Raporlama Dili) dili kullanılması gerekli kılınmış ve dosya boyutları, yapı gibi unsurlarla ilgili teknik zorunluluklar belirtilmiştir. E-defterlerin XBRL Global Ledger

---

77 GİB, **Elektronik Yolcu Listesi Raporu**, **a.g.e.** ; GİB, **E-Bilet Raporu Teknik Kılavuzu (Havayolu)**, **a.g.e.** ; GİB, **e-Bilet Raporu Teknik Kılavuzu (Etkinlik)**, **a.g.e.**

78 "509 Sıra No'lu VUK Genel Tebliği", **a.g.e.**

79 E-berat, 1 Sıra No'lu Elektronik Defter Tebliği'ndeki esaslar çerçevesinde e-defterlerin GİB tarafından belirlenen standartlara uygun bilgileri içeren ve yine GİB tarafından onaylanan elektronik dosyaları ifade etmektedir ("1 Sıra No'lu Elektronik Defter Tebliği", **R.G.**, S 28141, tar. 13.12.2011, (Çevrimiçi) https :// www. resmigazete. gov. tr/ eskiler/ 2011/ 12/ 20111213-10.htm, 7 Ocak 2021).

80 "3 Sıra No'lu Elektronik Defter Tebliği", **R.G.**, S 30923, tar. 19.10.2019, (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2019/10/20191019-4.htm, 7 Ocak 2021.

81 "509 Sıra No'lu VUK Genel Tebliği", **a.g.e.**

(Küresel Defter) taksonomisine göre oluşturulması gerekmektedir[82]. Kılavuzda, bir dizin yapısının benimsenerek ilgili kayıtların ait olduğu dosya içerisinde bulunması yönünde bir yaklaşım görülmektedir. Mesela bu dizin yapısında her ay gerçekleştirilen işlemlerin delili olan yevmiye ve kebir defterleri ile beratlara ilişkin belgeler, o ay için açılmış olan Ocak, Şubat, Mart gibi dosyalarda saklanmaktadır. Bu dosyalar ise ait olduğu dönemlerine göre Ocak-Aralık ya da Mayıs-Aralık gibi dosyalar içerisinde muhafaza edilebilmektedir. Bütün bunlar, en üstte "vergi kimlik numarası" adlı dosyada dizinlenmektedir. Bu dosyanın ana hizmet olan vergi işlemleri fonksiyonunu yansıttığı düşünülmektedir. Çünkü dizin yapısında bu fonksiyona ilişkin faaliyetler, Ocak, Şubat, Mart gibi ait olduğu aya göre dosyalanmıştır[83].

Bu dizin yapısının, arşivcilikte belge hiyerarşisi olarak bilinen ve belgeleri işlem, faaliyet, fonksiyon silsilesi içerisinde aralarında organik bağ kurarak dosyalayan yaklaşıma benzediği düşünülmektedir. Bu yaklaşımda, ana hizmetler fonksiyon olarak adlandırılıp seri/alt seriyi, bu fonksiyonların yürütülmesi için gerekli olan işler dosyaları, faaliyetler ve işlerin gerçekleştirilmesi sırasında oluşan belgeler de işlemleri temsil etmektedir. Bütün kurumların vergiyle alakalı dosyalarının tamamı seriyi, bir mükellefin vergi kimlik numarası altında yıllara göre ayrılan dosyaları alt seriyi, her yıla ait malzeme dosyayı, her yıl içerisindeki aylara ait föyler faaliyeti, her föy içerisinde o ay üretilen belgeler de işlemlere karşılık gelmektedir. Bu yapı, e-belge yönetimi uygulamalarında da önerilmektedir[84]. O hâlde, bilişsel bir süreç olan dosyalama mantığının[85], E-Defter Uygulaması Yazılım Uyumluluk Onayı Kılavuzu'na göre e-defterlerin yönetiminde de bir norm olarak benimsendiği anlaşılmaktadır.

VUK'un yanı sıra muhasebe işlemleriyle ilgili hususlar içeren Türk muhasebe standartlarında da belgelerin delil değeriyle ilişkilendirilebilecek özellikler görülmektedir. Buna göre, defter ve kayıtların Türkçe'den başka bir dilde tutulmayıp Türk muhasebe standartları ve international financial reporting standards (IFRS -

---

82 GİB, **E-Defter Uygulama Kılavuzu V. 1.8**, Ankara, 2021, (Çevrimiçi) http :// www. edefter. gov.tr/dosyalar/kilavuzlar/e-DefterUygulamaKilavuzu_(V_1.8)_21.05.2021.pdf, 3 Ağustos 2021.

83 GİB, **E-Defter Uygulaması Yazılım Uyumluluk Onayı Versiyon 1.8**, Ankara, 2021, (Çevrimiçi) http :// edefter. gov. tr/ dosyalar/ kilavuzlar/ e-DefterUygulamaKilavuzu _ (V_ 1.8)_21.05.2021.pdf, 15 Temmuz 2021.

84 Türk Standartları Enstitüsü [TSE], **13298 Elektronik Belge Yönetim Sistemi Standardı**, Ankara, TSE, 2015.

85 Çiçek, "Elektronik Belge Yönetimi Uygulamalarında Bir Alt Sistem Olarak Dosya Yönetimi", **a.g.e.**

Uluslararası finansal raporlama standartları)'a uyumlu bir şekilde düzenlenmesi gereklidir[86]. Türk muhasebe standartlarına göre finansal bilgi, ihtiyaca ve gerçeğe uygun olmalıdır[87]. Bununla birlikte, bilgi, anlaşılabilir olmak için sınıflandırılmalı, tanımlanmalı ve erişime sunulmalıdır. Finansal bilgilerin sınıflandırılmasında birimin yapısı ve işletmenin yürüttüğü faaliyetlerdeki rolünün açıklanmasına gayret edilir[88]. Hazırlanan bilgiler, işletmenin sürekliliğine hizmet ederek[89] güvenilir olmalıdır[90]. Aksi takdirde, ciddi sorunlara sebep olacak hatalarla karşılaşılabilir[91]. O hâlde, üretilen belgelerin doğru, tam, erişilebilir, anlaşılabilir ve tanımlanabilir olması; ait olduğu faaliyetle ilişkisi kurularak dosyalanması gerektiği anlaşılmaktadır.

Finansal bilgilerle ilgili yukarıdaki hususlar, denetim aşamasında kontrol edilir. Denetim sırasında bilgilerin güvenilirliğinden şüphe edilirse ne yapılabilir sorusu akla gelmektedir. Resmî Gazete'de yayınlanan Bağımsız Denetim Kanıtları'na göre prosedürlerin incelenip değerlendirilmesi önerilmektedir[92]. Bununla birlikte, pek çok mevzuatta belgenin fiziki ortamdaki hâliyle e-imzalı ortamdaki hâli çeliştiğinde, elektronik ortamın esas alınacağı belirtilmekteyken[93], finansal bilgilerin denetimlerinde karşılaşılan çelişkili durumlarla ilgili olarak farklı bir uygulama görülmektedir. Adı geçen Kanıtlar'da geçtiği hâliyle, bir belgenin aslından elde edilen denetim kanıtı, güvenilirliği, hazırlanması ve korunması üzerindeki kontrollere bağlı olabilen fotokopilerden, fakslardan veya filme alınmış, dijitalleştirilmiş ya da başka

---

86 Kayar, **a.g.e.**, s. 227.

87 İhtiyaca uygunluk, bilginin karar verme süreçlerine etki etmesi olarak tanımlanabilir. Gerçeğe uygunluk ise sunulan bilginin meselenin özünü anlatabilme kapasitesi olarak ifade edilebilir. Bilgi, ihtiyaca ve gerçeğe uygun olmak için karşılaştırılabilir, tam, doğrulanabilir, anlaşılabilir olmalı ve zamanında sunulmalıdır. Tamlık, bilginin ve sunumun bir olayın anlaşılması için gerekli olan tanımlamalar ve açıklamalar içermesi olarak ifade edilmektedir ("Finansal Raporlamaya İlişkin Kavramsal Çerçeve", **R.G.**, S 30578, tar. 27.10.2018, (Çevrimiçi) http:// www.resmigazete.gov.tr/eskiler/2018/10/20181027-16.pdf, 11 Mart 2019).

88 **a.e.**

89 "Emeklilik Fayda Planlarında Muhasebeleştirme ve Raporlama", **R.G.**, S 26095, tar. 01.03.2006, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2006/03/20060301-20.htm, 11 Mart 2019.

90 "Finansal Tabloların Sunuluşu", **R.G.**, S 30430, tar. 24.05.2018, (Çevrimiçi) http:// www. resmigazete.gov.tr/eskiler/2018/05/20180524-14.pdf, 11 Mart 2019.

91 "Muhasebe Politikaları, Muhasebe Tahminlerinde Değişiklikler ve Hatalar", **R.G.**, S 30450, tar. 13.06.2018, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2018/06/20180613-14.pdf, 11 Mart 2019.

92 "Bağımsız Denetim Kanıtları", **R.G.**, S 30443 Mükerrer, tar. 06.06.2018, (Çevrimiçi) http :// www.resmigazete.gov.tr/eskiler/2018/06/20180606M1-18.pdf, 11 Mart 2019.

93 CMK, **a.g.e.** ; "Noterlik Kanunu", **a.g.e.**

bir yolla elektronik ortama aktarılmış belgelerden elde edilen denetim kanıtından daha güvenilir bulunmaktadır[94].

VUK kapsamında oluşan e-defter ve e-belgelerin delil değeri teşkil etmesi için Kanun'da belirlenen şekilde tutulması ve düzenlenmesi gerekir. Bunun için "eksiksiz ve usulüne uygun olarak tutulup, açılış ve kapanış onaylarının yaptırılarak birbirini doğrulaması sağlanmalıdır"[95]. Aksi durumda güvenilirliği sorgulanabilir.

TTK ve diğer kanunlardaki hükümlere göre tutulması gereken defterleri onaylayan merci noterlerdir. Noterler, defter onaylamasını kanunlarda gösterilen şekilde gerçekleştirir. Özel bir hüküm bulunmadığı takdirde defter onaylaması, defterin başından son sayfasına kadar toplam kaç sayfa olduğunu yazmak ve her sayfasını numaralayıp mühürlemek suretiyle yapılmaktadır[96]. Elektronik ortamda düzenlenen e-defterlerde ise onay makamı noterlikler değil, GİB'tir. Onay için e-defter tutmakla yükümlü olanlar, e-defterleri nitelikli elektronik sertifika veya mali mühürle zaman damgalı imzalayıp, GİB tarafından geliştirilen e-Defter Uygulaması'na yüklemelidir[97].

1.2.1.6. Noterlik Kanunu

Noterlik, hukuki güvenliği sağlamak ve anlaşmazlıkları önlemek amacıyla farklı işlemler sonucunda oluşan belgelere resmiyet kazandıran kamu görevliliğidir. Bundan dolayı noterler tarafından düzenlenen ve onaylanan belgeler, resmî belge olarak kabul edilmektedir[98]. Noterlik Kanunu ve ilişkili mevzuatta da belgelerin delil değerine ilişkin hükümler görülmektedir.

Noterler tarafından Noterlik Kanunu'nun ikinci bölümünün hükümlerine göre düzenlenmiş olan hukuki işlemler, sahteliği sabit oluncaya kadar geçerlidir. Bunlar, düzenleme şeklinde yapılması zorunlu işlemlerdir[99]. Noter tarafından yapılan "imza onaylaması, onaylanan imzanın ilgiliye aitliğini belgelendirme niteliğinde olup hukuki

---

94 "Bağımsız Denetim Kanıtları", **a.g.e.**

95 Gümüşkaya, **a.g.e.**, s. 277.

96 "Noterlik Kanunu", **a.g.e.**

97 "3 Sıra No'lu Elektronik Defter Tebliği", **a.g.e.**

98 Süleyman Çetin ve Derya Ateş, **Avukatlık ve Noterlik Hukuku**, 2. bs., Ankara, Seçkin Yayıncılık, 2019, s. 175.

99 Niteliği bakımından tapuda işlem yapılmasını gerektiren sözleşme ve vekaletnamelerle, vasiyetname, mülkiyeti muhafaza kaydı ile satış, gayrimenkul satış va'di, vakıf senedi, evlenme mukavelesi, evlat edinme ve tanıma, mirasın taksimi sözleşmesi ve diğer kanunlarda öngörülen sair işlemler ("Noterlik Kanunu", **a.g.e.**).

işlemlerin içindekileri kapsamaz. Onaylama şeklindeki bu işlemlerde imza ve tarih, sahteliği sabit oluncaya kadar geçerlidir"[100]. Noterler tarafından düzenlenen işlerde bir tutanak tutulur. Bu tutanakta bulunması gereken bilgiler Noterlik Kanunu'nda belirtilmiştir. Bununla birlikte, onaylama şeklinde yapılan işlemler de mevcuttur. "Hukuki işlemlerin altındaki imzanın onaylanması, imzanın, imzayı atan şahsa ait olduğunun bir şerhle belgelendirilmesi şeklinde yapılır". Yine, bu işlemlerde de tutanak hazırlanır. Kanun'da tutanakta bulunması gereken bilgiler açıklanmıştır[101]. Noterler tarafından onaylanan ve düzenlenen belgelerin delil değerini koruyabilmesi için tutanaklarda yer alması gereken bu bilgiler, belgelerde de bulunmalıdır.

Noterlik Kanunu'nda kâğıt ortamda hazırlanan belgeler için içerikle beraber form özellikleriyle alakalı açıklanan bu hususiyetler, e-belgeler için de geçerlidir. Ancak, temel farklılık diğer birçok e-belge türünde olduğu gibi belgenin hazırlandığı format ile kimlik tespiti araçlarıdır. Başka bir deyişle, e-belge bilgi teknolojisi araçlar vasıtasıyla hukuki sonuç doğurmaya elverişli metin hazırlamaya uygun bir yazılımda düzenlenip uluslararası geçerliliği olan bir formatta da kaydedilir. Hazırlanan belgede yetkili kişi/lerin e-imzaları bulunur. Kanun'da işlemlerin e-imza aracılığıyla yapılmasına yönelik şu hüküm yer almaktadır:

"Noterlik Kanunu'nda öngörülen işlemler, elektronik ortamda güvenli elektronik imza kullanılarak da yapılabilir. Ancak, düzenleme şeklinde yapılması zorunlu tutulan işlemler ile irade beyanlarının alınmasına ilişkin işlemlerde güvenli elektronik imza kullanılabilmesi için ilgililerin noter huzurunda olmaları gerekir. Güvenli elektronik imza ile imzalanmış belgelerde, kanunlarda belirtilen mühürleme işlemi uygulanmaz ve ayrıca suret aranmaz. Güvenli elektronik imza ile oluşturulan belge, talep edilmedikçe ayrıca fiziki olarak düzenlenmez. Elektronik ortamdan fiziki örnek çıkartılması gereken hâllerde, belge, aslının aynı olduğu belirtilerek noterlikçe imzalanır ve mühürlenir. Güvenli elektronik imza ile imzalanmış belgenin elle atılan imzalı suretiyle çelişmesi hâlinde noterlerin kullandığı bilişim sisteminde kayıtlı olan güvenli e-imzalı belge esas alınır"[102].

---

100 **a.g.e.**

101 Noterin adı ve soyadı, noterliğin ismi, işlemin yapıldığı yer ve tarih, ilgili kişinin veya tercüman, tanık, bilirkişinin kimlik ve adresleri ile Türkiye Cumhuriyeti kimlik numaraları, ilgilinin arzusu hakkındaki beyanı, işleme katılanların ve noterin imzası ile noterin mührü (**a.e.**).

102 **a.e.**

Durum böyle olunca, herhangi bir sebeple, e-imzası doğrulanamayan belgelerin delil değerinin nasıl inceleneceği akla gelmektedir. E-imzanın yanında belgelerin noterlik faaliyetleri sonucunda oluştuğunu gösterebilecek başka mekanizmaların da kullanılabileceği düşünülmektedir. Belgelerin diplomatik özelliklerinden hareket edilerek oluşturulacak tanımlama bilgilerinden faydalanılabileceği kabul edilmektedir[103].

Noterler, elektronik ortamda tespit işlemleri de yapmaktadır. Bu tespit işlemi, "bir donanımdaki veya internet ortamındaki verinin tespiti işlemi ile o verinin belirli bir anda ya da zaman aralığında o anki veya zaman aralığındaki hâlinin değişmez olarak belirlenmesi, tekrar edilebilir hâlde tutulması ve saklanması" şeklinde ifade edilmektedir[104]. Acaba ilerleyen yıllarda e-imzalı belgelerin tespit işlemleri için noterler, arşivci ve belge yöneticilerini bilirkişi olarak mı tayin edecek ya da bu kişileri Türkiye Noterler Birliği (TNB)'nde mi görevlendirecektir? Çünkü noterliklere ait evrakın korunması ve saklanması için ortak tedbirler almak aynı zamanda TNB'nin görevleri arasındadır.

Noterler tarafından elektronik ortamda yapılan tüm işlemlere dair bilgi ve belgeler, Türkiye Noterler Birliği Bilişim Sistemi'nde (TNBBS) kaydedilir ve saklanır. Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik ile güvenli e-imzayla yapılan tüm noterlik işlemlerinde zaman damgası kullanılması zorunludur. TNB, elektronik ortamda güvenli e-imza ile işlem yapılmasına imkân sağlayacak altyapıyı kurmak ve işletmekten sorumludur. Bunun için gerekli standartlar ve şartları belirler. İlgili Yönetmelik'te bu konuda şöyle bir hüküm bulunmaktadır[105]:

"Noterlerdeki işleme katılanların tamamının güvenli elektronik imzası ile elektronik ortamda yapılan bir işlem için talep edilmedikçe fizikî olarak belge düzenlenmez ve bu işleme ilişkin olarak elektronik ortam dışında bir saklama yapılmaz. Bu kayıtlar, iş sürekliliği ve bilgi güvenliğine ilişkin uluslararası kabul görmüş standartlara uygun olarak yedekli ve güvenli bir şekilde saklanır. Sistem tarafından tutulacak iz bilgilerinin kapsamı, Birlik tarafından belirlenir".

---

103 Sevil Pamuk, "Türkiye'de Noter Belgelerinin Form Özellikleri", Yayınlanmamış Doktora Tezi, İstanbul, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı, 2014.

104 "Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik", **a.g.e.**

105 **a.e.**

TNB, aynı zamanda iz bilgilerinin güvenliği, gizliliği ve bütünlüğünü sağlamakla görevlidir. Bu Yönetmelik gereğince elektronik ortamda yapılan işlemlere ilişkin bilgi ve belgeler, Noterlik Daireleri Arşiv Hizmetleri Hakkında Yönetmelik hükümlerine ve "iş sürekliliği ve bilgi güvenliğine ilişkin uluslararası kabul görmüş standartlara uygun olarak yedekli ve güvenli bir şekilde TNBBS'de saklanır"[106]. Bu hükümlerden hareket edildiğinde e-imzalı belgelerin delil değerinin korunmasının daha çok teknolojik bir mesele olarak algılandığı düşünülmektedir.

1.2.1.7. Tebligat Kanunu

Sözlüklerde bildirim olarak açıklanan tebligat, "hukukî işlemlerin kanunun öngördüğü esas ve usullere uygun olarak yetkili makam tarafından muhataba bildirilmesi ve bu bildirimin belgelendirilmesi" olarak ifade edilmektedir[107]. Tebligatın belgelendirme unsurunun bulunması ona çeşitli şekil özellikleri yüklemiştir. Bu nedenle Tebligat Kanunu ve ilgili yönetmelik hükümlerinde belirlenen şekilde yapılmamış ve belgelendirilmemiş tebligatlar, geçerli kabul edilmemektedir[108].

Tebliğ, kâğıt ortamında yapılabildiği gibi elektronik olarak da gerçekleştirilebilir. Fakat elektronik ortamda yapılan her tebligat, hukukî sonuç doğurmamakta; mevzuatın öngördüğü kurallar ışığında yapılan tebliğ işlemleri hukuken geçerli kabul edilmektedir[109]. 2018 yılında çıkarılan Elektronik Tebligat Yönetmeliği ile pek çok kamu ve özel kuruma tebligatın elektronik yollarla yapılması bir zorunluluk hâline gelmiştir[110]. Elektronik ortamda tebligat, ilgili Yönetmelik hükümlerine göre yapılır.

Adı geçen Yönetmelik'te e-tebligat işlemlerinin gerçekleştirilmesi için Posta Telgraf Telefon (PTT) Anonim Şirketi tarafından bir sistem kurulması gerektiği belirtilmektedir. Buna istinaden PTT, Ulusal Elektronik Tebligat Sistemi (UETS)'ni kurmuştur. Tebligat Kanunu gereği, tebligat oluşturmaya yetkili makam ve merciler, tebligatı UETS'ye yükler ve UETS, bu mesajı zaman damgasıyla ilişkilendirerek

106 **a.e.**

107 Murat Atalı, İbrahim Ermenek ve Hilal Üçüncü, **Tebligat Hukuku**, 3. bs., Ankara, Seçkin Yayınları, 2020, s. 18.

108 **a.g.e.**, s. 19-20.

109 **a.g.e.**, s. 57.

110 "Elektronik Tebligat Yönetmeliği", **R.G.**, 30617, tar. 06.12.2018, (Çevrimiçi) http :// www. resmigazete.gov.tr/eskiler/2018/12/20181206-2.htm, 10 Mart 2019.

muhatabın adresine iletilmesini sağlar. Hem mesajın yüklenmesi hem de muhatabın mesajı aldığına dair kayıtlar, UETS'de muhafaza edilir. Yönetmelik'te, tebligatın adı geçen sistem tarafından teslim alındığı, muhatabına gönderildiği, muhatap tarafından okunduğu ve usulen tebliğ edilmiş olduğuna dair üretilen ve e-sertifika ile imzalanan kayıtlar, delil kaydı olarak tanımlanmaktadır. Bu kayıtlar, aksi ispat edilmedikçe kesin delil sayılırlar. Elektronik Tebligat Yönetmeliği'nde bu işlem ve delil kayıtlarının 30 yıl boyunca erişilebilir, güvenli ve gizli bir şekilde bütünlük içerisinde saklanması gerektiği hüküm altına alınmıştır[111]. Tebligatla ilgili bu delil kayıtlarının saklama süresi, gerek EBYS'ler için geliştirilen saklama planlarında gerekse arşivlerde muhafaza edilirken göz önünde bulundurulmalıdır.

UETS'yi kurmak, işletmek, sistemin güvenliğini ve sistemde kayıtlı verilerin muhafazasını sağlamak PTT'nin görevidir. E-tebligata ilişkin ana ve yedek sistemler, Türkiye'de bulunmalıdır. PTT, e-tebligatların imzalanmasında kendisi için oluşturulan nitelikli sertifikayı kullanmalı ve delil kayıtlarının doğrulanması hizmetini sunmalıdır. PTT'nin UETS'nin yukarıda belirtilen kriterler ışığında çalışması için gerekli önlemleri alması benimsenmişse de bu konuda bir teknik rehberin hazırlandığı henüz görülememektedir[112].

1.2.1.8. Bankacılık Kanunu

Dünyadaki fon kaynaklarının transferini sağlamak amacıyla ciddi miktarda parayla bankacılık faaliyetleri gerçekleştirilmekte ve finansal işlemler yapılmaktadır. Bu işlemler, belgelere dayanarak yürütülmektedir. Söz konusu işlemlerin hilesiz yapılacağına dair bir güven ortamının tesisine ihtiyaç duyulduğundan çeşitli denetimler uygulanmakta, bunların nasıl olacağı bankacılıkla ilgili kanunlarda düzenlenmektedir[113]. Türkiye'deki Bankacılık Kanunu ve ikincil düzenlemelerde faaliyetlerin delili olan belgelerin sahip olması gereken bazı özellikler ifade edilmektedir. Burada dikkat çeken ilk hüküm şöyledir[114]:

---

111 **a.e.**

112 **a.e.**

113 Aysel Gündoğdu, **Bankacılık Hukuku**, 6. bs., Ankara, Seçkin Yayıncılık, 2019, s. 21.

114 "Bankacılık Kanunu", Kanun No: 5411, **R.G.**, S 25983 Mükerrer, tar. 01.11.2005, (Çevrimiçi) http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5411.pdf, 18 Şubat 2019.

"Alınan yazılar ve faaliyetler ile ilgili belgelerin asılları veya bunun mümkün olmadığı hâllerde sıhhatlerinden şüpheye mahal vermeyecek kopyaları ve yazılan yazıların makine ile alınmış, tarih ve numara sırası verilerek düzenlenecek suretleri, usûlleri çerçevesinde ilgili banka nezdinde on yıl süreyle saklanır. Bu belgelerin mikrofilm, mikrofiş şeklinde veya elektronik, manyetik veya benzeri ortamlarda saklanmaları mümkündür".

Bankacılık faaliyetlerine ilişkin e-belgelerin delil değerinin korunması için gerekli olan bir diğer özellik ise sıhhatlerinden şüpheye mahal vermemektir[115]. Ayrıca, belgelerin evrak kayıt sistemine tarih, numara ve konusu belirtilerek kaydedilmesi zorunludur[116]. Buradan, bankacılık faaliyetlerine ilişkin belgelerin bir tarih, numara ve konuya sahip olması sonucu ortaya çıkmaktadır.

Her ne kadar Bankacılık Kanunu'nda banka işlemlerindeki belgelerin delil değeriyle alakalı belirtilen bu hususların göz önünde bulundurulması gerektiği ifade edilse de yine bankacılık işlemleriyle ilgili diğer prosedürlerde belgelerin zamanında[117], doğru[118] ve okunabilir hâlde denetime sunulup güvenilir bir şekilde muhafaza edilerek[119] her zaman erişilebilir[120] olması gerektiği vurgulanmaktadır. Ayrıca, 15 Mart 2020 tarihinde yayımlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'te "bilgi sistemlerine ilişkin işlemlerin doğruluğu ve güvenilirliği asgari olarak, yapılmak istenen işleme ait anahtar öneme sahip bilgilerin işlemin başlangıcından tamamlanışına kadar doğruluğunu

115 Kanun'da bu özellik açıklanmasa da bunun belgenin özniteliklerinin zaman içerisinde korunması olarak değerlendirilebileceği düşünülmektedir.

116 "Bankaların Muhasebe Uygulamalarına ve Belgelerin Saklanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik", **R.G.**, S 26333, tar. 01.11.2006, (Çevrimiçi) http:// www. resmigazete. gov.tr/eskiler/2006/11/20061101.htm, 19 Şubat 2019.

117 "Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ", **R.G.**, S 28841, tar. 04.12.2013, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2013/ 12/ 20131204.htm, 18 Şubat 2019.

118 "Ödeme ve Menkul Kıymet Mutabakat Sistemlerinde Kullanılan Bilgi Sistemleri Hakkında Tebliğ", **R.G.**, S 29588, tar. 09.01.2016, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2016/01/20160109.htm, 18 Şubat 2019.

119 "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun", **R.G.**, S 28690, tar. 27.06.2013, (Çevrimiçi) http:// www. mevzuat.gov.tr/MevzuatMetin/1.5.6493.pdf, 18 Şubat 2019.

120 "Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmelik", **R.G.**, S 29043, tar. 27.06.2014, (Çevrimiçi) http :// www. resmigazete.gov.tr/eskiler/2014/06/20140627.htm, 18 Şubat 2019.

yitirmemesini ve yapılmak istenen işlemin kendinden beklenen sonucu yerine getirmesini; tamlığı ise asgari olarak bütün işlemlerin hata üretmeden gerçekleşmesini ve mükerrer olamamasını gerektirir" hükmü dikkat çekmektedir[121]. Yönetmelik'teki bu hükümden anlaşıldığına göre belgeler bütünlük, tutarlılık, güvenilirlik, doğruluk ve hesap verebilirlik koşullarına sahip olmalıdır.

Mezkûr Yönetmelik'te, e-imzalı belgelerin delil değerinin zaman içerisinde korunmasıyla ilişkilendirilebilecek yaklaşımlar görülmektedir. Bilgi sistemleri yönetiminin kurumsal yönetimin bir parçası olduğu ve bilgi sistemleri stratejisi ile iş hedeflerinin uyumlu olması gerektiği dile getirilmektedir. Ayrıca, bilgi sistemlerinin yönetimiyle ilgili birimler, yönetsel hiyerarşi içerisinde uygun yere yerleştirilmeli; gerekli finans ve insan kaynağı tahsis edilmelidir. Bununla birlikte, Yönetmelik'te bu konuda politika ve prosedürlerin hazırlanması ile risk yönetimine ihtiyaç duyulduğu belirtilmektedir. İlgili mevzuatta, risk yönetiminde dikkate alınabilecek unsurlar açıklanmaktadır. Bunlar, teknolojik gelişmeler, hizmet alımı, işlem kayıtları, güvenilirlik ve bilgi güvenliği önlemleri şeklindedir. Bilgi güvenliğinin sağlanmasında, belgelerin gizlilik, bütünlük ve ulaşılabilirliklerine dikkat edilmesiyle güvenlik hassasiyetlerine göre sınıflandırılıp uygun düzeyde güvenlik kontrollerinin tesis edilmesi ve sızma testlerinin gerçekleştirilmesi gibi yaklaşımlar önerilmektedir[122]. Yönetmelikte sergilenen bu yaklaşımlar, e-belgelerin delil değerinin korunmasının daha çok teknolojik bir mesele olarak algılandığını düşündürmektedir.

1.2.1.9. Elektronik Haberleşme Kanunu

Her ne kadar Elektronik Haberleşme Kanunu, haberleşme alt yapısı, şebeke ve hizmet alanlarında teknolojik gelişime ilişkin usul ve esasları düzenlemiş[123] olsa da belgelerin delil değeriyle alakalı hükümlere daha çok Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği'nde rastlanmaktadır. İşletmecilerin sahip oldukları varlıkları dokümante ettikleri varlık envanteri için şu hüküm yer almaktadır[124]:

---

121 "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik", **a.g.e.**

122 **a.e.**

123 "Elektronik Haberleşme Kanunu", Kanun No: 5809, **R.G.**, S 27050 Mükerrer, tar. 10.11.2008, (Çevrimiçi) https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf, 22 Şubat 2020.

124 "Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği", **a.g.e.**

"Asgari olarak varlığın adı, tipi, yeri, yedekleme bilgisi, değeri, sorumlusu ve kimlik bilgileri bulunur. Varlıklar, gizlilik sınıfı, kritiklik derecesi, yasal gereksinimler ile hassasiyet kriterlerine göre etiketlenir. Ayrıca, erişim, kullanım, depolama, iletim, imha, paylaşım ve dağıtım kuralları da belirlenir".

Bununla birlikte, işletmeciler, elektronik ortamda tutulan bilgilerin yetkisiz olarak erişilmesi, değiştirilmesi, silinmesi ve zarar görmesine karşı gerekli önlemleri almalıdır. Bunun için öncelikle hangi yetkilinin nelere erişip erişemeyeceği belirlenir. İmha edilmesi gereken bilgiler, geri döndürülemez şekilde silinmelidir. Mükellefler, e-belgelerle alakalı bu uygulamalar için bilgi teknolojileri yazılım ve donanım hizmetlerini gerçekleştirerek, şebeke kurarak ve bilgi güvenliği yönetim sistemi tesis ederek koşulları sağlamalıdır[125].

Bu mevzuata göre, felaket ya da hata durumları karşısında yedekleme yapılmalıdır. Bunun için ihtiyaçlar ve sistemlerin kritiklik seviyesine uygun olarak yedekleme periyodu, yedekleme türü ve saklama zamanı belirlenir. Yedekleme aşamasında, yedek kopyaların kaydı tutulur; yedekler birbirinden farklı yerlerde saklanır ve periyodik olarak test edilir[126].

Adı geçen Yönetmelik'te tutulacak sistem kayıt dosyalarıyla ilişkili hükümler bulunmaktadır. Buna göre, kullanıcı kimlikleri, oturum açma ve kapatma, veri ekleme/silme/değiştirme gibi işlemlerin tarihi, zamanı ve açıklamaları, erişimin sağlandığı teçhizatın kimliği, sistem, veri ve diğer kaynaklara başarılı ya da reddedilmiş erişim girişimleri, sistem ayarlarındaki değişiklikler, kullanılan özel izinler ve ayrıcalıklar, kullanılan sistem araçları ve uygulamaları, erişilen dosyalar ve erişim tipi, ağ adresleri, güvenlik sistemlerinin aktif ve pasif hâle getirilmeleri, güvenlik ayarları ve kontrollerine ilişkin değişiklikler veya değişiklik girişimleri, sistem yöneticileri tarafından yapılan işlemler ve rapor edilen sistem hatalarını içeren

---

125 Elektronik haberleşme hizmeti sunan ve/veya şebekesi sağlayan ve altyapısını işleten şirketler yani işletmeciler, bilgi güvenliği yönetim sistemi kurmakla mükellef kılınmıştır. Bu sistem, bilginin gizliliği, bütünlüğü ve erişilebilirliğini sağlamalı; bunlarla birlikte kuralları belirlenmiş, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, yönetimce onaylanmış ve uluslararası güvenlik standartlarına uyumlu olmalıdır. Bunun için işletmeciler, öncelikle bilgi güvenliği yönetim sistemi politikası oluşturmalıdır. Burada uygulanan güvenlik politikaları, prosedürler, kurallar, prensipler ve standartlar hakkında genel bilgiler verilir. Risk değerlendirmesi yapılarak varlıklar sınıflandırılmaktadır (**a.e**).

126 **a.e.**

log kayıtlarının en az 2 yıl süre ile saklanması gerekmektedir[127]. Buradaki hususların, EBYS'lerde tutulan log kayıtları ve denetim günlüklerinde bulunması gereken özellikler için yol gösterici olabileceği düşünülmektedir.

1.2.1.10. Sigortacılık Kanunu

İnsanların ve kurumların günlük yaşamda çeşitli risklere maruz kalması ve bu risklerin gerçekleşmesi neticesinde ciddi ekonomik zararların oluşması, sigorta fikrini ortaya çıkarmış ve sigortacılık gelişmiştir[128]. Tüm gelişmiş ve gelişmekte olan ülkelerde olduğu gibi Türkiye'de de sigortacılık sektörünün güvenli ve istikrarlı bir ortamda etkin bir şekilde çalışmasını temin etmek için Sigortacılık Kanunu hazırlanmıştır. Adı geçen Kanun'a göre kamu kurum ve kuruluşları, birlikler ile sivil toplum kuruluşları, denetim amaçlarına uygun olarak sigortacılıkla ilgili bilgi işlem sistemlerini erişime açmalı ve verilerin güvenliğini sağlamalıdır[129].

Kanun kapsamında hazırlanan yönetmeliklerden biri olan Sigortacılık Bağımsız Denetim İlkelerine İlişkin Yönetmelik'te, konuyla alakalı önemli hükümler görülmektedir. Yönetmelik'e göre denetimlerde, faaliyetlere ve finansal tablolara ilişkin her türlü belgenin içeriği ve kayıtlara uygunluğu ayrıntılı bir şekilde incelenmektedir. Her bir muhasebe kaydı, bir belgeye dayandırılmaktadır. Bu kayıtlar, aynı zamanda denetçilerin de erişimine açılmaktadır. Eğer kayıtlar, bilgi işlem sistemleri tarafından oluşturuluyorsa denetçiler, sistemin kayıtları nasıl oluşturduğunu, kayıtların iş süreci ile sistemde nasıl kontrollerden geçtiğini araştırır. Çünkü denetçiler, güvenilir kanıtlar derlemek zorundadır. Bunun için denetime konu olan kayıtlar, mevzuata uygun hazırlandıklarına dair güven oluşturacak bir açıklık taşımalıdır.

Bununla birlikte, etkin kontrol sistemlerinin hataları azalttığı, yapısal zayıflıkların ise hataları artırdığı belirtilmektedir[130]. O hâlde, e-belgelerin güvenilirliği için belgelerin yaşam döngüsünde hangi kontrollerin benimsendiğini açıklayan araçlar kullanılmalıdır. Bu araçlar, belgelerin delil değerini güçlendirecek mahiyette olmalıdır.

---

127 **a.e.**

128 Barış Günay, **Sigorta Hukuku**, Ankara, Seçkin Yayıncılık, 2019, s. 17.

129 "Sigortacılık Kanunu", Kanun No: 5684, **R.G.**, S 26552, tar. 14.06.2007, (Çevrimiçi) https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5684.pdf, 23 Şubat 2020.

130 "Sigortacılık Bağımsız Denetim İlkelerine İlişkin Yönetmelik", **R.G.**, S 26934, tar. 12.07.2008, (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2008/07/20080712-7.htm, 23 Şubat 2020.

1.2.1.11. Elektronik İmza Kanunu

Kurumlar, faaliyetlerini elektronik ortama taşırken bu faaliyetlerin birer delili olan belgeleri de bu ortamda üretmek için e-imza gibi güvenilir bir araca ihtiyaç duymaktadır[131]. E-imza, bir veri birimiyle ilişkilendirilen, onaylama ve veri bütünlüğü mekanizması olarak işlev gösteren, onaylayanın inkâr edemeyeceği kriptografik veri iletimidir[132]. İdari işlemlerin delili olan belgeler de bir kimlik tespiti aracı olan e-imzayla imzalanarak bütünlüğü sağlanmış, inkâr edilemeyecek şekilde düzenleyeni belli edilmiş olur.

E-imzanın hukuken tanınabilmesi için BM tarafından United Nations Commission on International Trade Law (UNCITRAL - Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu), AB tarafından Electronic Identification, Authentication and Trust Services (eIDAS – Elektronik Kimlik Belirleme ve Güven Hizmetleri) mevzuatı çıkarılmış, Türkiye'de de 2005 yılında EİK yayınlanmıştır[133]. Bu Kanun, e-imzanın hukukî yapısı, elektronik sertifika sağlayıcılarının faaliyetleri ve e-imzanın kullanımına ilişkin hükümler içerir[134]. E-belgeler, ıslak imzalı belgeler ile aynı delil değerini taşımak için güvenli elektronik imza ile imzalanmalıdır.

Güvenli elektronik imza, sadece imza sahibine bağlı olan ve imza sahibinin tasarrufundaki güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifika aracılığıyla imza sahibinin kimlik tespitine imkân veren ve imzalanmış elektronik veride sonradan değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imza olarak

---

131 Gonca Hülya Selçuk, **E-Devlet Uygulamaları için Elektronik İmza Formatları**, (Çevrimiçi) http://www.kamusm.gov.tr/dosyalar/makaleler/EDevletUygulamalariIcinElektronikImzaFormatlari.pdf, 29 Şubat 2020.

132 Bralic, Kules ve Stancic, **a.g.e.**, s. 90.

133 "Model Law on Electronic Signatures", **United Nations Commission on International Trade Law (UNCITRAL)**, 2001, (Çevrimiçi) https :// www. uncitral. org/ pdf/ english/ texts/ electcom/ ml-elecsig-e.pdf, 24 Mayıs 2018. ; Elektronik İmza Kanunu, **a.g.e.** ; Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repailing Directive, **Official Journal [OJ]**, L 257/73, tar. 28.08.2014, (Çevrimiçi) https :// eur-lex. europa. eu/ legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN, 15 Mart 2020.

134 E-imza, zaman damgası ve elektronik sertifika ile ilgili hizmetleri sağlayan gerçek ve tüzel kişiler, elektronik sertifika hizmet sağlayıcısı (ESHS) olarak tanımlanmıştır. ESHS'ler, hizmetin güvenilir bir biçimde yürütülmesinden sorumludur ("Elektronik İmza Kanunu", **a.g.e.**). ; 2004/21 ve 2006/13 sayılı genelgelerle kamu kurumları için ESHS olarak Kamu Sertifikasyon Merkezi (KAMU SM) belirlenmiştir ("2004/21 sayılı Başbakanlık Genelgesi", **R.G.**, S. 25575, tar. 06.09.2004, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2004/ 09/ 20040906.htm#8, 15 Mart 2020. ; "2006/13 sayılı Başbakanlık Genelgesi", **R.G.**, S. 26144, tar. 19.04.2006, (Çevrimiçi) https :// www. resmigazete. gov. tr/ eskiler/ 2006/ 04/ 20060419-5. htm, 15 Mart 2020).

tarif edilmektedir[135]. Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurmaktadır. Fakat kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukuki işlemler (tapu alım-satımı, evlilik akdi gibi) ile banka teminat mektupları dışındaki teminat sözleşmeleri, güvenli elektronik imza ile imzalanamamaktadır[136].

Elektronik ortamda hazırlanan kayıtların belge olabilmesi için temel mekanizma olan bu kimlik tespiti aracının imza oluşturma ve doğrulama özelliklerinin incelenmesi gerekli görülmektedir. EİK'de açıklanan hükümlere göre güvenli elektronik imza oluşturma aracı, ürettiği imza oluşturma verilerini eşsiz kılmalı, bunların gizliliğini ve üçüncü kişilerce elde edilemeyip kullanılamamasını sağlamalı ve e-imzayı sahteciliğe karşı korumalıdır[137]. Güvenli elektronik imza doğrulama araçları ise imza sahibinin kimliğini, imzanın doğrulanması için kullanılan veriler ile doğrulama işlemini güvenilir biçimde çalıştırmalıdır. Doğrulama sonuçlarını değiştirmeksizin olduğu gibi göstermeli ve imzalanmış verileri güvenilir bir biçimde sunabilmelidir. Bunun yanı sıra bu doğrulama aracı, kullanılan elektronik sertifikanın geçerliliğini güvenilir bir biçimde tespit ederek sonuçları değiştirmeksizin doğrulama yapan kişiye göstermelidir[138].

1.2.2. Delil Değerine İlişkin Ortak Hükümler

"E-belge kanunu" gibi müstakil bir kanun olmadığından, arşivlenen e-imzalı belgelerin taşıması gereken delil değeri özellikleri kanunlar ve yönetmelikler arasında değişiklik gösterebilmektedir. Mevzuatın birleştiği ortak kriterler açısından kabul edilen delil değeri özellikleri yanı sıra, prosedürün çıktığı ve kullanıldığı sahaya göre de özel hususiyetlerle karşılaşılabilmektedir. Bundan dolayı, e-imzalı belgelerin delil değerine ilişkin hususları mevzuat açısından üç kategoride ele almanın mümkün olduğu görülmüştür: Bunlardan ilki, bütün prosedürlerde geçtiği düşünülenler; ikincisi çoğunluğunda yer alanlar; üçüncüsü ise sahaya göre özel hususiyetlerdir.

Bütün prosedürlerde ortak olan özelliklerde elektronik ortamda düzenlenen bir kaydın, ıslak imzalı belgelerle eş değer kabul edilebilmesi için zaman damgalı güvenli

135 **a.e.**
136 **a.e.**
137 **a.e.**
138 **a.e.**

e-imzanın bulunmasının ilk belirleyici unsur olduğu görülmektedir. Bununla birlikte, düzenleyenin belli olması, hukuki sonuç oluşturabilecek bir içeriğe sahip olmak, ait olduğu işlemin gerektirdiği form özelliklerini taşımak gibi kriterler, hemen hemen bütün mevzuatta yer almaktadır. Bundan dolayı, belirtilen kriterlerin belgenin delil değeri bakımından ortak özellik olarak kabul edilebileceği düşünülmektedir.

Bu ortak özelliklerin yanı sıra, bir kısım mevzuatta bulunup diğerlerinde geçmeyen bilgi güvenliği, dosyalama ve belgelerin Türkiye'de saklanması gibi normların mevcut olduğu görülmektedir. Yedekleme ve sızma testleri türünden işlemlerin, bilgi güvenliğinde olduğu gibi kabul edilmiş standartlara göre yapılması gerektiği vurgulanmaktadır. Ayrıca elektronik ortamda bulunan belgelerin gerek ulusal gerekse uluslararası kriterlere göre güvenliğinin sağlanması gerektiği birçok mevzuatta ortak hüküm olarak geçmektedir.

Bütün prosedürlerde ortak olarak geçmeyip çoğu mevzuatta yer aldığından delil değeri unsuru olarak kullanılabilecek özelliklerden biri de dosyalamadır. Dosyalama işi, TTK'da "... belgeleri sınıflandırılmış bir şekilde saklamakla yükümlüdür" denilerek; VUK'da ise belgelerin "icabına göre dosyada muhafaza edilmesi mecburidir" ifadesiyle bir norm olarak benimsenmiştir. Görüldüğü üzere dosyalamanın fonksiyona göre yapılması gerektiği özellikle belirtilmektedir.

Çoğu prosedürde yer aldığı görülen delil değerine ilişkin ortak özelliklerden sonuncusu ise belgelerin Türkiye'de saklanmasıdır. VUK ve Tebligat Kanunu'na göre e-imzalı belgeler, Türkiye'de muhafaza edilmelidir.

Bu ortak özelliklere karşın, farklı kanun ve yönetmeliklerde özel hükümlerin bulunduğu görülmektedir. Örneğin TBK, e-belgelerin delil değeriyle alakalı hükümleri açıklarken yazı dilinin Türkçe olması ve ait olduğu faaliyet alanını düzenleyen prosedürlerdeki şekil özelliklerini taşıması gerektiğini belirtmektedir. Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği hükümlerine göre ise belgenin tür ve formatı, gizlilik sınıfı, erişim, depolama ve imha gibi kuralların kayıt altına alındığı varlık envanterinin oluşturulması gerektiği anlaşılmaktadır. Bu niteliklerin yanı sıra politika ve prosedürler hazırlayıp risk analizi yapmak gibi süreçlere Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'te rastlanmaktadır. Delil değeriyle alakalı hususiyetlerin

kullanıldığı sahaya göre kanundan kanuna, yönetmelikten yönetmeliğe farklılıklar gösterebildiği anlaşılmaktadır.

Her ne kadar, belgenin delil değeri konusunda mevzuatta ortak özellikler kadar farklılıklar bulunsa da EBYS'lerde oluşan e-imzalı bir belgenin nitelikleri şöyle tarif edilebilir: Elektronik vasıtalar aracılığıyla kullanılmaya elverişli bir cisme kaydedilen, işlemlerin doğruluğunu belirtme yetkisine sahip makam tarafından usulüne göre düzenlenmiş e-imzalı belgeler, okunabilir, anlaşılabilir, doğrulanabilir ve güvenilir olmalıdır. Bunlar, kurumun elektronik belge yönetim sistemlerinde kayıt altına alınıp güvenli e-imza ile oluşturulurlar. Belgelerin içerik, ilişki ve formatını koruyup ait olduğu fonksiyon veya işlem için delil teşkil etmesi hedeflenir. Böylece, e-imzalı bir belge aidiyet zincirini muhafaza ederek belirli bir düşünce, hukuki ilişki veya vakayı yansıtır. Aynı zamanda e-imzalı bir belge, doğduğu faaliyet alanını düzenleyen prosedürlerdeki şekil özelliklerini taşır. Bu niteliklere göre oluşan belgeler içerik, ilişki ve formatı ile ait olduğu fonksiyon için delil teşkil edecek bir şekilde erişime sunulur. Bununla birlikte, belgeler risk analizleri yapılarak bilgi güvenliğine ilişkin uluslararası standartlara uygun olarak saklanıp yedeklenmelidir. Bu süreçlerin log kayıtlarında yer alması gerekir.

1.2.3. Seçilmiş Ülkelerin Mevzuatı

Belgelerin delil değeri özellikleriyle alakalı olarak farklı ülkelerin mevzuatına bakılmış, hukuk literatüründeki tartışmalar da incelenmiştir. Literatürde Avrupa Birliği (AB) ülkeleri, Amerika Birleşik Devletleri (ABD), Kanada, Malezya, Çin ve

Hindistan gibi ülkelerdeki[139] çalışmaların ön plana çıktığı görülmüştür[140]. İncelenen ülkelerin bir kısmında ortak özellikler bulunduğu gözlenmiş, Fransa'da ise özel hükümlerin olduğu dikkat çekmiştir.

İncelenen AB ülkeleri ile Kanada ve ABD gibi devletlerin hukuk sistemleri farklılık gösterse de belgelerin delil değeri taşıması için aranan özelliklerin benzerlikler içerdiği görülmektedir. Bunlar, belgelerin ulusal ya da uluslararası standartlara uygun olarak üretilmesi[141], oluşan belgelerin dosya planı kodu alarak girmeleri gereken dosyayla ilişkilendirilmesi[142] ve belgelerin aidiyet zincirini

---

139 Bu ülkelerin müşterek hukuk (common law) veya Kıta Avrupası (civil law) gibi farklı hukuk sistemlerine sahip oldukları görülmektedir. Mesela AB ülkeleri, Kıta Avrupası hukuk sistemine sahipken, ABD, Avustralya ve Yeni Zelanda gibi ülkelerde müşterek hukuk sistemi geçerlidir. Common law ifadesinin, Türkçe'ye Anglo-Amerikan, Anglo-Sakson ve ortak hukuk gibi ifadelerle çevrildiği görülmektedir. Fakat, müşterek hukuk tanımlamasının daha kapsayıcı olduğu belirtilmektedir (Meltem Dündar, "İngiliz ve Türk Ceza Muhakemesi Hukuklarında Hukuka Aykırı Deliller", Yayınlanmamış Doktora Tezi, İstanbul, İstanbul Üniversitesi Sosyal Bilimler Enstitisü Kamu Hukuku Anabilim Dalı, 2014, s. 3). Müşterek hukuk ve Kıta Avrupası hukuk sistemleri arasında delillerin sunumu ve ispat gücü, hâkimin rolü ve duruşmanın usulü gibi temel farklılıkların söz konusu olduğu ifade edilmektedir (Ayşe Gülin Güralp, "Anglo-Amerikan ve Kıta Avrupası Medeni Yargılama Sistemlerindeki Yeni Gelişmeler ve Türk Hukuku ile Karşılaştırılması", Yayınlanmamış Doktora Tezi, İzmir, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, 2010, s. 5-11, 148-157).

140 Luciana Duranti ve Corinne Rogers, "Trust in Digital Records: An Increasingly Cloudy Legal Area, **Computer Law & Security Review**, No: 28, 2012, s. 522-531. ; David Stephens, "Legal Issues", **Managing Electronic Records**, ed.: Julie McLeod ve Catherine Hare, Londra[Birleşik Krallık], Facet Publishing, 2005, s. 102. ; Jonathan Herbest ve Simon Lovegrove, "Moves towards a Common Regulatory Framework for Financial Services in the European Union", **Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra[Birleşik Krallık], Facet Publishing, 2011, s. 45-46. ; Ed Sautter, "Conflicts of Laws in Multiple Jurisdictions", **Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra[Birleşik Krallık], Facet Publishing, 2011, s. 17, 20.

141 "Canada Evidence Act", **Revised Statutes of Canada**, 1985, Chapter 5, (Çevrimiçi) http :// laws-lois.justice.gc.ca/eng/acts/C-5/, 20 Mayıs 2018. ; Canadian General Standards Board [CGSB], **National Standart of Canada: Electronic Records as Documentary Evidence**, Gatineau[Kanada], CGSB, 2017. ; Luciana Duranti, Corinne Rogers ve Anthony Shepperd, "Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later", **Archivaria**, No: 70, 2011. ; Ken Chasse, "Electronic Records for Evidence and Disclosure and Discovery", **Criminal Law Quarterly**, No: 57, 2011. ; "Code of United States, Title 44, Chapter 31, Records Management by Federal Agencies", (Çevrimiçi) **Government Publishing Office [GPO]**, https :// www. govinfo. gov/ content/ pkg/ USCODE-2011-title44/ pdf/ USCODE-2011-title44-chap31.pdf, 23 Mayıs 2018. ; Code of United States", Title 44, Chapter 21, National Archives and Records Administration, **GPO**, (Çevrimiçi) https :// www. gpo. gov/ fdsys/ pkg/ USCODE-2016-title44/ pdf/ USCODE-2016-title44-chap21. pdf, 26 Mayıs 2018. ; Antoine Meissonnier ve Françoise Banat-Berger, "French Legal Framework of Digital Evidence", **Records Management Journal**, C. 25, No:1, 2015, s. 100.

142 Michael H. Dore, "Forced Preservation Electronic Evidence and the Business Records Hearsay Exception", **Columbia Science and Technology Law Review**, No: 76, 2010, s. 85-86. ; "Federal Rules of Evidence", **GPO**, (Çevrimiçi) https:// www. uscourts. gov/ sites/ default/ files/ evidence-rules-procedure-dec2017_0.pdf, 23 Mayıs 2019. ; Maria Guercio, "The Italian Case:

yönetebilmek için tasarlanmış prosedürlerin hazırlanması gibi hükümlerdir[143]. Bununla birlikte, belgeler güvenli bir e-arşiv sisteminde saklanarak[144] ileride formatı bozulmayacak şekilde muhafaza edilmelidir[145]. Tüm bunların belgelerin yaşam döngüsündeki süreçleri ortaya koyup delil değeriyle ilgili bilgileri açığa çıkarması için üstverilerden yararlanıldığı görülmektedir[146].

İncelenen ülkelerde delil değerine ilişkin bu hususiyetler ortak özellik olarak öne çıkarken, Fransa'da arşivlenen e-belgelerle alakalı özel hükümler ortaya konulduğu gözlenmektedir. Bunlar, e-belgelerin kurum arşivlerinden devlet arşivine devri sırasında bulunması gereken normlar olarak karşımıza çıkmaktadır. Bu normlar, kullanılan yazılım ve donanım özelliklerinin belge bütünlüğüne zarar vermeyecek nitelikte olması, gerçekleştirilen teknolojik göç işlemlerinin kayıt altına alınması ve bu sürece ilişkin işlemlerin dokümantasyonunun oluşturulmasıdır[147].

Legal Framework and Good Practices for Digital Preservation", **Policies for Recordkeeping and Digital Preservation: Recommendations for Analysis and Assesment Services**, ed.: Stefano Allegrezza vd., yayım yeri yok, yayımcı yok, 2016, s. 30.

143 **a.g.e.**, s. 28. ; "Code of Federal Regulations", Title 36, Chapter XII, Subchapter B Records Management, **GPO**, (Çevrimiçi) https :// www. gpo. gov/ fdsys/ pkg/ CFR-2017-title36-vol3/ pdf/CFR-2017-title36-vol3-chapXII-subchapB.pdf, 24 Mayıs 2018. ; Mursilalaili Mustapa Sa'di vd., "Authentication of Electronic Evidence in Cybercrime Cases Based on Malaysian Laws", **Pertanika Journal of Social Sciences & Humanities**, C. 23, s. 159-165.

144 Meissonnier ve Banat-Berger, **a.g.e.**, s. 97-101. ; Regan Adams, "Information Privacy in the USA", **Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra[Birleşik Krallık], Facet Publishing, 2011, s. 79-80, 85. ; Mike Breen, "Nothing to Hide: "Why Metadata Should Be Presumed Relevant", **University of Kansas Law Review**, No: 56, 2008.

145 National Conference of Commissioners on Uniform State Laws, **Uniform Electronic Legal Material Act**, 2011, (Çevrimiçi) http:// www. uniformlaws. org/ shared/ docs/ electronic %20legal%20material/uelma_final_2011.pdf, 14 Ekim 2018. ; Aradya Sethia, "Rethinking Admissibility of Electronic Evidence", **International Journal of Law and Information Technology**, C. 24, No: 3, 2016, s. 229-250. ; "Décret n° 2017-719 du 2 mai 2017 relatif aux services publics d'archives, aux conditions de mutualisation des archives numériques et aux conventions de dépôt d'archives communales", **Journal Officiel de la Republique Française (JORF - Fransa Cumhuriyeti Resmî Gazetesi)**, S. 95, 4 Mayıs 2017, (Çevrimiçi) https:// www. legifrance. gouv. fr/ affichTexte. do; jsessionid= 0B75 F6F5 67F3 B039 148A 0DF7 317A EDCB. tplgfr29s_ 2?cidTexte = JORF TEXT 0000 3456 7704 &dateTexte= 2017 05 04, 14 Ekim 2018.

146 Meissonnier ve Banat-Berger, **a.g.e.**, s. 100-101. ; Lucy L. Thomson**, Admissibility of Electronic Documentation as Evidence in U.S. Courts**, 2011, s. 15-18, 28-29, (Çevrimiçi) http://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf, 14 Ekim 2018. ; Terrance K. Bryne, "Time for an Upgrade- Amending the Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation", **Journal of Law and Health**, C. 28, No: 379, 2015, s. 385.

147 Fransa'da bu hususların açıklandığı görülmektedir. Bunlar, kullanılan yazılım ve donanımla ilgili dokümantasyon, belgelerin bütünlüğünün sağlanmasına ilişkin prosedürler, kullanılan formatların eskimesi durumunda gerçekleştirilecek teknolojik göç işlemleriyle ilgili benimsenecek ilkeler, elektronik arşivde kullanılan zaman damgası vb. gibi bütünlük tespiti

Her ne kadar Fransa örneğinde olduğu gibi arşivlenen e-belgelerin delil değerine ilişkin özel hükümler bulunsa da ülke mevzuatlarında tanımlanabilirlik, bütünlük, tamlık, gerçeklik, doğrulanabilirlik ve erişilebilirlik gibi ortak özelliklerin ön plana çıktığı görülmektedir. Bu ortak özelliklerin belirlenmesinde Birleşmiş Milletler gibi bir çatı kuruluşun 2000'li yılların başında çıkardığı Elektronik Ticaret Model Kanunu ve Elektronik İmza Model Kanunu gibi mevzuatın etkili olduğu düşünülmektedir. Çünkü, bilgi teknolojisinin gelişmesiyle küreselleşen dünyada çok uluslu şirketlerin artması ve e-ticaretin yaygınlaşmaya başlamasıyla bu faaliyetler sonucunda oluşan e-belgelerin sahip olması gereken ortak özelliklerin belirlenmesi ihtiyacı doğmuştur. Bunun neticesinde ülkeleri bağlayacak bir prosedürün çıkarılması gündeme gelmiş ve BM tarafından adı geçen mevzuat hazırlanmıştır[148].

BM'nin yanı sıra bir diğer çok uluslu kuruluş olan AB'nin de e-belgelerin delil değeriyle ilgili hükümler belirlemeye çalıştığı bilinmektedir. Belgelerin delil değeri taşıması için sahip olması gerektiği ifade edilen bu ortak özelliklerin AB mevzuatında da yer aldığı görülmektedir[149]. Örneğin 251/9 (2004) numaralı Avrupa Birliği Komisyonu kararında Komisyon birimlerinde işlem gören elektronik ortamda üretilmiş ve sayısallaştırılmış belgelerin sahip olması gereken hususiyetler

araçları ve bilgi güvenliğiyle ilgili dokümantasyon şeklinde belirlenmiştir ("Annexe au décret n° 2011-573 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine (Décrets en Conseil d'Etat et en conseil des ministres) et au décret n° 2011-574 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine (livres Ier à VI)", **JORF**, S. 186, 26 Mayıs 2011, (Çevrimiçi) https:// www. legifrance. gouv. fr/ affichTexte. do; jsessionid= 0B75 F6F5 67F3 B039 148A 0DF7 317A EDCB. tplg fr29s_ 2?cidTexte= JORF TEXT 0000 2423 2917 & date Texte=20110526, 14 Ekim 2018). ; Ancak, her ülkede bu açıklamaların yapılmadığı anlaşılmaktadır. Örneğin Çin'deki e-belgelerin delil değeriyle ilgili yürütülen bir çalışmada arşive devredilecek belgelerin sahip olması gereken özelliklerin belirlenmesine ihtiyaç duyulduğu ifade edilmektedir (Weimei Pan ve Luciana Duranti, "Sitting in Limbo or Being the Flaming Phoenix: The Relevance of the Archival Discipline to the Admissibility of Digital Evidence in China", **Archives and Manuscripts**, C. 48, No: 3, 2020, s. 310).

148 "Model Law on Electronic Commerce", **UNCITRAL**, 1996, (Çevrimiçi) https :// www. uncitral. org/ pdf/ english/ texts/ electcom/05-89450_Ebook.pdf, 24 Mayıs 2018; "Model Law on Electronic Signatures", **a.g.e.** ; Stephens, **a.g.e.**, s. 106-110.

149 Mustafa Yılmaz, "Elektronik İmzalı Belgelerin Karşılaştırmalı Hukukta ve İdari Yargılama Hukukunda Delil Niteliği", **Marmara Üniversitesi Hukuk Fakültesi Araştırmaları Dergisi**, C. 22, No: 3, 2016, s. 3431-3441. ; Oliver Leroux, "Legal Admissibility of Electronic Evidence", **International Review of Law, Computers & Technology**, C. 18, No: 2, 2004, s. 200-201. ; "Commission Decision of 23 January 2002 amending its Rules of Procedure", **OJ**, L 21/23, 23.01.2002, (Çevrimiçi) https: // eur-lex. europa. eu/ legal-content/ GA/ TXT/ ?uri= CELEX: 3200 2D0047, 25 Nisan 2019. ; **Policies for Recordkeeping and Digital Preservation: Recommendations for Analysis and Assesment Services**, ed.: Stefano Allegrezza vd., yayım yeri yok, yayıncı yok, 2016, s. 19. ; **OJ**, L 317/3, 29.11.2011, (Çevrimiçi) https :// publications. europa.eu/s/lhdE, 25 Nisan 2019.

belirlenmiş; bilgi güvenliği önlemlerinin alınması, belgelerin bütünlüğü ve okunabilirliğinin muhafaza edilerek saklanması şeklinde açıklanmıştır[150].

E-belgelerin delil değerine ilişkin farklı ülkelerin mevzuatı ve ülkelerin üye olduğu uluslararası örgütlerin kararlarında belirlenen bu özellikler, belgenin güncel kullanım süresinde şekillense de e-arşiv boyutunda da aranmalıdır. Böylece belgeler, yaşam döngüsü boyunca korunabilir. Bunun için söz konusu hususiyetleri korumaya yönelik yöntemler belirlenebileceği düşünülmektedir. Bu koruma yöntemleri ise tasnif edilerek gruplandırılacak özellikler üzerinde uygulanabilir. Adı geçen tasnif, belgeler, teknolojik koşullar ve kurumsal politika ile prosedürler şeklinde yapılabilir.

Belgelerle ilgili hususlarda belgenin usulüne uygun olarak düzenlenmesi öne çıkmaktadır. Bunun için belge özgün, gerçek, tam ve kullanılabilir olmalıdır. Bununla birlikte, belgelerin tasnif edilerek saklanması ve ait olduğu faaliyet ve fonksiyonla ilişki kurularak dosyasında tutulması gerekir. Böylece belge, üstveri, format ve ilişkisel özelliklerini koruyarak aidiyet zincirini muhafaza edebilir.

Teknolojik koşullarla ilgili hususlara ise belgenin standartlara uygun bir e-belge yönetim sisteminde kayıt altına alınması, üretildiği sistemin bütünlüğünün sağlanması, periyodik olarak yedekleme yapılması ve log kayıtlarının düzenli bir şekilde oluşturup saklanması örnek verilebilir. Kurumsal politika ve prosedürlerle alakalı niteliklerde ise belirlenen belge ve arşiv yönetimi politikası, prosedürler aracılığıyla uygulanmalıdır.

E-belgelerin delil değeriyle ilgili bu hususlar, hukuk kurallarında açıklanan unsurlardır. Ancak, bu kurallara bir hak, yetki ya da sorumluluğun kötüye kullanılması durumunda başvurulmaktadır. Diğer bir ifadeyle hukuk ilmi belgelerin delil değerine ilişkin hususları uyuşmazlık yaşanan somut olaylar üzerinden inceler. Bu olaylar, incelenen belgenin düzenleyen, içerik, aidiyet zinciri gibi özniteliklerini korumadığı hakkında şüpheye düşülmesi ya da belge ile ilgili sahtecilik iddiaları gibi vakalar olabilir.

Hukuk kuralları, bu olayları incelerken bir e-belgenin delil olarak değerlendirilebilmesi için düzenleyen, hukuki sonuç doğuracak bir içerik, kanunların emrettiği şekil özellikleri, aidiyet zinciri, güvenilirlik, doğrulanabilirlik, gerçeklik ve

---

150 "Commission Decision of 7 July 2004 amending its Rules of Procedure", **OJ**, L 251/9**,** 07.07.2004, (Çevrimiçi) https://publications.europa.eu/s/lhdF.

tamlık gibi unsurları arar[151]. Hukuk ilminin getirdiği bu delil değeri unsurlarının yanı sıra başka yaklaşımlar geliştiren disiplinler de bulunmaktadır. Bunlar arasında arşivcilik ve belge yönetimi gibi alanlar öne çıkmaktadır. Çünkü bu alanlar, uyuşmazlık konusu olsun olmasın kurumsal faaliyetlerin delili olması nedeniyle üretilen belgelerin özniteliklerinin korunmasını hedefler. Bundan dolayı bu iki disiplin, belgenin üretiminden imhasına kadar geçen süreçte delil değerinin korunması için hukuk kurallarının e-belgeler için belirlediği delil değeri unsurlarının yanı sıra başka hususiyetler de aramaktadır.

E-belgelerin güncel kullanım safhasındaki delil değeri özellikleri belge yönetiminin alanına girer. Bu özellikler, belgedeki işlemin gerçekleştirilmesinden sorumlu kişiler, belgeyi üreten, üretildiği/alındığı tarih, içerik ve arşivsel bağ gibidir[152]. Belge yönetiminde, bu hususiyetlerin belgenin oluşumundan arşive devrine kadarki süreçte değişmemesi hedeflenir. Belge, bu özelliklerinin güncel kullanım süresinde değişmediği onaylanarak arşive devredilir[153]. Arşivlenen bu belgelerde teknolojik zorunluluktan dolayı format değişikliği, e-imza algoritmasının güncellenmesi, teknolojik göç ettirme gibi işlemler söz konusu olabilir[154]. Ancak, bunları şekillendiren düzenleyen, içerik ve kontekst gibi unsurların belge arşiv malzemesi olmadan önce, güncel kullanım safhasında kimliklendirilerek kayıt altına alınması gerekir[155]. Çünkü arşivlenen e-belgelerin delil değeri, belgeler arşive devredilmeden önce güncel kullanım safhasındaki koşullarla şekillenmektedir.

1.3. Arşivlenen E-Belgelerin Delil Değeri

1.3.1. Delil Değeri Tartışmaları

1.3.1.1. E-Belge Bileşenlerinin Korunamaması Riski

Günümüzde EBYS'lerde yaygın olarak Portable Document Format Archive (PDF/A - Arşiv Taşınabilir Doküman Formatı), Tagged Image File Format (TIFF -

151 Sağlık ve Çiçek, **a.g.e.**, s. 133-135.

152 Heather MacNeil vd., "Requirements for Assessing and Maintaning the Authenticity of Electronic Records", **The Long-term Preservation of Authentic Electronic Records: Findings of the INTERPARES Project**, s. 3-7, (Çevrimiçi) http:// www. interpares. org/book/interpares_book_k_app02.pdf, 28 Aralık 2020.

153 **a.g.e.**, s. 3.

154 **a.g.e.**, s. 7-8.

155 **a.g.e.**, s. 3.

Etiketlenmiş Görüntülü Dosya Formatı), JPEG (Joint Photographic Experts Group - Birleşik Fotoğraf Uzmanları Grubu) gibi formatlarda belge üretildiği görülmektedir[156]. Her ne kadar bu e-belge formatları yaygın endüstri standartları olsa da zaman içerisinde ne gibi değişikliklere uğrayacakları hâlâ kestirilememektedir. Bunun sebepleri olarak taşıyıcı ortamın teknolojik ihtiyaçları yeteri kadar karşılayamaması ve uygulama yazılımlarının güncellenmesi gibi nedenler ileri sürülmektedir. Bundan dolayı, bugün PDF formatındaki bir belgenin ilerleyen yıllarda yeni bir formata dönüştürülmesi gerekebilir. Hâl böyle olunca, belgenin delil değeri unsurlarından olan form özellikleri ve içerik gibi bileşenler yeni formata nasıl aktarılacak, kontekstin bozulmaması sağlanabilecek mi ve belgenin bit yapısı korunabilecek mi soruları gündeme gelmiştir[157].

Bu bileşenler muhafaza edilemezse delil değeri korunamayacağından belgelerin hukuki geçerliliği sorgulanabilir. Bu çekinceler, yeni formata dönüşen belgelerde bunların nasıl korunacağı tartışmalarını gündeme getirmiştir. Durum böyle olunca, saha uzmanları bu tartışmaya çözüm olması için birtakım görüşler ileri sürerek destek olmaya çalışmışlardır. Bunlardan bir tanesi, e-belgeleri oluşturan bileşenlerin yeniden tanzimi şeklindedir. Bit yapısının olduğu gibi muhafazası yerine, -her ne kadar belgenin ilk üretildiği gibi orijinal hâli olmasa da- söz konusu bileşenler korunarak belge yeniden tanzim edilebilir[158]. Böylece hukukun geçerli kabul ettiği, delil değerini

---

156 Türkiye Cumhuriyeti Kalkınma Bakanlığı Bilgi Toplumu Dairesi, **e-Dönüşüm Türkiye Projesi: Birlikte Çalışabilirlik Esasları Rehberi**, Ankara, Sürüm 2.1., 2012, s. 13, (Çevrimiçi) http:// www. bilgitoplumu. gov. tr/ wp-content/ uploads/ 2014/ 04/ Birlikte_ Calisabilirlik_ Esaslari_ Rehberi_ 2.1.pdf, 8 Mart 2020.

157 INTERPARES, **INTERPARES 2: Experiential, Interactive and Dynamic Records**, ed.: Luciana Duranti ve Randy Preston, 2008, (Çevrimiçi) http:// www. interpares. org/ ip2/ display_file.cfm?doc=ip2_book_complete.pdf, 28 Aralık 2020.

158 Bu belge, reprodüksiyon olarak tanımlanmaktadır. Bu tanımlamanın nedeni, e-belgelerin ilk oluştuğunda meydana gelen bit yapısının korunmasının mümkün olamamasıdır. 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 (**a.g.e.**, s. 120. ; Kenneth Thibodeau, "Wrestling with Shape-Shifters: Perspectives on Preserving Memory in the Digital Age", **The Memory of the World in the Digital Age: Digitization and Preservation. An International Conference on Permanent Access to Digital Documentary Heritage**, 26-28 Eylül 2012, ed.: Luciana Duranti ve Elizabeth Shaffer, Vancouver[Kanada], UNESCO, 2013, s. 12-13, 15-17). Fakat bu husus, e-imzalı belgelerin düzenlenmesinden yani imzalanmasından sonra geçerli değildir. E-imzalı belgelerde, belge imzalandıktan sonra belgenin yeni bir bit yapısına kavuşması mümkün gözükmemektedir. Çünkü e-imza o anki bit yapısını değişmeyecek

hâlâ muhafaza eden aynı belgenin tekrar oluşturulabileceği fikri gündeme gelmiştir. Bu fikir, bileşenleri korunmuş bir belgeye dayanılarak orijinaline en yakın nüshanın düzenlenebileceğini ileri sürmektedir[159]. Bunun neticesinde, belgenin saklanan hâli (stored record) ve sunulan hâli (manifested record) olmak üzere bir ayrım yapılmıştır[160]. Belgenin saklanan hâli, delil değeri unsurlarından olan form özellikleri, belgedeki kişiler, faaliyet, kontekst, arşivsel bağ ve içerik gibi bileşenlerin korunduğu belgeyi, belgenin sunulan hâli ise orijinale en yakın nüshayı ifade etmektedir[161]. Bu ayrım, arşivlenen e-belgelerin delil değeri tartışmalarında adı geçen bileşenlerin korunamaması riskinden kaynaklanmaktadır.

Her ne kadar bu riskler, e-belgelerin uzun süre saklandıklarında format değişikliği sırasında gündeme gelse de birtakım vakalar, güncel uygulamalarda da benzer problemlerin yaşanabileceğini göstermektedir. Mesela Kanada'da yapılan bir incelemede e-belgelerde kullanılan üstverilerin konteksti açığa çıkarmak için yetersiz olduğu anlaşılmıştır[162]. Bununla birlikte, ABD Başkanlık Ofisi ile The National Archives and Records Administration (NARA - Amerika Milli Arşivi ve Belge Yönetimi İdaresi) arasında yaşanmış bir ihtilaf dikkat çekmektedir. Bu ihtilafın

---

bir şekilde şifrelemektedir. Bu nedenle e-imza, e-belgelerin orijinalliğini koruyan bir mekanizma olarak benimsenmiştir. Fakat e-imzalı belgelerin formatının değişmesi gibi bir durumda hangi işlemlerin uygulanacağının henüz yeteri kadar açığa kavuşturulamadığı görülmektedir.

159 INTERPARES, **INTERPARES 2: Experiential, Interactive and Dynamic Records**, **a.g.e.**, s. 120-121. ; Luciana Duranti ve Kenneth Thibodeau, "The Concept of Record in Interactive, Experiential and Dynamic Environments: The View of Interpares", **Archival Science**, No: 6, 2006, s. 32. ; Duranti ve Thibodeau, bu uygulamanın bir benzerinin Ortaçağ Avrupası'nın noterlerinde de görüldüğünü ifade etmektedir. Buna göre noterler, şahit oldukları bir işlemi kâğıda aktarmak yerine, imbreviatura adını verdikleri bir belgeye yazardı. Bir parşömeni köşesinden ikiye katlayarak işlemin türü, tarihi, zamanı, kimler arasında yapıldığı, işlemin tanımı ve diğer ilgili verileri kaydederlerdi. Köşesi katlanmış parşömen, dosyasına kaldırılırdı. Her yıl sonunda, imbreviatura adını verdikleri bu belgeler ciltlenir ve muhtevasıyla birlikte yapılan işlemler kayıt defterine (regesta) yazılırdı. Eğer, işlemi yapanlardan biri bunun belgesini isterse kayıt defterinden imbreviatura bulunup o işlemin türüne göre sahip olması gereken form özelliklerini belirten kurallar (formularium) ışığında imbreviatura'daki bilgilerden hareketle yeni bir belge oluşturulurdu. Bu durum, kâğıt ortamda saklanan belge ile sunulan belge arasında bir ayrıma gidildiğini gösteren örneklerinden biri olarak kabul edilmektedir. İşlemin türüne ait form özelliklerinin sunulan belgenin oluşturulmasında önemli bir rol oynadığı dikkat çekmektedir (**a.g.e.**, s. 52-54).

160 Belgenin saklanan hâli ile sunulan hâli arasındaki ayrımı EBYS'lerde de görmek mümkündür. Mesela, imza süreçleri tamamlanmış e-imzalı bir belge XML Advanced Electronic Signature (XADES – XML Gelişmiş Elektronik İmza) XADES ile imzalanıp XML olarak saklanabilmekteyken, sistemde kullanılmak amacıyla PDF ya da istenilen başka bir formatta sunulabilmektedir.

161 Duranti, "Structural and Formal Analysis: The Contribution of Diplomatics to Archival Appraisal in the Digital Environment", **a.g.e.**, s. 80.

162 MacNeil, **Trusting Records: Legal, Historical and Diplomatic Perspectives**, yayım yeri yok, Springer, 2000, s. XII, XIII.

mahkemeye taşınması sonucunda mahkeme, e-belge türlerinden biri olan e-postalarda kontekstin belirlenmesine yardımcı olan alıcının adı gibi eksik form elemanlarının bulunduğunu belirtmiş; belgenin delil değerinin anlaşılabilmesi için bu özelliğin önemli olduğunu vurgulamıştır[163].

1.3.1.2. Uygulama Yazılımlarından Kaynaklanan Sorunlar

Arşivlenen e-belgelerin delil değerine ilişkin tartışmaların bir diğer odak noktası uygulama yazılımları üzerinedir. Buradaki tartışmaların daha çok yazılımların standartlara uygun olarak geliştirilmemesi ile yazılımlarda belge yönetimi yerine bilgisayar mühendisliği odaklı bakış açısının benimsenmesi üzerine yapıldığı görülmektedir[164]. Bu tartışmaların öne çıkarılmasının nedeni, birçok farklı hususla beraber uzun vadede özgünlüğü koruyamamaktan dolayı arşivlenen e-belgelerin delil değerinde risk oluşturma ihtimalidir. Çünkü, yazılımın standartlara uygun olarak geliştirilmemesi sonucunda EBYS'lerde sabit bir form ve içeriğe sahip olmayan, arşivsel bağı kurulamayan belgelerin oluştuğu anlaşılmaktadır[165]. Bunlar, delil değerinde problemler oluşturacak sorunlar olarak değerlendirilmektedir. Ayrıca, uygulama yazılımlarında belge yönetimi yerine bilgisayar mühendisliği odaklı problemlerin belge hiyerarşisinin oluşturulamamasına, dosyalamanın yanlış yerde başlatılmasına ve neticesinde aidiyet zincirinin kurulamamasına neden olduğu gözlenmektedir[166].

---

163 1984-1988 yılları arasında ABD Başkanı olan Ronald Reagan, döneminin sonunda Başkanlık Ofisinden gönderilen e-postaların silinmesini emretmiştir. Amerikan Milli Arşivi, bu e-postaların arşivlik bir malzeme olduğunu belirterek sürece itiraz etmiş ve konu mahkemeye taşınmıştır. Başkanlık Ofisi savunmasında, e-postaların çıktılarının alındığını ve alıcının adının yer almaması gibi eksik form elemanlarının bulunması, elektronik ortamda e-postaların içeriğinin yeteri kadar seçilememesi gibi nedenlerle silinmesini talep ettiklerini beyan etmiştir. Mahkeme, e-postaların kurumsal belge olduğunu ifade ederek ABD Başkanlık Ofisinin verdiği talimatın yasalara uygun olmadığına karar vermiştir (Terry Eastwood, "Introduction", **Preservation of the Integrity of Electronic Records**, ed.: Luciana Duranti, Terry Eastwood ve Heather MacNeil, yayım yeri yok, Springer, 2002, s. 3).

164 Anne Thurston, "Digitization and Preservation: Global Opportunities and Cultural Challenges", **The Memory of the World in the Digital Age: Digitization and Preservation**, 26-28 Eylül 2012, ed.: Luciana Duranti ve Elizabeth Shaffer, Vancouver[Kanada], UNESCO, 2013. ; Thurston, "Records as Evidence for Measuring Sustainable Development in Africa", **a.g.e.**, s. 13.

165 Luciana Duranti, The INTERPARES2 Project (2002-2007): An Overview, **Archivaria**, No: 64, 2007. ; Anne Thurston, "Digitization and Preservation: Global Opportunities and Cultural Challenges", **The Memory of the World in the Digital Age: Digitization and Preservation**, 26-28 Eylül 2012, ed.: Luciana Duranti ve Elizabeth Shaffer, Vancouver[Kanada], UNESCO, 2013.

166 Thurston, "Records as Evidence for Measuring Sustainable Development in Africa", **a.g.e.**, s. 13.

Uygulama yazılımlarının arşivlenen e-belgelerin delil değerine ilişkin riskler taşıdığı çeşitli çalışmalarda ifade edilmiştir[167]. Bunlardan biri de 1996 yılında Kanada Savunma Bakanlığında yapılan çalışmadır. Analizler neticesinde uygulama yazılımları standartlar ışığında geliştirilmediğinden kimin ne zaman hangi işlemleri yaptığını gösteren log kayıtlarının değiştirildiği ve silindiği anlaşılmıştır[168]. Burada, aynı zamanda bir delil değeri unsuru olan denetim mekanizmasının eksikliğine dikkat çekilmiştir. Bu gibi problemlere karşılık, uygulama yazılımlarının belirlenen ilkeler dâhilinde çalışıp çalışmadığını denetleyen kontroller, veri bütünlüğünün ve tanımlanabilirliğin korunduğunu analiz eden teknolojik yaklaşımlar ve bilgi güvenliğine ilişkin prosedürlerin tesis edilmesi önerilmektedir[169].

Bu tartışmalar, e-belgelerin güvenilirliği konusunda ciddi çalışmaları bulunan Luciana Duranti'nin de dikkatini çekmiş ve onun öncülüğünde University of British Columbia (UBC) Projesi olarak da bilinen Elektronik Belgelerin Bütünlüğünün Korunması Projesi (The Preservation of the Integrity of Electronic Records) başlatılmıştır. Bu projede, uygulama yazılımlarında e-belge nasıl oluşur, bu belge nasıl transfer edilir, hangi türde belgeler üretilir, e-belgelerin karakteristik özellikleri nelerdir ve bunlar uygulama yazılımlarında nasıl korunur gibi sorulara cevap aranmaya çalışılmıştır[170]. Bu çalışmalar, INTERPARES Projesi'nin başlamasına kaynaklık etmiştir.

Duranti, INTERPARES'in ilk safhasında (1999-2001) uygulama yazılımlarının standartlardan uzak olması nedeniyle arşivlenen e-belgelerin delil değerinin korunmasında sorunlar yaşandığını ifade etmektedir. Bu sorunların, sabit bir form ve değişmeyen bir içeriğe sahip olmayan, arşivsel bağın kurulamadığı e-arşiv belgelerinin varlığına neden olduğunu ileri sürmektedir. Duranti, e-belgelerin

---

167 The National Archives [TNA], **Understanding Digital Contunity**, 2017, s. 5, (Çevrimiçi) https:// www. nationalarchives. gov. uk/ documents/ information-management/ understanding-digital-continuity.pdf, 5 Mart 2020. ; David S. Rosenthal vd., "Requirements for Digital Preservation Systems: A Bottom-Up Approach", **D-Lib Magazine**, C. 11, No: 11, 2005, (Çevrimiçi) http :// www. dlib. org/ dlib/ november05/rosenthal/11rosenthal.html, 2 Şubat 2020. ; Victoria L. Lemieux, **One Step Forward, Two Steps Backward? Does EGovernment make Governments in Developing Countries more Transparent and Accountable?**, Washington[ABD], 2016, s. 12-13, (Çevrimiçi) https :// openknowledge. worldbank. org/ handle/10986/23647, 10 Ağustos 2020.

168 MacNeil, **Trusting Records: Legal, Historical and Diplomatic Perspectives**, **a.g.e.**, s. XII, XIII.

169 **a.e.**

170 **Preservation of the Integrity of Electronic Records**, ed.: Luciana Duranti, Terry Eastwood ve Heather MacNeil, yayım yeri yok, Springer, 2002.

arşivlenmesine yönelik uygulamaların, belgeler üretildikten sonra değil, üretilmeden önce başlatılmasını önermektedir[171].

E-belgelerin güvenilirliği üzerine çalışan Corinne Rogers, Uluslararası Arşiv Konseyinin (International Council of Archives [ICA]) de 1990'lı yıllardan itibaren e-belgelerin özgünlüğü üzerine çalışmalar başlattığını ifade etmektedir[172]. ICA'nın, Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütünün (United Nations Educational, Scientific and Cultural Organization [UNESCO]) bu konuda girişimler başlatmasını teşvik ettiği belirtilmektedir. Bu girişimler neticesinde bir rapor hazırlanmış ve arşivlenen e-belgelerin delil değeriyle ilişkilendirilebilecek sorunlar açıklanmıştır. Uygulama yazılımlarının geliştirilmesinde belge yönetimi bakış açısının benimsenmeyerek sadece bilgisayar mühendisliği odaklı bir bakışın varlığı dile getirilen bu sorunlar arasında dikkat çekmektedir[173]. Bunların yanı sıra arşivlenen e-belgelerin delil değerine ilişkin tartışmaların bir kaynağının da kurumsal politika ve prosedürlerin eksikliği olduğu düşünülmektedir.

1.3.1.3. Kurumsal Politika ve Prosedürlerin Yetersizliği

Arşivlenen e-belgelerin delil değerine ilişkin belgeyi oluşturan unsurlar ile teknolojik koşullar dışındaki tartışmaların, politika ve prosedürler, yeterli standartların tesis edilememesi ve gerekli eğitimin verilememesi gibi kurumsal süreçler üzerine olduğu görülmektedir. E-belgelerin arşivleme işlerinin nasıl yapılacağını gösteren prosedürlerin eksikliği, çalışanları bir yasal dayanaktan yoksun bırakmaktadır. Bu yoksunluk, delil değerinin korunması için gerekli adımların atılamamasına neden olabileceğinden delil değeri açısından problemli bir durum olarak değerlendirilmektedir.

Prosedürlerin eksikliğinin yanı sıra, yeterli standartların tesis edilememesi de karşılaşılan bir diğer problemdir. Çünkü standartlar, bir işin nasıl yapılacağını göstermese de o işte olması gereken özellikleri belirler. Arşivlenen e-belgelerle ilgili işlemlerde hangi standartlara başvurulabileceğinin belirtilmesi, delil değerini artıran bir unsur olarak düşünülmektedir.

---

171 Duranti, The INTERPARES2 Project (2002-2007): An Overview, **a.g.e.**, s. 114.

172 Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice", **a.g.e.**, s. 26-30.

173 **a.e.**

Delil değerini tehdit eden unsurlardan bir diğeri ise kurum çalışanlarına gerekli eğitimlerin verilememesidir. Çünkü delil değeri korunan belgeler, donanımlı arşivciler tarafından yönetilir. Bu donanımı artıran unsurlardan biri de arşivcilerin eğitilmesidir. Aksi takdirde, prosedür ve standartlarda ifade edilen hususların yerine getirilememesi ihtimali gündeme gelecektir. Örneğin belgenin bütünlüğü ve tamlığıyla alakalı sistem kriterlerinin uygulunamaması neticesinde özgünlüğün tartışılması ihtimal dâhilindedir. Hâl böyle olunca, arşivlenen e-belgelerin delil değerinde şüphe oluşabilir. Bu sorunlara bir çözüm olarak özgünlüğün korunmasına yönelik uygulamalar içeren belge ve arşiv yönetimi kapasite geliştirme programının hazırlanıp, gerekli politika ve prosedürlerle de desteklenmesi tavsiye edilmektedir[174].

Bu politika ve prosedürlerin nelerden oluşabileceği UBC Projesinde incelenmiştir. Burada kullanılacak idari, prosedürel ve teknik yöntemler neler olabilir, delil değerini korumak için ihtiyaç duyulan gereksinimler farklı idari, hukuki ve kültürel yapılarda nasıl tesis edilir gibi sorulara cevaplar arandığı görülmektedir. Bu sorular INTERPARES çalışmaları neticesinde geliştirilerek delil değerinin korunmasında kullanılabilecek belge ve arşiv yönetimi gereksinimleri hazırlanmıştır[175].

Delil değerinin korunmasında politika ve prosedürlere vurgu yapan bir diğer projenin Richard Cox'un öncülüğünde Pittsburgh Üniversitesinde gerçekleştiği görülmektedir. Burada, belgelerin mevzuata uyumluluğu ile yazılı politika ve prosedürlerin oluşturularak saklama planlarının varlığına vurgu yapıldığı gözlenmektedir[176]. Bu çalışmalar neticesinde delil değeri incelemelerinde kritik edilecek unsurlar ortaya çıkarılmıştır.

1.3.2. Arşivlenen E-Belgelerin Delil Değeri Unsurları

Arşivlenen e-belgelerin delil değeri kritik edilirken kullanılacak unsurlar, sabit bir form (yapı), değişmeyen içerik ve tanımlanabilir kontekst olarak öne

---

174 **a.e.**

175 Heather MacNeil vd., "Requirements for Assessing and Maintaning the Authenticity of Electronic Records", **a.g.e.**

176 Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice", **a.g.e.**, s. 31-32.

çıkmaktadır[177]. İçerik, belgenin ihtiva ettiği metnin ilk hazırlandığı gibi kalması, var olan bilgilerin değişmemesi ve metni oluşturan yazının bit yapısının bozulmaması gibi hususlar olarak ifade edilmektedir. Belgelerde bit yapısının korunması, belge ve arşiv yönetimi sürecinde de oldukça önemlidir. Bu süreçte, özet değerlerinin otonom araçlarla oluşturulup yedeklenmesi ve değişip değişmediğinin kontrol edilmesi gibi yöntemler benimsenmektedir[178].

Yapı, bir belgenin nasıl oluşturulduğu ve muhafaza edildiğini gösteren fiziksel ve entelektüel özellikler olarak kabul edilmektedir[179]. Belge nasıl oluştu sorusuna cevap verir. Belgenin formatına göre farklı yapısal özellikler söz konusudur. Örneğin, PDF formatındaki ile TIFF formatındaki farklı yapılara sahiptir. Formatın yanı sıra, e-belgelerin yapısal özellikleri saklandığı sistemlere göre değişiklik göstermektedir. Mesela, kurumsal belge yönetim sisteminde saklanan ile kişinin kendi bilgisayarında sakladığı, hukuki açıdan e-belge olabilmekle alakalı birtakım yapısal özelliklere sahip olup olmamaları sebebiyle farklılık gösterir. Çünkü, kurumsal belge yönetimi sistemlerinde saklanan belgelerin yapısal özelliklerinden olan üstveriler, iletildiği kişi ve kurum ile KEP gibi hususlar tespit edilebiliyorken, kişinin kendi bilgisayarında tuttuklarında bu özellikler çok da belirgin değildir.

İçerik ve yapının yanı sıra bir diğer delil değeri kritik unsuru olan kontekst, belgelerin üretiminden arşivde sürekli saklanmasına kadar yaşam döngüsü sürecindeki bütün aşamaların açığa çıkarılmasıdır. Bu bağlamda, belge kim tarafından üretildi, nasıl kullanıldı ve dosyalandı, kimin emanetinde kaldı, hangi şartlarda nereye devredildi ve arşive nasıl geldi sorularına cevap aranır. Böylece belgeyle alakalı delillerin sağlıklı bir şekilde korunması ve erişilip kullanılması hedeflenir. Kontekst, her belge için aynı süreci ifade etmeyebilir. Bundan dolayı, Millar, kontekstin üretene, üretildiği fonksiyona, dosyalanma şekline, muhafaza edene ve kullanana göre değişebileceğine işaret etmektedir[180]. Örneğin, kurumlarda norm kadro planlamalarıyla ilgili oluşan evrakın konteksti, doğduğu fonksiyondan dolayı personel

177 Luciana Duranti, "The Concept of Electronic Record", **Preservation of the Integrity of Electronic Records**, ed.: Luciana Duranti, Terry Eastwood ve Heather MacNeil, yayım yeri yok, Springer, 2002, s. 12.

178 Laura Millar, **Archives, Principles and Practices**, 2. bs., Londra[Birleşik Krallık], Facet Publishing, 2017, s. 12

179 **a.e.**

180 **a.e.**

dairesinde farklı, strateji, muhasebe ve finans dairelerinde daha farklıdır. Çünkü, bu dairelerdeki norm kadro planlamasıyla ilgili belgelerin değeri, saklama süresi, ilişkili olduğu paydaş belgeler ve işlem gördüğü imza süreçleri birbirinden farklılık gösterebilmektedir. Dolayısıyla belgenin konteksti işlem gördüğü fonksiyona göre aranmalıdır.

Durum böyle olunca, hukuki açıdan incelenen bir olayda belgenin aynı fonksiyon kapsamında oluşan diğer belgelerle olan ilişkisi göz önünde tutulmayıp sadece kendisinin kritik edilmesi, araştırılan olay hakkında yeteri kadar delil elde edilememesine neden olabilir. Burada belgelerin kontekstinin dikkate alınması gerekir. Çünkü kontekst, aynı zamanda hukuki açıdan incelenen bir olayda belgeyle alakalı delillerin ispat kuvvetini de etkilemektedir. Laura Millar, bu durumu maaş bordroları üzerinden örneklendirerek şöyle açıklamaktadır: Çalışanların geçmiş yıllara yönelik maaşlarının incelendiği bir durumda, maaş farklarını gösteren bordrolar tek başına yeterli bilgiyi sunamayabilir. Çünkü maaş bordroları kendisinden önceki veya sonraki ayın maaş farklarını gösterir. Bu süreç, maaş bordrolarındaki değişikliklerin resmî, kurallara uygun ve yazılı bir onayla yapıldığını gösteren belgelerin de bordrolarla birlikte tutulmasını gündeme getirmektedir. Bunun için ilgili bordroların, diğer belgelerle birlikte güvenli bir şekilde muhafaza edilmesi ve gerektiğinde değişikliklerin onaylandığını göstermek amacıyla bir kanıt olarak saklanması gerekir[181]. Böylece maaşlardaki değişimin ne zaman meydana geldiği, kim tarafından onaylandığı, bu değişimle ilgili belgelerin nasıl kullanıp dosyalandığı ve arşive hangi şartlarda devredildiği delillendirilir. Buradaki hedef, belgenin neden böyle bir idari işlem sonucunda oluştuğunun gösterilmesidir[182].

Belgenin hangi idari işlemler sonucunda oluştuğunun gösterilmesinde dosyalamanın önemli bir rolü bulunmaktadır. Çünkü idari işlemlerin ardından oluşan belgeler, üretildikleri bağlama göre birbirleriyle ilişkilendirilerek bir araya getirilir. Dosyalama, ait olduğu işle ilgili bilgi bütünlüğünü sağlarken, her belge bu bütünlüğe katkı yapar[183]. Bunun için belgelerle üretildikleri bağlam arasında entelektüel ilişkinin

---

181 **a.g.e.**, s. 6.

182 Hilary Jenkinson, **A Manual of Archive Administration**, Londra[Birleşik Krallık]: Percy Lund, Humphries & Co Ltd., 1937, s. 4.

183 Çiçek, "Elektronik Belge Yönetimi Uygulamalarında Bir Alt Sistem Olarak Dosya Yönetimi", **a.g.e**., s. 439.

kurulması gerekir. Bu ilişki, belgelerin konu ya da belirli bir vaka bağlamında bir araya getirilmesiyle, yani organik bağın kurulmasıyla ortaya çıkarılabilir. Organik bağ, belgenin kaldırıldığı dosya ile orada bulunan diğer malzemelerle arasında münasebet kurulmasıdır[184].

Dosyalama, belge ile üretildiği bağlam arasındaki entelektüel ilişkiyi ortaya çıkarır ve bilgi bütünlüğünü korur. Eğer, dosyaların doğduğu kaynak tespit edilemiyor ve bütünlüğe katkı yaptığı düşünülen belgelerin işlemleri ortaya çıkarılamıyorsa[185] arşivsel bağın[186] zarar gördüğü düşünülebilir[187]. Dosyayı meydana getiren her belge, kendinden sonraki sürecin ve doğacak olan belgenin delilini oluşturduğundan dosyada bulunması gereken bir belgenin olmaması ya da bulunmasına rağmen paydaş belgelerle ve dosyayla organik bağı kurulamaması delil değerinden şüphe duyulmasına sebep olur.

Fakat, e-belgelerde arşivsel bağı korumanın kâğıt belgedekilere göre biraz daha emek isteyen bir süreç olduğu gözlenmektedir. Çünkü e-belgede yaşanan değişimler, kâğıttakilerde olduğu gibi ilk bakışta gözle görülemeyebilir. Bu değişiklikleri tespit etmek için ayrıntılı incelemeler yapılmalıdır. E-belgelerin doğası, bu analizin belgenin üretiminden itibaren başlatılmasını gerekli kılmaktadır. Çünkü yaşanan tecrübeler neticesinde belge bileşenlerinin saklandığı veri tabanlarındaki verilerin herhangi bir kasıt olmaksızın değişikliğe uğrayabildiği görülmüştür[188]. Söz konusu sorunla karşılaşıldığında delil değerinin hangi oranda korunduğunun gösterilmesi için ihtiyaç duyulan politika ve prosedürler belirlenmelidir[189]. Bilgi güvenliği politikası, e-belgelerin korunmasıyla alakalı olarak arşivcilerin yetkinlikleri ve devlet arşivlerinin

184 **a.e.**

185 T. R. Schellenberg, **Arşiv İdaresi**, çev. Necla İlemin, T.C. Başbakanlık Devlet Arşivleri Genel Müdürlüğü, Cumhuriyet Arşivi Daire Başkanlığı, Ankara, 1993, s. 84, 91-92.

186 Arşivsel bağ, "ortamı ne olursa olsun bir belgenin üretilmesinden arşive intikal edene kadar geçen süreçte kim tarafından, hangi fonksiyon ve işlem kapsamında üretildiği, kime devredildiği, nasıl dosyalandığı ve hangi seride bulunduğunun açıklanıp bu seri içerisinde ait olduğu vaka ya da konu dosyasıyla ve bu dosyadaki diğer belgelerle ilişkisini kurabilmek" şeklinde tanımlanmaktadır (Çiçek, "Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme", **a.g.e.**, s. 98-99).

187 Çiçek, **Kurumsal Bilgi ve Belge Yönetimi**, **a.g.e.**, s. 157.

188 Eduardo del Valle Perez, "Sharing My Loss to Protect Your Data: A Story of Unexpected Data Loss and How to Do Digital Preservation", **Preservation and Archiving Special Interest Group [PASIG], 11-13 Eylül 2017, Oxford, Birleşik Krallık**, (Çevrimiçi) https :// pasig. figshare.com/articles/presentation/Sharing_my_loss_to_protect_your_data_A_story_of_unexpected_data_loss_and_how_to_do_real_preservation/5415046/1, 15 Aralık 2020.

189 Luciana Duranti, "The Concept of Electronic Record", **a.g.e.**, s. 19-20.

çıkaracağı standartlar ile güvenilirlikle ilgili prosedürler bu tarz uygulamalar olabilir[190].

1.3.3. Arşivsel Güvenilirlik

1.3.3.1. Arşivsel Güvenilirlik Yaklaşımları

Belgelerin delil değerinin koruması için taşıyıcı ortam, içerik, düzenleyen, kontekst gibi özelliklerin muhafaza edilmesi gerektiği bilinmektedir. Söz konusu niteliklerin korunup güvenilirliğin devamlılığıyla alakalı olarak diğer alanlara göre belgeyle daha çok ilişkisi olduğu düşünülen hukuk, diplomatik ve tarih disiplinleri farklı yaklaşımlar geliştirmişlerdir. Arşivsel güvenilirlik bakımından arşivlenen malzemenin güvenilirliği, e-belgeler ortaya çıkıncaya ve teknolojik güvenilirlik söz konusu oluncaya kadar bu üç alanın yaklaşımıyla değerlendirilmiştir.

Güvenilirliğin ilgili disiplinlere göre farklı tanımlandığı dikkat çekmektedir[191]. Mesela, hukuki güvenilirlik, belgenin yaşam döngüsü içerisinde onu üreten yetkilinin otorite ve garantisini gösteren hukuki delillere sahip olmasını ifade eder[192]. 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 edilir[193].

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[194]. 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 veritabanı kayıtları incelenmektedir[195].

---

190 INTERPARES, **INTERPARES 2: Experiential, Interactive and Dynamic Records**, **a.g.e.**

191 INTERPARES, **Terminology**, (Çevrimiçi) https:// interparestrust. org/ terminology/ term/ trustworthiness, 27 Nisan 2020.

192 Niyazi Çiçek, **Modern Belgelerin Diplomatiği**, İstanbul, Derlem Yayınları, 2009, s. 212.

193 MacNeil, **Trusting Records: Legal, Historical and Diplomatic Perspectives**, **a.g.e.**, s. 53-56.

194 Çiçek, **Modern Belgelerin Diplomatiği**, **a.g.e.**, s. 212.

195 MacNeil, **Trusting Records: Legal, Historical and Diplomatic Perspectives**, **a.g.e.**, s. 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 edilir[196]. Özellikle belgede geçen bilgilerin, açıklanan tarih, yer, kişi ve dönemle uyuşması gerekir.

INTERPARES gibi uluslararası projelerde bu güvenilirlik yaklaşımlarından yararlanıldığı bilinmektedir. Bu projede bir belgenin varlığını ortaya koyan, özellikle onun form özelliklerinin nasıl şekillendiği açıklanmaya çalışılmış; belgenin üretiminden dosyalanmasına transferinden arşiv malzemesi olana kadar geçen süreçte bu özelliklerin değişime uğrayıp uğramadığı değerlendirilmiştir. Bu form özellikleri diplomatik açıdan ele alınırken daha çok arşivcilik ve belge yönetimi bakış açısıyla hareket edilmiştir[197].

Ancak, e-belgelerin delil değerinin analizinde tek başına diplomatik güvenilirliğin yeterli olamayabileceği ifade edilmektedir[198]. Çünkü, belgelerin oluşumuna kaynaklık eden mevzuat ve kullanılan bilgi teknolojileri meselenin daha geniş bir bakış açısıyla ele alınmasını gündeme getirmiştir. Bu duruma örnek teşkil edecek çalışmalardan biri, adı geçen proje tarafından desteklenenen Jessica Bushey'in sosyal medya platformlarındaki fotoğrafların güvenilirliğini incelediği doktora tezidir. Bu çalışmada diplomatik analiz yöntemleri yanı sıra, fotoğrafçılık ve yeni medya yaklaşımı ile delil hukukundan yararlanmıştır. Bushey, bu incelemeyi yaptığı çalışmanın başlığını arşivsel güvenilirlik olarak belirlemiştir[199].

Hem adı geçen projede hem de belirtilen tezde açıklandığı şekliyle, güncel belgeler, hukukun öngördüğü delil değeri unsurlarından olan özgünlük, tamlık ve gerçekliği arşiv belgesi oldukları dönemde de muhafaza etmelidir[200]. Her iki çalışmanın sonuçlarına göre ancak bu durumda belgeler güvenilir kabul edilirler. Fakat belgenin muhafaza edildiği ortamın koşulları, güncellemeler ve taşıyıcı kayıt ortamının kırılganlığı gibi problemler, daha çok belge arşiv malzemesi olduğu dönemde ortaya çıktığından adı geçen delil değeri unsurlarının arşivsel güvenilirlik açısından ayrıca ele alınması gerekir.

---

196 Çiçek, **Modern Belgelerin Diplomatiği**, **a.g.e.**, s. 212.

197 INTERPARES, **INTERPARES 2: Experiential, Interactive and Dynamic Records**, **a.g.e.**

198 Jessica Bushey, "The Archival Trustworthiness of Digital Photographs in Social Media Platforms", Yayınlanmamış Doktora Tezi, British Columbia Üniversitesi[Kanada], 2016.

199 **a.g.e.**

200 **a.g.e.** ; INTERPARES, **INTERPARES 2: Experiential, Interactive and Dynamic Records**, **a.g.e.**, s. 335, 816.

1.3.3.2. Güvenilirlik Kriterleri

Belgenin özniteliklerinin üretildikten sonra işlem gördüğü ve dosyalanıp arşivlendiği dönem içerisinde değişmemesi olarak açıklanan özgünlük[201], aynı zamanda e-belgelerin hukuki bakımdan delil değeri unsurlarından biri olarak kabul edilmektedir. 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[202]. Özgünlüğün diğer bir adımı ise belgenin tüm bileşenleriyle birlikte bozulmamış ve değiştirilmemiş olmasını ifade eden bütünlüktür. Ancak, e-belgeler söz konusu olduğunda taşıyıcı ortamın kırılganlığı, teknolojik eskimeler ve sistemlerin standartlardan uzak bir şekilde geliştirilmesi, belgelerin bütünlüğünü oluşturan unsurlardan biri olan bit akışını olumsuz etkileyebilir[203]. Bit akışı, e-belgelerin yazılım kodları aracılığıyla anlamlı bir şekilde görünür olmasını sağlar. Bu bit akışı, form özellikleri, içerik, onay ve imzalar gibi bir belgenin bütününü kapsar. Dolayısıyla belge üretilirken oluşan bit akışının bozulması, delil değeri unsurlarından olan belgedeki yetki veya hakların gösterilememesi, form özelliklerinin bozulması ve içeriğin değişmesi anlamına gelebilir. Böyle olumsuz bir durum, arşivlenen belgelerin güvenilirliği için büyük bir risktir. Bunun yanı sıra, bit akışının korunup içeriğin değişmemesi her ne kadar güncel belgeler için önkoşul olarak kabul edilse de arşivlendikleri dönemde tek başına bütünlüğün muhafazası için yeterli görülmemektedir. Çünkü arşivlenen belgenin semantik yapısında yaşanacak bir kayıp, belgedeki yetki veya hakların yeteri kadar anlaşılamamasına neden olabilecektir[204]. Semantik yapı, bir belgenin ortaya çıkış serüvenini, tamamlayıcı ve paydaş belgelerle ilişkisini açıklayan, aynı zamanda bir dosyada bulunma sebebini gösteren kontekst bilgisidir. İşte e-belge arşivlendiği zaman bu bilginin de korunmaya ihtiyacı vardır. Güncel dönemde olduğu gibi arşivlendikleri zaman da belgelerin bit akışı ve semantik yapılarını koruyup korumadıklarına bakılarak bütünlükleri kontrol edilmelidir[205].

---

201 Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice", **a.g.e.**, s. 26.

202 Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 150-151.

203 **a.g.e.**, s. 151.

204 **a.g.e.**, s. 152.

205 **a.e.**

Bütünlüğün yanı sıra belgelerin bir diğer güvenilirlik unsuru tamlıktır. Kaynaklarda tamlık arz eden bir belgede delil değeri unsurlarından olan 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[206].

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 aynı zamanda delil değeri unsurlarından olan belgeyi hukuki bir sonuç doğurmaya elverişli hâle getirecek entelektüel formun tüm elemanlarının mevcut olmasını ifade etmektedir[207].

1.3.3.3. Güvenilirliğin Korunmasına Yönelik Görüşler

Özgünlük, tamlık ve gerçekliğin yani güvenilirliğin korunması için çeşitli yöntemlerin benimsenmesi gerekir. Corinne Rogers'a göre benimsenecek yöntemler, belge üretildikten, alındıktan ve dosyasına kaldırıldıktan sonra da 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 tanımlanması ve onun provenans, kontekst ve format ile bit özellikleri demek olan yapısının sunulmasını içermektedir[208]. Burada, taşıyıcı ortam, içerik, form özellikleri, belgedeki işlem ve kişiler, arşivsel bağ, üstveriler, kontekst ve belge formunun tamlığı ile diplomatik özellikler öne çıkmaktadır[209]. Teknolojik yöntemler ise kullanılan donanım ve yazılım gibi

206 **a.e.**

207 **a.g.e.**, s. 152-153.

208 Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice", **a.g.e.**, s. 28, 35.

209 MacNeil, **Trusting Records: Legal, Historical and Diplomatic Perspectives**, **a.g.e.**, s. 91, 96-97.

belgelerin teknolojik yönüyle ilişkili olup[210] e-imza, e-mühür, log kayıtları, denetim günlükleri ve veri tabanı kayıtlarının analiz edilmesini gündeme getirmektedir[211].

Yukarıdaki hususların yanı sıra, Jennifer Meehan belge ile belgedeki işlem ve faaliyet arasındaki ilişkinin incelenmesi gerektiğini ileri sürmektedir[212]. Bu durum, belgenin aynı faaliyet kapsamında üretildiği diğer belgelerle olan ilişkisinin ortaya konulmasına duyulan ihtiyaçtan kaynaklanabilir. Bu ihtiyaç, aynı zamanda delil değeri unsurlarından olan arşivsel bağın açığa çıkarılmasını gündeme getirmektedir. Bunun için provenans ile kontekst analiz edilerek belgelerin oluşumuna kaynaklık eden fonksiyonlar saptanır; aynı faaliyet kapsamında oluşan ve aralarında organik bağ bulunanlar bir araya getirilir[213]. Böylece, belge ile belgedeki faaliyet arasındaki ilişki ortaya konur[214] ve arşivsel bağ açığa çıkarılır. Belgelerin delil değerinin süreklilik arz etmesinin hedeflendiği arşivsel bağın açığa çıkarılması sürecinde kimliklendirme ve tanımlama gibi çeşitli mekanizmalar ile bu mekanizmaların nasıl kullanılacağını gösteren prosedürlerden yararlanılmaktadır. Terry Cook'a göre bu mekanizmalardan fonlara saygı, asli düzeni korumak ve provenansı tesis etmek ilkeleriyle arşivsel bağı açığa çıkarmak mümkün olabilir[215].

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 arşivciler olduğu belirtilmektedir[216]. O hâlde, arşivler ve arşivcilerin belgelerin

---

210 Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice", **a.g.e.**, s. 35.

211 MacNeil, **Trusting Records: Legal, Historical and Diplomatic Perspectives**, **a.g.e.**, s. 73-75, 100-102.

212 Jennifer Meehan, "Towards an Archival Concept of Evidence", **Archivaria**, No: 61, 2006, s. 142.

213 Çiçek, **Kurumsal Bilgi ve Belge Yönetimi**, **a.g.e.**, s. 154.

214 Meehan, **a.g.e.**

215 Terry Cook, "Evidence, Memory, Identity and Community: Four Shifting Archival Paradigms", **Archival Science**, C. 13, No: 2-3, 2013, s. 99-100.

216 Luciana Duranti ve Corinne Rogers, "Educating for Trust", **Archival Science**, C. 11, No: 3-4, 2011, s. 376-377.

güvenilirliğinin korunmasında önemli görevleri bulunduğu anlaşılmaktadır. Bu görev, arşivlerin başka kurumlarda üretilmiş ve kendisine devredilmiş belgelerin güvenilirliğini korumak gibi bir özelliğe sahip olmasından kaynaklanmaktadır[217].

Oluşan bu tecrübe neticesinde arşivler, kâğıt belgelerin güvenilirliğinin başarılı bir şekilde korunması konusunda ciddi bir bilgi ve deneyime sahip olmuştur. Bu bilgi ve deneyim, kâğıt belgeler nasıl tanımlanacak, provenans nasıl açığa çıkarılacak, depolardaki ısı ve nem koşulları nasıl belirlenecek gibi hususlarda bir birikim meydana getirmiştir.

1.3.3.4. Güvenilirlik Analizi Düzeyleri

Sahadaki uygulamalar, e-imzalı belgelerin güvenilirliği söz konusu olduğunda arşivlerde kâğıt belgelerdeki gibi yeterli bir birikimin henüz oluşmadığı kanaatini uyandırmaktadır. Bu olumsuz kanaat, e-imzalı belgelerin formatının değişmesi durumunda nasıl geçerli olacağı, bileşenlerinin nasıl muhafaza edileceği gibi konularda henüz yeterli prosedür ve uygulamaların geliştirilmemesinden kaynaklanmaktadır. Mesela birçok arşivde e-imzalı belgelerin arşivlenmesine ilişkin ilkelerin yer aldığı bir prosedür ya da rehbere henüz rastlanmamaktadır. Fakat konuyla alakalı sorunlar daha belgeler güncel dönemdeyken başlamaktadır. Dosyalamanın yanlış yerde başlatılması, dosya kodunun sadece veri tabanında belgelere erişim için bir etiket olarak kullanılması ve dosya bütünlüğünün sağlanmaması gibi çeşitli sorunlar yaşandığı bilinmektedir[218]. Aynı zamanda, bu belgelerin üretilip arşivlendiği bazı uygulama yazılımlarının standartlardan uzak bir şekilde geliştirildiği gözlenmektedir[219].

Bu gibi problemler, e-imzalı belgelerin tanımlanıp provenansının açığa çıkarılmasına engel teşkil edebilir. Bunun sonucunda arşivsel bağın kurulamaması riski ortaya çıkacaktır. Bu risk, e-imzalı belgelerin delil değerinin korunamamasına sebep olabilir. Bu nedenle e-imzalı belgelerin delil değerinin arşivsel güvenilirlik açısından

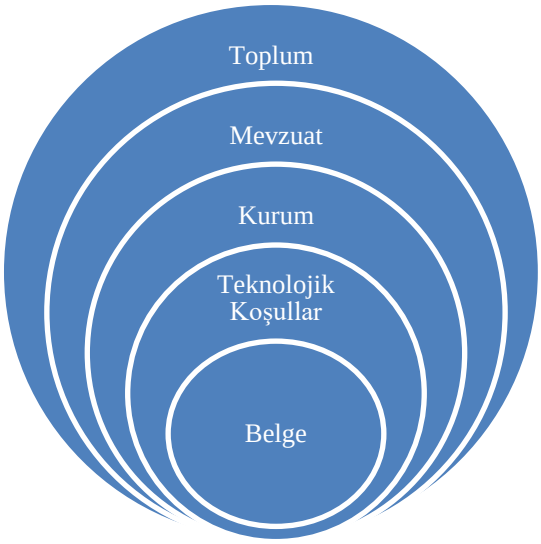
---

217 Çeşitli kaynaklar, arşivlerin bu özelliğiyle ilk olarak 529 yılında Roma İmparatorluğunda karşılaşıldığını söylemektedir. Bu kaynaklarda saklanan belgeler için dönemin arşivleri "güvenilir delillerin muhafaza edildiği mekânlar" olarak kabul edilmektedir (Wei Guo vd., "Archives as a Trusted Third Party in Maintaining and Preserving Digital Records in the Cloud Environment, **Records Management Journal**, C. 26, No: 2, 2016, s. 171-172).

218 Çiçek, "Elektronik Belge Yönetimi Uygulamalarında Bir Alt Sistem Olarak Dosya Yönetimi", **a.g.e**.

219 Selman Solhan, "Fizikselden Elektroniğe; Belge Yönetim ve Arşivleme Sürecinin Sürdürülebilirliği", **e-Beyas 2015 Sempozyumu Kurumsal Belleklerin Geleceği: Dijitalleştirme-Elektronik Arşiv-Elektronik Belge Yönetimi**, 21-22 Ekim 2015, ed.: Fahrettin Özdemirci vd., Ankara, Ankara Üniversitesi, 2016, s. 53-56.

incelenmesi için bir yaklaşım geliştirilmelidir. Buradan hareketle delil değerinin belgeyi oluşturan unsurlar, kullanılan teknolojik koşullar, kurumsal politika-prosedürler, mevzuat ile toplum düzeyleri bakımından kritik edilebileceği düşünülmektedir[220].



Şekil 1. Arşivsel Güvenilirlik Analizi Düzeyleri

Belge: Arşivsel güvenilirlik analizinde ilk ele alınacak unsur belgedir. Öncelikle belgeyi oluşturan unsurlar incelenir. Bu incelemede kontekst, arşivsel bağ, üstveriler ile taşıyıcı ortam ve form özellikleri gibi unsurlardan yararlanılır. Burada, kontekst ve arşivsel bağla ilgili olarak belge kim tarafından üretildi, nasıl kullanıldı ve dosyalandı, kimin emanetinde kaldı, hangi şartlarda nereye devredildi ve arşive nasıl geldi sorularına cevap aranır. Kontekst ve arşivsel bağa yönelik bu soruların yanı sıra, hangi üstveriler kullanıldı, taşıyıcı ortamın değişikliğe ihtiyacı olup olmadığı nasıl tetkik edildi, form özellikleri nasıl kayıt altına alındı şeklinde sorular geliştirilebilir.

Teknolojik Koşullar: Arşivsel güvenilirlik analizinde belgelerin üretildiği, transfer edildiği ve saklanıp arşivlendiği uygulama yazılımlarının ve kullanılan donanımların incelenmesi de önemli bir aşamadır. Burada, belge kim tarafından nasıl üretildi, kime iletildi, e-imza kontrolü hangi aralıklarla yapıldı, zaman içerisinde özgünlükleri hangi yöntemlerle kontrol edildi, donanımlar üreticisi tarafından önerilen

220 International Organization for Standardization [ISO], **18128 Risk Assesment for Records Process and Systems**, Cenevre[İsviçre], ISO, 2014, s. 4.

kullanım ömrü bittikten sonra yenilendi mi gibi sorular sorulabilmektedir. Ayrıca, e-belgelerin özgünlüklerinin kontrolü için arşiv bilimi bakış açısıyla geliştirilen yapay zekâ, derin öğrenme, elektronik delil elde etme gibi araçlardan da yararlanmak mümkündür[221].

Kurum: Belge ve teknolojik koşullar düzeyiyle birlikte, arşivsel güvenilirlik analizinde incelenebilecek bir diğer husus, belge yönetimi ve arşivcilikle alakalı kurumsal politika ve prosedürlerdir. Bu politika ve prosedürler incelenirken belge yönetimi politikası üst yönetim tarafından onaylanmış mı[222], prosedürler, belge üretme, dosyalama, imza süreçleri ve arşive devretme kurallarını içeriyor mu gibi sorular sorulabilmektedir[223].

Mevzuat: Kurumlar, politika ve prosedürlerini oluştururken gerçekleştirdikleri fonksiyon ve faaliyetlerle ilgili kanun, yönetmelik, genelge gibi mevzuata göre hareket ederler. İlgili mevzuatta, belgelerin saklama süresi, belgelerde bulunması gereken zorunlu üstveriler, belge türüne özgü form özellikleri gibi hususlar yer alabilmektedir. Bununla birlikte, ülkelerde bulunan milli arşivlerin belge yönetimi uygulamaları konusunda kurumları nasıl denetleyeceği arşivsel güvenilirlik analizinde incelenebilecek hususlar arasındadır. Burada, milli arşivler belgelerin arşivlenme kurallarını belirledi mi, teknolojik göç prosedürleri oluşturuldu mu, hangi formatların kullanılabileceği tayin edildi mi gibi sorular sorulabilmektedir.

Toplum: Arşivsel güvenilirliğin mevzuat düzeyini oluşturan unsurlar, hükümetler tarafından belirlenir. Hükümetler de toplumların ihtiyaçlarını karşılamak amacıyla çalışırlar. Bu nedenle belgelerin delil değerinin arşivsel güvenilirlik açısından incelenmesinde benimsenebilecek son düzeyin toplum düzeyi olduğu düşünülmektedir. Bu düzeyde, bir ülkedeki vatandaşların inceleyecekleri arşiv

---

221 Gregory Rolan vd., "More Human than Human? Artificial Intelligence in the Archive", **Archives and Manuscripts**, C. 47, No: 2, 2019. ; Frederick B. Cohen, "Digital Diplomatics and Forensics: Going Forward on a Global Basis", **Records Management Journal**, C. 25, No: 1, 2015.

222 Niyazi Çiçek, "E-Devlet Stratejisi Bağlamında Elektronik Belge Yönetimi için "Yazılı Politika" Gereksinimi: Türkiye'deki Uygulamalar Üzerine Bir İnceleme", **Türk Kütüphaneciliği**, C. 34, No: 3, 2020.

223 Heather MacNeil vd., "Authenticity Task Force Report", **The Long-term Preservation of Authentic Electronic Records: Findings of the INTERPARES Project**, s. 32-33, (Çevrimiçi) http://www.interpares.org/book/interpares_book_d_part1.pdf, 28 Aralık 2020.

malzemesi olmuş e-belgelere güven duymaları için hangi unsurlara dayandıkları araştırılmaktadır. Bu kısımda, güveni tesis eden araçlar neler olabilir, vatandaşlar e-belgelere hangi oranda güveniyor, duyulan güveni artıran unsurlar nelerdir şeklinde sorular yöneltilebilir[224].

1.3.3.5. Düzeyleri İnceleme Gerekçesi

Arşivsel güvenilirlik analizi düzeylerinin bazılarında kurumlar daha etkinken bazılarında daha pasiftir. Mesela, toplum ve mevzuat düzeyinde kurumların diğerlerine göre daha pasif olduğu ileri sürülebilir. Çünkü toplum ve mevzuat düzeylerinde kurumların kendi tasarrufları dışındaki faaliyetler söz konusudur. Örneğin toplum düzeyinde vatandaşların düşünceleri kritik edilmektedir. Her ne kadar kurumların yaptıkları icraatla vatandaşların düşüncelerini etkilediği bilinse de onların kurumlarda oluşan belgelere güven duyup duymayacağı kendi insiyatiflerindedir. Mevzuat düzeyinde ise hükümetlerin belirlediği kanun, yönetmelik, genelge gibi prosedürler incelenir. Hükümetler, bir faaliyet alanıyla ilgili düzenleme yaparken o alandaki kurumların görüşünü alabilmektedir. Fakat bu süreç, kurumların kendi dinamikleriyle şekillenememektedir. Kurumlar oluşturulan mevzuata uymakla mükelleftir. Bu nedenle mevzuat düzeyinde de kurumların pasif bir durumda olduğu ifade edilebilir.

Arşivsel güvenilirlik analizinin kurum, teknolojik koşullar ve belge düzeylerinde ise organizasyonların diğerlerine göre daha etkin olduğu düşünülmektedir. Çünkü bu düzeylerde organizasyonların kendi tasarrufları söz konusudur. Örneğin örgütler dosyalama ve arşive devirle ilgili prosedürler oluşturup donanımların ne zaman yenileneceğini belirleyebilmekte; log kayıtlarının nasıl saklanacağına karar verebilmektedir. Aynı zamanda, taşıyıcı ortamın ne zaman değiştirileceğini tayin edebilmekte ve zorunlu olanlar haricinde de kullanılabilecek üstverileri kararlaştırabilmektedir.

Belge, teknolojik koşullar ve kurum düzeylerinin diğerlerine göre daha etkin kabul edilmesi, örgütleri odak noktaya taşımaktadır. Bu durum, organizasyonların bu

---

224 Laura Millar, "An Obligation of Trust: Speculations on Accountability and Description", **American Archivist**, C. 69, No: 1, 2006, s. 76.

düzeylerle ilgili uygulamalarının incelenebileceğini düşündürmektedir. Bundan dolayı, tezde e-imzalı belgelerin arşivsel güvenilirliği, belge, teknolojik koşullar ve kurum düzeyleri açısından analiz edilmektedir.

Arşivsel güvenilirliğin getirdiği bu yaklaşımlara, bir sürecin hangi niteliklerde yapılması gerektiğini açıklayan standartlarda da rastlanılmaktadır. Standartlarda belgelerin delil değeriyle ilgili üstveri, kontekst, fonksiyon analizi, dosyalama, form özellikleri, saklama koşulları, teknolojik göç ve kurumsal politika ile prosedürler gibi hususların yer aldığı görülmektedir. Durum böyle olunca, belgelerin delil değerinin standartlar açısından da incelenebileceği düşünülmüştür.

Arşivcilik ve belge yönetiminin temel uygulama fonksiyonlarının açıklandığı bu standartlarda yer alan kriterlerin kurumlarda ve arşivlerde layıkıyla yürütülmesinin e-belgelerin delil değerini korumaya yönelik önemli bir ölçek olduğuna inanılmaktadır. Bu ölçek neticesinde geliştirilecek yöntemler, belgelerin güvenilirlik incelemelerine de kaynaklık edebilir. Burada, arşivcilik ve belge yönetimini etkileyen hem ulusal hem de uluslararası geçerliliği bulunan standartlar öne çıkmaktadır[225]. Standartlarda delil değeriyle ilgili olduğu düşünülen hususların arşivsel güvenilirlik analizinin belge, teknolojik koşullar ve kurum düzeyiyle ilişkilendirilebileceği düşünülmektedir.

---

225 Margaret Pember, "Sorting out the Standards: What Every Records and Information Professional Should Know", **Records Managament Journal**, C. 16, No: 1, 2006. Fakat, standartlarda bir sürecin hangi nitelikte yapılacağı ortaya konulsa da nasıl yapılacağı tam olarak açıklanmamaktadır. Bu nedenle standartların ülkelerin o alandaki geçmişlerini yeteri kadar dikkate almadığı ve dile getirilen hususların her ülkede aynı şekilde anlaşılamayabileceği ifade edilmektedir (AR Bell, "Standards and Standards Culture: Understanding the Nature and Criticisms of Standardisation", **Comma**, No: 2, 2011'den aktaran Greg Bak, "Trusted by Whom"? TDRs, Standards Culture and Nature of Trust", **Archival Science**, No: 16, 2016, s. 385. ; Gillian Oliver, "International Records Management Standards: The Challenges of Achieving Consensus", **Records Management Journal**, C. 24, No: 1, 2014, s. 25). Buna rağmen, bir ölçek oluşturması nedeniyle kurumların belge yönetimi pratiklerinin analiz edilmesinde standartlardan yararlanıldığı görülmektedir (Şahika Eroğlu ve Özgür Külcü, "TS 13298 Çerçevesinde Kurumsal Bilgi Yönetim Sistemleri ve Elektronik Belge Yönetimi Standartlarının Değerlendirilmesi: İçişleri Bakanlığı Örneği", **Bilgi Dünyası**, C. 15, No: 2, 2014. ; Julie McLeod vd., "Records Management Capacity and Compliance Toolkits: A Critical Assessment", **Records Managament Journal**, C. 17, No: 3, 2007. ; Johanna Gunnlaugsdottir, "Information and Records Management: A Precondition for a Well Functioning Quality Management System", **Records Managament Journal**, C. 22, No: 3, 2012).

1.4. Bilgi ve Belge Yönetimi Standartlarında E-Belgelerin Delil Değeri

1.4.1. Delil Değeri Unsurları

Bir hizmet ya da ürüne ilişkin üretim sürecinin kalite normlarını ortaya koymak amacıyla çıkarılan standartların belge yönetimi ve arşivcilik alanında da birçok örneğine rastlanmaktadır. Bu standartlar, belge üretilmesinden iş süreçlerinin açığa çıkarılmasına; kayıt, üstveriler, dolaşım, dosyalama, dosya planları gibi fonksiyonlarla belge yönetimi sistemlerinin kurulmasına; ayıklama-imha, sayısallaştırma (dijitalleştirme), transfer, uzun süreli koruma, sayısal süreklilik, kullanıcı hizmetleri ve uygulama yazılımlarının geliştirilmesine kadar birçok süreci kapsamaktadır. Hatta bu standartlar, belgelerin nasıl üretilmesi gerektiği ve bulunması gereken form özellikleriyle de alakalıdır. Böylece, belgenin türüne ve üretilmesine karar verildiğinde delil değerlerinin oluşmaya başladığı görülür. Fonksiyonun akışı boyunca delil değeri unsurları e-belgede şekil alır.

E-belgelerin delil değerine ilişkin unsurların anlaşılması, en başta kurum analizi yapılıp fonksiyonların açığa çıkarılmasıyla başlar. Bu süreçte, fonksiyonun nasıl yürütülmesi ve işlemler sırasında belgelerin nasıl üretilmesi gerektiğine dair kriterleri ortaya koyan standart gibi prosedürleri incelemek gerekir. Bu kriterler, belge arşivlendikten sonra da delil değeri analizinde kullanılabilir. Bundan dolayı, e-belgelerin üretilmesinden arşivlenmesine kadar olan süreci kapsayan belge yönetimi ve arşivcilikle ilgili standartlarda delil değerinin analiz edilebileceği çeşitli unsurlar görülmüştür. Bunlar, *fonksiyon analizi*, *değerlendirme*, *form özellikleri*, *kontekst*, *üstveriler*, *dosya ve saklama planları* ile *dosyalama* gibi daha çok arşivsel güvenilirliğin belge düzeyini niteleyebilecek unsurlardır.

Fonksiyon Analizi: Fonksiyon analizinde belgelerin oluşumuna kaynaklık eden kurumsal süreçler incelenmektedir. Süreçlerde yürütülen işlem adımlarında ne tür belge/lerin üretilmesi gerektiği görülür. Üretilen bu belgelerin yapılan işlemlerin delili olması için sahip olmaları gereken form özellikleri değerlendirilir[226]. Bununla

---

226 ISO, **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, 2020, s. 2. Burada fonksiyon analizinin iki türü olan iş analizi ve ardışık analizden yararlanıldığı görülmektedir. İş analizinde bir iş süreci bütün olarak analiz edilir. Bunun neticesinde belgelerin tasnifi yapılır. Sonrasında, belgelerin

birlikte, işlemleri gerçekleştirebilmek için gerekli olan üstveriler ile belgede bulunması gereken bilgiler yani içerik anlaşılmaya çalışılır; belgenin üretimi, kaydedilmesi ve yönetilmesi süreçleri ile imza yetkilileri tanımlanır[227].

Fonksiyon analizi sırasında üretilecek belge türüne karar verilirken aynı zamanda belgeyi oluşturacak düzenleyen, sorumlu, içerik, birim kodu ve dosya kodu gibi form özellikleri de belirlenir. Belgelerin tanımlanmasına yardımcı olacak bu özelliklerin belge formunda yer almasına dikkat edilerek delil değerinin korunması amaçlanır. Bunun neticesinde, işlemin türüne göre belgede bulunması gereken içerik, kontekst ve türe özgü yapısal özellikler, üstveri şemasının oluşturulması, kontrollü terminoloji kullanılması, risk analizi yapılması, gizlilik ve ivedilik derecelerinin tayin edilmesi gibi delil değeri kritik unsurları kararlaştırılır[228]. Bu unsurlar, fonksiyon analizi neticesinde ortaya çıkarılır ve belgelerin tanımlanmasında kullanılır.

Değerlendirme: Değerlendirme, "evrakların arşivlik değerine göre nihai tasfiyesine karar vermeyi kapsayan temel arşivcilik işlevi" olarak bilinmektedir[229]. Her ne kadar belgelerin tasfiye dönemiyle ilişkili olsa da bu kavramın belgenin üretilme safhasında da kullanılabileceği tartışılmıştır[230]. Fonksiyon analiziyle oluşan belgeler

---

erişim, muhafaza ve tasfiye koşulları belirlenir. Ardışık analizde ise süreçlerdeki her bir iş adımı incelenerek yapılacak işlemlerin sırası çıkarılır. Böylece, belgelerin hangi aşamada üretileceği belirlenir. Bununla birlikte, ardışık analizde sürecin rutin gidişatı ve bu gidişatta karşılaşılan değişkenler tespit edilir. Bunun sonucunda işlemleri gerçekleştirebilmek için gerekli olan üstveriler ile belgede bulunması gereken bilgiler yani içerik açığa çıkartılır; belgenin üretimi, kaydedilmesi ve yönetilmesi süreçleri ile imza yetkilileri tanımlanır (ISO, **26122 Work Process Analysis for Records**, Cenevre[İsviçre], ISO, 2008, s. V, 3-4, 8-9). ; Örgütlerdeki iş süreçlerinin analiziyle alakalı toplam kalite yönetimi bakımından TS 9001 Kalite Yönetim Sistemi ve ISO 10244 gibi Business Process Baselining and Analysis (Kurumsal Süreç Değerlendirme ve Analizi) gibi standartlar bulunsa da belgenin delil değeri arşivsel güvenilirlik açısından incelendiğinden ISO 16175-1, ISO 26122 ve ISO 30301 Standartları göz önünde bulundurulmuştur (TSE, **9001 Kalite Yönetim Sistemi Standardı - Şartlar**, Ankara, TSE, 2015. ; ISO, **10244 Business Process Baselining and Analysis**, Cenevre[İsviçre], ISO, 2010. ; ISO, **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**, **a.g.e.** ; ISO, **26122 Work Process Analysis for Records**, **a.g.e.** ; ISO, **30301 Management Systems for Records: Requirements**, Cenevre[İsviçre], ISO, 2019).

227 **a.g.e.**, s. 8-9.

228 **a.g.e.**, s. V, 3-4. ; ISO, **30301 Management Systems for Records: Requirements**, **a.g.e.**, s. 8-9.

229 **Arşivcilik Terimleri Sözlüğü**: **Almanca, İngilizce, Fransızca, İtalyanca, Hollandaca, Rusça ve İspanyolca Karşılıklarıyla**, Türkçe hazırlayan ve genişleten: Bekir Kemal Ataman, İstanbul, Librairie de Pera Yayınları, 1995, s. 23.

230 Değerlendirmede hangi belgelerin oluşup kaydedileceği, bu belgelerin ne kadar süre ile saklanacağını belirlemek için kurumsal faaliyetler incelenir. Ancak, değerlendirmenin bu özelliği delil değerinin korunması için yeterli gelmemiş olacak ki 2016 yılında güncellenen ISO

görülürken, değerlendirme yapılarak da belgelerin teknolojik göç işlemleri, üstveri şeması, dosyalama gibi belge yönetimi süreçleri açığa çıkarılır. Bu analiz neticesinde belge tanımlanarak onun türe özel hususiyetlerinden kaynaklanan delil değeri unsurları da anlaşılmış olur.

Bu durumda belgenin varlığı ya da yokluğunu anlamak olan değerlendirme sonucunda belge yönetimi ve bilgi güvenliği politikası, teknolojik göç stratejileri, kurumsal süreklilik ve risk yönetimi planı ile kişisel verileri koruma politikalarının geliştirilebileceği düşünülmektedir. Bununla birlikte, değerlendirmeden üstveri şeması, tasnif planı, dosyalama, belgeye erişim kuralları ile tasfiye yetkileri gibi belgelerle ilgili kontroller için de yararlanmak mümkündür[231]. Değerlendirme safhasında belirtilen bu kontrol araçlarının doğru işletilmesiyle belgelerin delil değerinin başarıyla korunması sağlanabilir.

Form Özellikleri: Antetten imzaya, tarihten eklere kadar belgelerin sahip olması gereken iç ve dış kaynaklı hususiyetler olarak tanımlanan form özellikleri belge türüne göre değişebilmektedir[232]. Hukuki normlar ve idari uygulamalara göre şekil alan işlemlerin neticesinde oluşan bu özellikler, her belge türü için temel delil değeri unsurlarıdır. Mesela, üniversitelerdeki doktora diplomalarıyla lisans diplomaları birbirinden farklı form özelliklerine sahiptir. Bu durum, belgelerin oluşumunu düzenleyen yasal ve idari prosedürlerden kaynaklanır. Bu prosedürlerle belirlenen form özellikleri, belgenin türünü belirlemede başvurulan temel kaynaklardan biridir.

Bu özelliklerin incelenmesiyle belgenin ait olduğu faaliyet ve fonksiyon ortaya çıkarılıp kontekst belirlenebilir. Durum böyle olunca, bir belgenin hukuki ve idari açıdan gerçekliğini ve geçerliliğini açıklayan bu form özelliklerini belgeler, arşivlendikleri dönemde de korumalıdır. Özgünlük ve tamlık nitelemesi bu özelliklere göre yapılır. Bu sebeple form özelliklerini arşivlenen belgenin başlıca delil değeri kritik unsurları olarak görmek mümkündür.

15489 Standardı ile kavramın mahiyetine yeni bir anlam yüklenerek kurumsal faaliyetler ve risklerin analiz edilmesi de gündeme getirilmiştir. Böylece, belgelerle ilgili kurumsal ihtiyaçlar, toplumsal beklentiler ve belge yönetimini etkileyen fırsat ve tehditlerin analiz edilmesi önerilmiştir (ISO, **15489 Records Management Part 1: Concepts and Principles,** Cenevre[İsviçre], ISO, 2016, s. 10).

231 ISO, **21496 Appraisal for Managing Records**, Cenevre[İsviçre], ISO, 2018, s. V.

232 Çiçek, **Modern Belgelerin Diplomatiği**, **a.g.e.**, s. 87, 115.

Örgütlerde sadece kurumda üretilen belgelerin değil, dışarıdan gelenlerin de form özelliklerinin korunması gerekir. Dışarıdan kuruma gelen bir belge, mevcut formatıyla, içerik ve yapısı değiştirilmeden, ait olduğu bileşenleriyle arasındaki ilişki korunarak uygulama yazılımına dâhil edilmelidir[233]. Fonksiyon analizi ve değerlendirme yapılıp belgelerde hangi form özelliklerinin kullanılacağı belirlendikten sonra belgenin kontekstinin açığa çıkarılması hedeflenir.

Kontekst: Belgelerin üretilmesinden arşive devrine kadar yaşam sürecinin evrelerindeki bağlamsal ilişkiyi anlamak olan kontekst, delil değeri analizinde kullanışlı bilgiler sunar. Örgütlerde bu kontekst bağlamında teşekkül eden belgeler, arşiv malzemesi olduklarında da bu ilişki ağını muhafaza etmelidir[234]. Böylece konteksti açığa çıkarmak, delil değeri unsurlarının anlaşılmasına yardımcı olur.

Bunun gerçekleşebilmesi için kurumsal faaliyet ve işlemleri şekillendiren iç ve dış dinamiklerin incelenmesi gerekir[235]. Örgütsel fonksiyon ve faaliyetler gerçekleştirilirken kurumun uymak zorunda olduğu ulusal ve uluslararası prosedürler, dış dinamikleri oluşturur. Kurumun iç dinamiklerine ise yönetişim, kurumsal yapı, görevler, politikalar, stratejiler, bilgi sistemleri, karar alma süreçleri ve iç paydaşlar örnek gösterilebilir[236]. Tüm bu dinamiklerin incelenmesiyle fonksiyon, faaliyet, işlem ve belge mimarisi ortaya çıkarılarak aralarındaki ilişki ağı tanımlanabilir[237].

Bu ağı tanımlamak için belgelerle üstveri ve ekleri arasındaki ilişkiyi korumak ve kuruma dışarıdan gelen belgeleri kurumun kendi dosya planına göre tasnif edip

---

233 ISO, **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**, **a.g.e.**, s. VI, 16, 20.

234 INTERPARES, **INTERPARES 2: Experiential, Interactive and Dynamic Records**, **a.g.e.**, s. 779.

235 ISO, **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**, **a.g.e.**, s. 2.

236 ISO, **26122 Work Process Analysis for Records**, **a.g.e.**, s. 5, 7. ; ISO, **18492 Long-term Preservation of Electronic Document-based Information**, Cenevre[İsviçre], ISO, 2005, s. 4-5. ; ISO, **30301 Management Systems for Records: Requirements**, **a.g.e.**, s. VI. ; ISO, **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**, **a.g.e.**, s. 2.

237 ISO, **26122 Work Process Analysis for Records**, **a.g.e.**, s. 5, 7. ; ISO, **18492 Long-term Preservation of Electronic Document-based Information**, **a.g.e.**, s. 4-5.

dosyalamak gibi yöntemler benimsenmektedir[238]. Bununla birlikte, kontekstin sürdürülebilirliği için uygulama yazılımlarının da sahip olması gereken özellikler bulunmaktadır. Bunlar, belgeleri kontekstinden ayırmadan üretip kaydetmek, üstverileri kayıt altına almak, belgeleri ihtiyaç duyulduğu sürece muhafaza etmek, devamlılıklarını sağlamak ve tasfiye işlemlerini gerçekleştirmek gibi özelliklerdir[239]. Bu hususlar, kontekst açısından e-belgelerin delil değeri kritik unsurları olarak değerlendirilebilir.

Üstveriler: 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 gerçekliğini artırır[240]. Durum böyle olunca, belge tasarlanıp üretilirken üretilme amacı, yapısal özellikler, kontekst bilgisi, sorumlu ve düzenleyen gibi delil değeri unsurlarını içeren bir üstveri şeması oluşturulur[241].

Bu unsurların standart bir yapıda tanzimi ve mahiyetlerinin doğru kavranması amacıyla hazırlanan bir şablon olan üstveri şeması, üstveri alanlarında kontrollü terminolojilerin kullanılmasına imkân verir. Belgeler, farklı kaynak kodları kullanılarak geliştirilmiş yazılımlarda üretilse dahi standart bir yapıdaki üstveri şemalarına sahiplerse üstveri elemanlarıyla birlikte transfer edilerek bu şemalar korunabilir. Böylece, uygulama yazılımları değişse de standart üstveri şemaları kullanıldığı için üstverilerde süreklilik sağlanmış olur[242]. O hâlde, layıkıyla geliştirilen üstveri şemalarından arşivlenen e-belgelerin delil değerinin korunmasında yararlanılabilir.

Belge yönetimindeki temel üstveri standardı olarak kabul edilen ISO 23081 Belge Üstverilerinin Yönetimi Standardı'nda belgenin içeriği, yapısal özellikleri ve kontekst bilgileriyle sayısal korumayla ilişkilendirilen teknolojik göç gibi çeşitli üstverilerin belirlendiği görülmektedir. Standart'ta belgelerle alakalı olarak

---

238 ISO, **16175-2 Processes and Functional Requirements for Software for Managing Records Part 2: Guidance for Selecting, Designing, Implementing and Maintaining Software for Managing Records**, Cenevre[İsviçre], ISO, 2020, s. 8-12.

239 **a.g.e.**, s. 2, 6.

240 ISO, **23081-2 Managing Metadata for Records Part 2: Conceptual and Implemantation Issues**, Cenevre[İsviçre], ISO, 2009, s. 3-4. ; ISO, **23081-1 Managing Metadata for Records Part 1: Principles**, Cenevre[İsviçre], ISO, 2017, s. 2-3.

241 ISO, **15489 Records Management Part 1: Concepts and Principles**, **a.g.e.**, s. 5.

242 ISO, **23081-1 Managing Metadata for Records Part 1: Principles**, **a.g.e.**, s. 11.

düzenleyen, dosya ve seri, üretildiği uygulama yazılımı ve sürümü, kayıt formatı, formatın değiştirildiği ve değişimin onaylandığı tarih gibi üstveriler, delil değeri açısından kritik unsurları olarak kullanılabilir. Bununla birlikte, tasfiye ve erişim kuralları da üstverilerde yer almaktadır[243]. Görüldüğü gibi üstveriler, belgelerin yaşam döngüsündeki tüm safhaları açıkladığından delil değerinin korunmasında oldukça önemli bir konuma sahiptir.

Durum böyle olunca, üstverilerin üretildiği uygulama yazılımlarında bazı hususlara dikkat edilmelidir. Uygulama yazılımları, dışarıdan gelen belgelerin üstverilerini de tanıyabilmeli, bunları kayıt altına alarak muhafaza etmelidir. Üstverilerde yaşanacak herhangi bir değişiklik, açıklamalarıyla birlikte müstakil bir log kaydı olarak tutulmalıdır[244]. Üstveri dosyasının belgeden ayrı olarak saklanması fakat belgenin her aşamasında onunla birlikte hareket etmesi gerekmektedir. Belge imha edilse bile bazı alanları hiç silinmeyecek şekilde bir üstveri kaydı oluşturulmalıdır[245]. Bununla birlikte, üstveri dosyalarının da korunması gerekir. Bunun için EBYS'lerde üstveri bütünlüğü kontrol edilebilmeli, üstveri dosyasına erişim seviyeleri belirlenebilmeli, sistemsel hatalarla karşılaşıldığında iyileştirme araçları geliştirilebilmeli, geri yükleme prosedürleri oluşturulabilmeli ve gerekli olduğu durumlarda teknolojik göç yapılabilmelidir. Üstverilerin güvenilirliği, belgelerin güvenilirliği için alınan önlemlerden ayrı düşünülmemelidir[246]. Çünkü üstveriler, belgenin özgünlüğünü oluşturan temel unsurlar olduğundan delil değeri için de başlıca kritik elemanlarındandır.

Dosya ve Saklama Planları: Kurumda oluşan belgeleri ait olduğu fonksiyona göre tasnif eden dosya planları, düzenlemenin nasıl yapılacağını açıklarken yasal ve idari prosedürler kapsamında belgelerin ne kadar süre saklanacağını da gösterir[247]. Bu planlar, güncel dönemde belgelerin yönetilme şeklini açıkladığı gibi imhalıkları tespit

243 ISO, **ISO 23081-1 Managing Metadata for Records Part 1: Principles**, **a.g.e.**

244 ISO, **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**, **a.g.e.**, s. 7, 8, 12.

245 ISO, **ISO 23081-1 Managing Metadata for Records Part 1: Principles**, **a.g.e.,** s. 5-6.

246 **a.g.e.**, s. 10.

247 ISO, **27003 Information Security Management Systems: Guidance**, Cenevre[İsviçre], ISO, 2017, s. 26-28. ; ISO, **15489 Records Management Part 1: Concepts and Principles, a.g.e.**, s. 14.

etmeye yararken, sürekli saklanması gerekenlerin de arşiv malzemesi olarak ayrılmasını sağlar. Fonksiyonel yaklaşımla geliştirilen planlar, örgütün fonksiyon, faaliyet ve işlem ilişkisini şema olarak ortaya koyar[248]. Üretilen belgenin bu hiyerarşiye göre yönetilmesi gerekir. Bundan dolayı arşivlenen e-belgelerin delil değeri analizinde bu unsurlar oldukça etkilidir. Durum böyle olunca, uygulama yazılımları belgeleri daha üretim safhasındayken ait olduğu faaliyetle ilişkisinin kurulması gibi bir sistem kriterini dosya planına göre sağlamalıdır[249]. Dosyalama işi ve dosya planlarının kullanılması, belgelerin işlemi bittikten sonra değil, -belgeye dosya kodu verilerek- daha üretilme safhasındayken başlar. Plandan belirlenerek belgeye yazılan bir dosya kodu, başlıca form özelliklerinden biri olurken aynı zamanda delil değeri kritik unsuru olarak kullanılabilir. Bu nedenle olsa gerek dosya planları, uygulama yazılımlarının vazgeçilmez bir sistem kriteri niteliğindedir[250].

Dosyalama: Dosyalama, kurumlarda aynı fonksiyon kapsamında oluşan belgeleri aralarında organik bağ kurarak bütünlük içerisinde bir araya getirme işlemi olarak tarif edilebilir[251]. Organik bağ, bir vaka ya da konu ışığında oluşurken belgeler de bu bağ etrafında kümelenerek bir araya getirilir[252]. Vaka/konuya göre dosya kodu vermek gibi araçlar kullanılarak oluşturulan organik bağ, aynı zamanda belgelerin delil değerini işaret eden entelektüel bir eylem olarak kabul edilebilir.

"Vaka dosyaları, bir olay, durum ya da vakayla ilgili bütün belgelerin bir arada dosyalanmasıyla oluşur"[253]. Bu tür dosyalara personel, ihale ve dava dosyaları örnek verilebilir. Mesela bir personel dosyasında, personelin işe giriş belgelerinden, izinlerine, çeşitli konulardaki başvurularından şikâyetlere kadar pek çok farklı muhtevaya sahip belgeler bulunur. Bu belgeleri muhtevasına göre dosyalamak

248 TSE, **13298 Elektronik Belge Yönetim Sistemi Standardı**, **a.g.e.**, s. 4.

249 ISO, **17068 Trusted Third Party Repository for Digital Records**, ISO, Cenevre[İsviçre], 2017, s. 10-12.

250 ISO, **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**, **a.g.e.**, s. 17. ; ISO, **16175-2 Processes and Functional Requirements for Software for Managing Records Part 2: Guidance for Selecting, Designing, Implementing and Maintaining Software for Managing Records**, **a.g.e.**, s. 11.

251 Çiçek, **Kurumsal Bilgi ve Belge Yönetimi**, **a.g.e.**, s. 154.

252 **a.g.e.**, s. 155.

253 **a.g.e.**, s. 172.

mümkün olsa da belgelerin mahiyeti söz konusu personelle ilgilidir. Bu mahiyet, farklı muhteva ve forma sahip ancak kişiyle ilgili olan belgelerin personel dosyasında bulunmasını gerekli kılar. Bu nedenle, vaka dosyalarında aynı fonksiyon sonucunda oluşan farklı tür ve formattaki belgeler, aralarında organik bağ kurularak bir araya getirilir. Vaka dosyalarının teşekkülü böyleyken konu dosyalarında konu esas alınır. Konu dosyaları, her yıl aynı şekilde yürütülen fonksiyonlar için oluşur. Bu dosyalar, genellikle aynı dosya adı ve kodu ile yıl başlarında açılır, yıl sonlarında kapanır. Konu dosyaları, aynı konuda giden-gelen ve türleri farklı olan belgelerin birikmesiyle oluştuğu gibi sözleşmeler, yönetim kurulu kararları ve makam olurları gibi tek tip belge türünden de meydana gelebilir[254].

Konu ve vaka dosyası ayrımı yapılmadığı takdirde, aynı fonksiyon sonucunda oluşan belgelerin bir arada tutulmaması riski oluşur. Bunun neticesinde kurumsal faaliyetlerin nasıl gerçekleştirildiğinin tespiti noktasında ciddi güçlükler yaşanabileceği ileri sürülebilir. Mesela bir ihaleyle ilgili soruşturma evrakı, ihaleyle ilgili tüm belgelerin yer aldığı vaka dosyasında bulunmayıp soruşturma yazışmaları gibi bir konu dosyasında yer alıyorsa söz konusu ihale süreciyle ilgili kontekst bilgisinin doğru şekilde açığa çıkarılamaması riski doğabilir. Başka bir deyişle bir vaka dosyasında bulunması gereken belge, alakasız bir dosyaya kaldırıldığında ya da vaka kapsamındaki faaliyet ve işlemlerle hiç alakası olmayan bir belge o vaka dosyasına girdiğinde, kontekstin doğru şekilde açığa çıkarılması engellendiği gibi sahtecilik durumu da gündeme gelebilir. Bu risk, belgenin delil değerinden şüphe duyulmasına sebep olabilir. O hâlde, delil değerinin başarıyla korunması için konu-vaka dosyası ayrımının yapılması gerektiği gibi, belgeler de organik bağ ışığında bütünlük içerisinde ait olduğu dosyasında bulunmalıdır.

Konu ve vaka dosyaları için güncel dönemde sağlanması gereken bu koşul, arşiv safhasında da muhafaza edilmelidir. Çünkü doğru dosyalama, işlemlerin delili olan belgelerin delil değerini koruduğu gibi arşive devredildiklerinde de aynı değerin korunmasına yardımcı olur. Delil değerinin korunması için arşivlenen belgelerin en az bir dosyayla, dosyaların da en az bir seriyle ilişkilendirilmesi son derece önemlidir. Belge hiyerarşisi olarak adlandırılan bu ilişki ağı, işlem, belge, faaliyet, dosya,

254 **a.g.e.**, s. 170.

fonksiyon, seri ve birim münasebetini kurarak açığa çıkarılabilir[255]. Bu sebeple arşivlenen belgelerin ait oldukları konu ya da vaka dosyalarıyla bunların doğduğu fonksiyon ve seriyle olan ilişkileri koparılmadan devam ettirilmelidir.

Kâğıt belgelerle ilgili geçerli olan bu ilişki ağı prensibi elektronik belgeler için de vazgeçilmezdir. Hâliyle üretilmesini sağlayan uygulama yazılımı buna imkân vermelidir. Fakat zaman içerisinde sayısal ortamın kırılganlığı nedeniyle bu ilişkinin korunamama riski bulunmaktadır. Durum böyle olunca, belgelerin güncel kullanımı sırasında oluşan bu ilişki ağı arşiv döneminde de korunmalıdır. Olumsuz teknolojik koşullardan kaynaklanan sebepler bunu engellememelidir.

1.4.2. Önerilen Teknolojik Koşullar

Donanım ve yazılım ürünü bilgi teknolojisi araçlar vasıtasıyla üretilen e-belgelerin sürdürülebilirliğini sağlamak için standartlarda birtakım kriterler belirlendiği görülmektedir. Arşivcilik ve belge yönetimiyle ilgili standartlar, belgelerin yetkisiz değişimlerden korunmasından[256] teknolojik eskimeye önlem almak için belge formatının yenilenmesine[257], bir kez yazılabilir ortamların kullanılmasından disklerdeki veri kaydetme hatalarını tespit edebilmek için döngüsel artıklık denetimi (Cycle Redundancy Check - CRC)[258] yapılmasına ve belgeler için özet değeri alınmasına kadar[259] teknolojik koşullarla ilgili birçok kriteri içerir. Örneğin bu kriterler, birlikte çalışabilirlik esaslarına uyum, onay ve kayıt prosedürlerine bağlılık, log kayıtları ve denetim günlüklerinin tutulması, yazılım ve donanım koşullarının sürdürülebilir olması, erişim seviyelerinin tanımlanması ve teknolojik göç şartlarının belirlenmesidir. Tüm bunlar, arşivsel güvenilirliğin teknolojik koşullar düzeyini yapılandırır. Daha baştan e-belgelerin üretim aşamasında devreye alınan bu kriterler, arşivlenen belgelerin delil değeri analizinde kullanılabilir.

---

255 TSE, **13298 Elektronik Belge Yönetim Sistemi Standardı**, **a.g.e.**, s. 6.

256 ISO, **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**, **a.g.e.**, s. 5-6.

257 ISO, **18492 Long-term Preservation of Electronic Document-based Information**, **a.g.e.**, s. 7.

258 Döngüsel artıklık denetimi, elektronik ortamda oluşan verilerdeki değişimi tespit edebilmek için kullanılan bir algoritmadır (**a.g.e.**, s. 6).

259 ISO, **27035-2 Information Security Incident Management Part 2: Guidelines to Plan and Prepare for Incident Response**, Cenevre[İsviçre], ISO, 2016, s. 32.

Birlikte Çalışabilirlik: E-belgeler için birlikte çalışabilirlik, belgelerin başka yazılımlarda da okunabilir olmasını ifade eder. Türkiye'de arşivlenen e-belgelerin delil değerinin korunmasının gereklerinden biri, belgelerin Birlikte Çalışabilirlik Esasları Rehberi'ndeki ilkelere uyumlu olarak üretilmesidir[260]. Bu rehber, belgelerin formatı[261], EBYS uygulamalarında kullanılacak standartlar gibi ilkeler belirlemiştir. Rehber'de e-belgelerin üretilip arşivlenmesinde TS 13298 Standardı'nın esas alınması ifade edilmektedir.

TS 13298 Standardı'nda birlikte çalışabilirlikle ilişkilendirilen hususlar şöyle belirtilebilir: Belgeyi üreten ve belgenin muhatabı olan kamu kurumu/biriminin Devlet Teşkilatı Merkezi Kayıt Sistemi (KAYSİS)'deki kurum kimlik kodunun kullanılması zorunludur. Bununla birlikte, uygulama yazılımlarının kurum kimlik kodunu otomatik olarak çekmesi sağlanmalıdır. Gerçek kişilerle yapılan yazışmalarda ise Kimlik Paylaşım Sistemi ve Ulusal Adres Paylaşım Sistemi'ndeki bilgilerin kullanılması önerilmektedir. Tüzel kişilerle yapılacak yazışmalarda Merkezi Tüzel Kişilik Bilgi Sistemi, Merkezi Sicil Kayıt Sistemi (MERSİS), Vakıf Bilgi Yönetim Sistemi ve Dernekler Bilgi Sisteminin kullanılması tavsiye edilmektedir[262]. TS 13298 ve Birlikte Çalışabilirlik Esasları Rehberi'ndeki hükümler neticesinde belgelerin Türkiye Cumhuriyeti kimlik numarası, KAYSİS kimlik kodu ve evrak kayıt işlemlerinde alınan referans numarası gibi tek biçim tanımlayıcılara sahip olması gerektiği anlaşılmaktadır. Durum böyle olunca, bu gereklilik arşivlenen e-belgelerin delil değeri kritik unsuru olarak benimsenebilir. Kurumlarda oluşan tüm belgeler ve belgeyle ilişkili bileşenler tek biçim tanımlayıcılara sahip olmalıdır[263].

Uygulama yazılımlarının tek biçim tanımlayıcılar oluşturmanın yanı sıra birlikte çalışabilirlikle ilişkilendirilebilecek diğer özellikleri de söz konusudur. Bunlar, kurum dışından gelen belgeleri okunabilir bir biçimde sisteme dâhil etmek ve kurumda üretilen belgelerin başka uygulama yazılımlarında da okunabilir olması gibi

---

260 Türkiye Cumhuriyeti Kalkınma Bakanlığı Bilgi Toplumu Dairesi, **e-Dönüşüm Türkiye Projesi: Birlikte Çalışabilirlik Esasları Rehberi**, **a.g.e.**

261 Kurumlar arasındaki yazışmalarda metin tabanlı belgeler PDF/A, sayısal grafik ve diyagramlar Graphics Interchange Format (Grafik Değiştirme Formatı [GIF]), sayısal fotoğraflar ise JPEG formatında olmalıdır (**a.g.e.**).

262 TSE, **13298 Elektronik Belge Yönetim Sistemi Standardı**, **a.g.e.**, s. 16.

263 ISO, **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**, **a.g.e.**, s. 8.

özelliklerdir. Bu gereklilik için açık kaynak kodlu ya da endüstri standartları ışığında geliştirilen formatlar tercih edilebilir[264].

Onay ve Kayıt Prosedürleri: E-belgedeki irade beyanının tespit edilmesi için kullanılan e-imza, zaman damgası, kurumsal mühür ve KEP gibi onay ve kayıt prosedürleri, ilk olarak belgelerin güncel safhasında işletilse de belge imha edilene kadar korunmalıdır. Bu prosedürler, mevzuatın tanımladığı şifreleme algoritmaları ve standartlar gibi birtakım teknolojik protokollerin kullanılmasını gündeme getirmektedir. Geliştirilen uygulama yazılımları bu protokollere uyumlu olmalıdır[265].

Onay ve kayıt prosedürleriyle ilgili olarak delil değeri analizinde kullanılabilecek diğer unsurlar ise belgedeki imza ile yetkinin uyumlu olması ve zaman içerisinde imza oluşturma verisinin değiştirilememesi olarak öne çıkmaktadır. Belgedeki imza ile yetkinin uyumlu olması için belge, ilgili işlemden sorumlu olan kişiler tarafından düzenlenmelidir[266]. Zaman içerisinde imza oluşturma verisinin değişmemesi için ise belgelerin European Telecommunications Standard Institute (Avrupa Telekomünikasyon Standartlar Enstitüsü [ETSI]) ve TÜBİTAK gibi kuruluşlar tarafından çıkarılmış ve mevzuat tarafından tanınmış e-imza formatlarıyla imzalanması önerilmekte, döngüsel artıklık denetiminin yapılması tavsiye edilmektedir[267].

Log Kayıtları ve Denetim Günlükleri: Belgelerin ne zaman, kim tarafından, nasıl, hangi yazılım ve donanım araçlarında düzenlendiği ve arşive nasıl devredildiği gibi bilgiler sunan log kayıtları ve denetim günlükleri, aidiyet zincirinin kurulmasına yardımcı olur. Log kayıtlarında hangi işlemin, kim tarafından ne zaman yapıldığı belirtilirken; denetim günlüklerinde bu işlemin yapıldığı bilgisayarın özelliklerinden, işlem sonucunda veri tabanında meydana gelen gelişmelere kadar pek çok ayrıntı yer

---

264 **a.e.**

265 TSE, **13298 Elektronik Belge Yönetim Sistemi Standardı**, **a.g.e.**, s. 28.

266 ISO, **14641 Design and Operation of An Information System for the Preservation of Electronic Documents: Specifications**, ISO, Cenevre[İsviçre], 2018, s. 18.

267 ISO, **10789 Information and Documentation Management**, Cenevre[İsviçre], ISO, 2011, s. 6, 11-12.

almaktadır[268]. Durum böyle olunca, bu kayıtlar ve denetim günlükleri arşivlenen e-belgelerin delil değeri analizinde kullanılabilir.

Ancak, bu analizin yapılabilmesi için log kayıtlarının bazı özelliklere sahip olması gerekir. Bunlar, sisteme kaydedilen belgeler, açılan ve kapatılan dosyalar, kullanıcıların yaptığı işlemler ve kullanılan onay prosedürleri gibi hususlara ilişkin bilgilerin otomatik oluşmasıdır[269]. Bu özelliklerdeki log kayıtları değiştirilmeyecek ve silinmeyecek şekilde korunmalı, gerektiğinde doğrulanabilmelidir[270]. Diğer bir deyişle, log kayıtlarının bütünlüğü de kontrol edilmeli;[271] bu kayıtların günlük raporları oluşturulup zaman damgasıyla damgalanmalıdır[272].

Log kayıtlarında olduğu gibi denetim günlüklerinin arşivlenen e-belgelerin delil değeri analizinde kullanılabilmesi için bazı hususiyetlere sahip olmaları gerekir. Örneğin, denetim günlükleri herhangi bir müdahaleye gerek duymadan sistem tarafından otomatik oluşmalı ve güvenli bir şekilde saklanmalıdır. Bu günlüklerin güvenli bir şekilde saklanması için bir kez yazılabilir disklerin kullanılması önerilmektedir. Eğer bir kez yazılabilir değil de yeniden yazılabilir ortamlar kullanılıyorsa diskteki veriler üzerinde değişimlerin olması engellenmelidir. Böyle yapılarak denetim günlüklerine erişimde bir sorun yaşanıp yaşanmadığı ve değiştirilip değiştirilmediği belirli aralıklarla kontrol edilmelidir[273].

Uygulama Yazılımları ve Depolama Donanımları: E-belgelerle ilgili olarak kullanılan uygulama yazılımları ve depolama donanımlarının teknik ve teknolojik özelliklerinde çeşitli kriterler aranır. Bunlar, belgelerin değiştirilmemesini sağlayan önlemlerin alınması, uygulama yazılımlarındaki veri tabanlarının belgenin bütünlüğünü koruyacak bir yapıda olması, hem uygulama yazılımlarına hem de depolama

---

268 ISO, **15801 Electronically Stored Information: Recommendations for Trusworthiness and Reliability**, Cenevre[İsviçre], ISO, 2017, s. 37.

269 TSE, **13298 Elektronik Belge Yönetim Sistemi Standardı**, **a.g.e.**, s. 20-24. ; ISO, **10789 Information and Documentation Management**, **a.g.e.**, s. 11. ; ISO, **27040 Security Techniques: Storage Security**, Cenevre[İsviçre], ISO, 2015, s. 48-49.

270 ISO, **18829: Assessing ECM/EDRM Implementations: Trustworthiness**, Cenevre[İsviçre], ISO, 2017, s. 6.

271 ISO, **27040 Security Techniques: Storage Security**, **a.g.e.**, s. 58.

272 "RYY", **a.g.e.**

273 ISO, **27040 Security Techniques: Storage Security**, **a.g.e.**, s. 38-39.

donanımlarına ilişkin teknik ve teknolojik özelliklerin kayıt altına alınması ve depolama donanımlarının kullanım ömrü bittikten sonra yenilenmesi gibi hususlardır.

Uygulama yazılımları ve depolamaya ilişkin özelliklerin kayıt altına alınmasında sistem tanımlama kılavuzunun oluşturulduğu görülmektedir. Bu kılavuzda, internet ağı, veri ve yazılım mimarisi, kullanılan şifreleme algoritmaları, uygulama yazılımlarının kaynak kodları, kullanılan donanımların seri numaraları ile depolama ortamının sıcaklık ve nem gibi koşulları belirtilebilmektedir[274]. Bununla birlikte, sistem tanımlama kılavuzunda belirtilen uygulama yazılımlarının veri tabanlarında belgelerin delil değerini etkileyecek çeşitli özellikler aranır. Bunlar, bölünmezlik, tutarlılık, diğer nesnelerden ayrılabilme ve süreklilik (atomicity, consistency, isolation, durability - ACID) olarak öne çıkmaktadır[275]. Bu özellikler sayesinde yapılan işlemin kim tarafından yapıldığını tespit etmek gibi tanımlanabilirlikle ilgili hususlar anlaşılabilmektedir. Durum böyle olunca, sistem tanımlama kılavuzunda yer alan bu nitelikler, belgelerin delil değeri analizinde kullanılabilecek önemli araçlar olarak karşımızda durmaktadır.

Sistem tanımlama kılavuzunda aranan bir diğer özellik, belgelerin zaman içerisinde değiştirilmeden muhafaza edilmesini sağlayacak hususların yer almasıdır. Çünkü bu nitelik, delil değeri unsurlarından olan belge bütünlüğünün bir gereğidir. Bütünlüğün muhafazası için bir kez yazılabilir disklerin kullanılması, belgedeki değişimleri kontrol eden otonom araçlardan faydalanılması, belgeler sisteme kaydedildiği gibi sağlama toplamının (checksum)[276] veya özet değerinin hesaplanması, log kayıtlarının incelenmesi, belgelerin birbirinden bağımsız olarak

---

274 ISO, **15801 Electronically Stored Information: Recommendations for Trusworthiness and Reliability**, **a.g.e.**, s. 32-33. ; ISO, **14641 Design and Operation of an Information System for the Preservation of Electronic Documents: Specifications**, **a.g.e.**, s. 8. ; ISO, **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**, **a.g.e.**, s. 11.; UNESCO, **Software Heritage Web Sitesi**, (Çevrimiçi) https :// en. unesco. org/ softwareheritage, 22 Ağustos 2020.

275 ISO, **15801 Electronically Stored Information: Recommendations for Trusworthiness and Reliability**, **a.g.e.**, s. 19-20. ; Nurullah Çakır, SQL Server ACID Kuralları, (Çevrimiçi) http :// www.veritabani.gen.tr/2017/10/18/sql-server-acid-kurallari/, 8 Nisan 2020.

276 Bu yöntemde her bayt, 16 ya da 32 bitlik bir polinoma tabi tutulmakta ve oluşan değer, sonraki kontrollerde referans olarak kullanılmaktadır (Mazlum Yalçınkaya, "Rekabet Hukuku Uygulamaları Kapsamında Elektronik Delil", Yayınlanmamış uzmanlık tezi, Rekabet Kurumu, Ankara, 2015, s. 17, (Çevrimiçi) https://www.rekabet.gov.tr/Dosya/uzmanlik-tezleri/143-pdf, 5 Mart 2020).

farklı konumlarda saklanması ve felaket kurtarma planlarının hazırlanması gibi yöntemlere başvurulmaktadır[277]. Bununla birlikte, belgelerin bütünlüğünü bozma ihtimali bulunduğundan sistem bakımlarının da incelenmesi gerektiği düşünülmektedir. Burada, bakımların kim tarafından yapıldığı, bakımlar sırasında karşılaşılan hatalar ve bu hatalar hakkında yürütülen işlemler kayıt altına alınabilir[278].

Uygulama yazılımlarında oluşan e-belgeler, saklama ünitelerinde muhafaza edilirler. Bundan dolayı, saklama ünitelerinde donanımsal ve yazılımsal olmak üzere çeşitli kriterler aranır. Donanımsal kriterlere tercih edilen ürünlerin üreticilerin tavsiye ettiği ürün ömrü süresince ve nem, sıcaklık gibi belirlenen çevresel şartlarda kullanılması örnek verilebilir[279]. Yazılımsal kriterler ise saklama ünitelerinde belgelerin muhafaza şekliyle ilgilidir. Burada dikkat çeken yazılımsal kriterlerden ilki, belgelerin saklama konumlarının ayrılması yani arşivlenen belgelerin sadece kendilerine hasredilmiş alanlarda tutulması gerektiğidir[280]. Diğer bir ifadeyle, arşivlenen belgeler henüz arşivlenmeyenlerden (güncel belgeler) ayrı alanlarda muhafaza edilmelidir. Görülen bir diğer yazılımsal kriter ise farklı saklama süresine sahip belgelerin saklama ünitelerinin ayrı bölümlerinde tutulmasıdır[281]. Mesela, güncel belgelerin saklanmasında arşivlenmesi düşünülen ve arşivlenmeyecek belgeler ayrımı yapılabilir. Böylece, bir kategorideki belgeler için yapılacak teknolojik göç, e-imza ve zaman damgası güncellemeleri gibi belgelerin delil değerini tehdit edebilecek muamelelerin diğer kategoridekileri etkilemesinin önüne geçilebilir.

Düzenleme ve Erişim Seviyesi: Erişim seviyesi, belgeleri kimin düzenleyebileceğini ve kimlerin erişilebileceğini ifade eder. Belge, onu üretme yetkisine sahip kişiler tarafından düzenlenir. Böylece, bir delil değeri unsuru olan kişi

277 ISO, **18492 Long-term Preservation of Electronic Document-based Information**, **a.g.e.**, s. 15-16. ; ISO, **27040 Security Techniques: Storage Security**, **a.g.e.**, s. 48-49. ; ISO, **15801 Electronically Stored Information: Recommendations for Trusworthiness and Reliability**, **a.g.e.**, s. 32-33. ; ISO, **11506 Archiving of Electronic Data: Computer Output Microform (COM)/Computer Output Laser Disc (COLD)**, Cenevre[İsviçre], ISO, 2017, s. 3, 14.

278 ISO, **15801 Electronically Stored Information: Recommendations for Trusworthiness and Reliability**, **a.g.e.**, s. 26-27.

279 TSE, **13298 Elektronik Belge Yönetim Sistemi Standardı**, **a.g.e.**, s. 30-31.

280 ISO, **27040 Security Techniques: Storage Security**, **a.g.e.**, s. 43-44.

281 ISO, **15801 Electronically Stored Information: Recommendations for Trusworthiness and Reliability**, **a.g.e.**, s. 32-33.

ile imzanın uyumlu olması sağlanır. Uygulama yazılımlarında düzenleyene yönelik yöntemler benimsenir. Mesela, belge düzenleme yetkisine sahip kişiler, görevleri haricindeki fonksiyonlarda bu yetkiye sahip olmamalıdır. Aksi takdirde imza ile yetkinin uyumu riske gireceğinden belgenin delil değerinde şüphe oluşabilecektir.

Düzenlemeyle ilgili dikkat edilen bir diğer husus, görev değişikliklerinde yetkilerin de aktarılmasıdır. Örneğin bir yetkilinin görevi değiştiğinde, göreviyle ilgili bir konuda oluşan gizli bir belgenin açılması gerekebilir. Bu gizli belgeye o görevdeki yetkili kişinin şifresiyle erişildiği bir durum söz konusuysa göreve atanan yeni kişilere de şifre çözme yetkisi verilmelidir[282].

Üretildiği fonksiyondan dolayı belgeler, kişiye özel, hizmete özel, gizli ya da çok gizli olabilir. Burada belgeyi düzenleme ve erişim seviyesi, kişinin onun işlemini yürütmeye yetkili olup olmamasına göre belirlenir. Bundan dolayı, erişim seviyeleri tayin edilirken belgelerin statüsüne göre erişim yetkileri kararlaştırılır. Mesela fonksiyonu yürütmekle görevli olmayan birinin, o fonksiyona ait belgelere erişim yetkisi bulunmamalıdır[283]. Aksi takdirde, gizlilik hükümleri uygulanmamış mı, sistem kendisinden beklendiği gibi çalışmamış mı gibi sorular sorulacak ve bunlar belgenin delil değerinden şüphe edilmesine neden olabilecektir.

Teknolojik Göç: Belgelerin güncel depolama ünitelerine aktarılması, uygulama yazılımının yenilenmesi ya da dosya formatlarının güncellenmesi gibi işlemler olarak bilinen teknolojik göç, teknolojik eskimenin önüne geçilmesi için kullanılır. Bu göç sürecinin layıkıyla yürütülebilmesi için uygulamaya ilişkin yöntemi açıklayan dokümantasyon mutlaka hazırlanmalıdır.

Teknolojik göç işlemleri zaman, emek ve para isteyen bir süreçtir. Bunun için kurumların, yetkin personel, insan ve teknoloji kaynağı, uygun teçhizat, gerekli zaman ve para ile kalite kontrolünü gerçekleştirebilecek kapasiteye sahip olması gerekir. Bu hususlar, kurumların teknolojik göç ettirme işlemleriyle ilgili bir rehber hazırlamasını gündeme getirmektedir. Bu rehberde, teknolojik göçle ilgili planlama, test, gerçekleştirme, doğrulama ve onaylama süreçlerine ilişkin hususların yer alması

282 ISO, **27040 Security Techniques: Storage Security**, **a.g.e.**, s. 48-49.
283 INTERPARES, **INTERPARES 2: Experiential, Interactive and Dynamic Records**, **a.g.e**, s. 35-37.

beklenir[284]. Buradaki süreçlerin kayıt altına alınması, delil değerinin korunmasına yardımcı olacaktır.

Göç işlemlerinin doğru yürütülebilmesi için mutlaka dokümantasyon hazırlanmalıdır. Burada e-belgelerin oluşturulduğu uygulama yazılımı ve formatı, teknolojik göç üstverisi gibi bilgiler yer almalıdır. Bunların yanı sıra, göç ettirme sonrasında doğrulama yapılarak belgelerin bileşenleri ve ekleri, arşivsel bağ ve erişim seviyeleri gibi unsurların korunup korunmadığı dokümantasyonda belirtilmelidir[285]. Teknolojik göç işlemleri sırasında bu unsurlarda bir değişiklik meydana gelirse karşılaşılan bu durum dokümantasyona kaydedilmelidir[286]. Böylece, teknolojik göç ettirme işlemleri sırasında belgenin delil değerini zayıflatacak ya da ortadan kaldıracak bir değişikliğin yaşanmadığını gösterecek bir karine sunulabilir[287]. Bu karineyi ortaya koyması nedeniyle teknolojik göç dokümantasyonu, arşivlenen e-belgelerin delil değeri kritik unsuru olarak kullanılabilir.

Ancak, burada belgelerin delil değeri unsurlarından olan okunabilirliğin olumsuz etkilenmesi gibi bir risk söz konusudur[288]. Bu riski azaltmak için çeşitli önlemlerin alınması gerekmektedir. Mesela bugün Birlikte Çalışabilirlik Esasları Rehberi'nde tavsiye edilen bir yapı olan PDF/A formatındaki belgelerin ilerleyen yıllarda başka bir formata dönüştürülmesi söz konusu olabilir. Bununla birlikte, bugünkü teknolojiyle kullanılan bir depolama ünitesinin yerini daha ucuz ve etkin bir teknoloji alabilir. Bundan dolayı depolama ünitesinin yenilenmesi söz konusu olabilir. Bu yenileme sırasında delil değerinin korunması için belgenin şekil özelliklerinin yeni formata aktarılması ve belge ile üstveriler arasındaki ilişkinin korunması gerekir. Tüm bunlar yapılırken depolama ünitesinin değişim öncesi ve sonrasındaki döngüsel artıklık denetimi ve özet değerlerinin karşılaştırılması gibi yöntemlerden yararlanılmaktadır. Bu işlemlerin ardından aynı dokümantasyonda teknolojik göç işlemlerinin kim tarafından ne zaman gerçekleştirilip onaylandığı belirtilmelidir[289].

---

284 ISO, **13008 Digital Records Conversion and Migration Process**, Cenevre[İsviçre], ISO, 2012, s. 6-7.
285 **a.g.e.**, s. 8-9.
286 **a.g.e.**, s. 9-11.
287 **a.g.e.**, s. 22-24.
288 TSE, **13298 Elektronik Belge Yönetim Sistemi Standardı**, **a.g.e.**, s. 44. ; ISO, **13008 Digital Records Conversion and Migration Process**, **a.g.e.**, s. V., 6-7.
289 ISO, **18492 Long-term Preservation of Electronic Document-based Information**, **a.g.e.**, s. 8-12.

Teknolojinin ilerlemesi ve değişmesi sebebiyle kurumdaki belge işlemlerinin yürütüldüğü mevcut uygulama yazılımı ihtiyaçlara cevap veremeyebilir. Hâl böyle olunca, bir teknolojik göç işlemi olarak uygulama yazılımının da güncellenmesi veya değiştirilmesi gündeme gelecektir. Ancak, güncelleme ya da değiştirilme işlemi layıkıyla yapılmadığında belgelerin özgünlüğünün bozulması, tamlığının muhafaza edilememesi ve arşivsel bağının korunamaması gibi delil değerini tehdit edecek problemler ortaya çıkabilir. Bu problemlerle karşılaşmamak için mevcut yazılımdaki seri, dosya, bölüm, belge, üstveri gibi tüm bileşenlerin yeni sisteme aktarıldığı kontrol edilmeli, belge ile üstveriler, ekler ve ilgileri arasındaki ilişkinin korunup korunmadığı incelenmelidir[290]. Konuyla alakalı bir kontrol listesi geliştirilebilir[291].

1.4.3. E-Belgelerin Güvenli Paylaşımında Kurumsal Politikalar

Tanımlanmış bir işe bağlı süreçlerin nasıl gerçekleştirileceğini, aynı zamanda tutum ve kararları açıklayan politika ve prosedürler, e-belge ve arşiv yönetimi için de hazırlanmaktadır. Bunlar, belgeyi üretme, dosyalama, arşivleme, teknolojik göç ettirme, paylaşımı ve güvenliğin sağlanması gibi süreç adımlarını kapsamaktadır. Burada, söz konusu adımların nasıl yürütülmesi gerektiği ifade edilir. Mesela belgelerin oluşumuna yönelik hususların yer aldığı bir prosedür, arşivlenen belgenin üretilme koşullarının incelenmesine kaynaklık eder. Durum böyle olunca, adı geçen prosedür, belgelerin delil değeri analizinde önemli bir başvuru kaynağıdır.

Belge ve arşiv yönetimi konusunda başarılı olan kurumların genellikle politika gibi bir prosedüre sahip oldukları görülmektedir[292]. Türkiye'de e-belge yönetimiyle ilgili standart olan TS 13298 Standardı'nda konuyla ilgili çeşitli yaklaşımlar yer almaktadır. Burada şu ifadeler dikkat çekmektedir[293]:

"Kurumlara öncelikle ne tür malzemeleri transfer edeceklerini ve hangi hizmet koşullarında belgeleri kullanıma açacaklarını belirten bir politika geliştirmeleri

290 ISO, **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**, **a.g.e.**, s. 10.

291 TNA, **Migrating Information between Records Management Systems**, 2017, (Çevrimiçi) https :// nationalarchives. gov. uk/ documents/ information-management/ edrms.pdf, 8 Aralık 2020.

292 Çiçek, "E-Devlet Stratejisi Bağlamında Elektronik Belge Yönetimi için "Yazılı Politika" Gereksinimi: Türkiye'deki Uygulamalar Üzerine Bir İnceleme", **a.g.e.**

293 TSE, **13298 Elektronik Belge Yönetim Sistemi Standardı**, **a.g.e.**, s. 41-44.

önerilmektedir. Bu politika dokümanı, arşiv kurumlarının mevzuat ile kendilerine verilmiş olan yetkilerine atıfta bulunmalı ve arşiv malzemesi üreten kurumlarla olan ilişkilerini açık bir şekilde ifade etmelidir".

Kurumların amaçlarıyla uyumlu olan bu politikalar, belge ve arşiv yönetimi süreçlerinin sürdürülebilirliği için birtakım normlar içerir. Bunlar, belge üretiminden arşiv işlemlerine kadar tüm fonksiyonlarda standart uygulamalar getirdiğinden belgelerin delil değerine yönelik kontrol mekanizması olarak kullanılabilir[294]. Bu mekanizmalar, belgeyi oluşturma, dosyasına kaldırma ve iletme, uzun dönemli muhafaza ve bütünlüğü korunmuş hâlde arşive transfer adımlarını belirtebilir. Aynı zamanda, kullanılacak belge formatları ve üstveriler, log kayıtlarının içeriği ve yedeklemelerin biçimleri gibi hususlar da açıklanır[295]. Tüm bunların yanı sıra, süreçlerdeki yetki ve sorumlulukları, güvenlik önlemleri, saklama ortamı, e-belge ve dosyaların formatları ile versiyon kontrollerine ilişkin hususları, hizmet alımına ilişkin ilkeleri, kullanılacak standartları, saklama ve imha sürelerini, teknolojik göç yöntemlerini içermesi de beklenir[296]. Söz konusu hususlar, belge yönetimi ve arşiv politikası şeklinde tek bir prosedürde yer alabileceği gibi yedekleme, belgelerin bütünlüğünün korunması ve teknolojik göç işlemleri gibi her bir alt sürece yönelik müstakil prosedürler de hazırlanabilir.

Bu prosedürler, süreçlerde yapılan işlemleri açıklayan ayrıntılı dokümantasyonlara kaynaklık etmelidir. Örneğin prosedürlerdeki normlar belge formatlarının tür ve niteliklerini açıklarken, bu niteliklerin nasıl uygulandığı dokümantasyonlarda yer alır. Böylece, dokümantasyonlar analiz edilerek prosedürlere

---

294 ISO, **30301 Management Systems for Records: Requirements**, **a.g.e.**, s. V, 2-4. ; Bu mekanizmalarla kurum çalışanlarına süreçlerin başarılı bir şekilde gerçekleştirilmesi için gerekli olan yetkinlikler kazandırılarak delil değerinin korunamaması riskini azaltmak hedeflenir. Bundan dolayı, kurum çalışanlarının belge ve arşiv yönetimi politikalarını başarılı bir şekilde içselleştirmesi gerekir (ISO, **18829 Assessing ECM/EDRM Implementations: Trustworthiness**, **a.g.e.**, s. V, 2, 8). Süreklilik arz eden bir eğitim programının oluşturulması önerilmektedir (ISO, **30301 Management Systems for Records: Requirements**, **a.g.e.**, s. 4-7).

295 ISO, **14641 Design and Operation of an Information System for the Preservation of Electronic Documents: Specifications**, **a.g.e.**, s. 1, 5, 7.

296 ISO, **15801 Electronically Stored Information: Recommendations for Trusworthiness and Reliability**, **a.g.e.**, s. VII-5.

ne oranda uyulduğu incelenir ve belgelerin delil değerinin başarıyla korunup korunmadığına dair bir karine sunulur[297].

Dokümantasyonların yanı sıra belge ve arşiv yönetimine ilişkin fonksiyonların işletilmesi konusunda dış kaynaklı hizmet alımı gerektiğinde bunu sağlama koşulları da prosedürlerde belirtilmelidir. E-belgelerin muhafazasında gerekli koşulların oluşturulması için hizmet alımı yapılarak üçüncü taraf hizmet sağlayıcılarla çalışıldığı bilinmektedir[298]. Arşivlenen e-belgelerin depolanması için bulut bilişim gibi hizmetleri sunan üçüncü taraf hizmet sağlayıcıların, çalışmalarını yürütürken takip etmesi gereken prosedürler önceden belirlenmelidir. Bu prosedürlerde, sistem ve belge bütünlüğünün korunması, belgelere ve üstverilere yetkisiz erişimlerin engellenmesi, gerekli durumlarda belgelerin şifrelenmesi, saklama süresi bitenlerin imha edilmesi ve güvenlik önlemlerinin alınması gibi hususlar yer alır[299]. Üçüncü taraf hizmet sağlayıcılar, bu prosedürlere uyarak gerekli koşulları oluşturduklarını, böylece belgelerin delil değerinin korunduğunu gösteren dokümantasyonları hazırlamalıdır. Mesela, depolama sürecinde belge bütünlüğünün hiçbir şekilde bozulmadığını gösteren özgünlük değerlendirme raporu oluşturulabilir. Bu raporda belgelerin erişimi, dağıtımı, transferi ve muhafazası, teknolojik göç işlemleri, doğrulama süreci ile imha gibi hususların belirtilmesi beklenir[300].

Özgünlük değerlendirme raporu, belge güvenliği kadar bilgi güvenliğine ilişkin hususların da dikkate alınmasını gerektirir. Çünkü standartlarda belge ve arşiv yönetimiyle ilgili süreçler işletilirken iç ve dış tehditlere karşı önlemler içeren bir bilgi güvenliği politikasının benimsenmesi önerilmektedir. Bu politika, malzemenin türüne göre gereksinimler, sorumluluklar, ilgili mevzuat ve standartların gerektirdiği ilkeler ile ihlaller karşısında yapılacakları içermelidir[301]. Bu özelliklere sahip olması nedeniyle ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı öne çıkmaktadır. Bunun nedeni, adı geçen standartta belgelerin bütünlüğü ve erişilebilirliği gibi delil

297 ISO, **15801 Electronically Stored Information: Recommendations for Trusworthiness and Reliability**, **a.g.e.**, s. 25-26. ; ISO, **14641 Design and Operation of an Information System for the Preservation of Electronic Documents: Specifications**, **a.g.e.**, s. 9.

298 ISO, **17068 Trusted Thirt Party Repository for Digital Records**, **a.g.e.**, s. 3, 6, 7.

299 **a.g.e.**, s. 10-12.

300 **a.g.e.**, s. 20-22, 26.

301 ISO, **15801 Electronically Stored Information: Recommendations for Trusworthiness and Reliability**, **a.g.e.**, s. VII-7

değeri unsurlarının risk yönetimi ilkeleri benimsenerek korunabilmesidir. Böylece, risklerin doğru yönetilerek belgelerin delil değerinin korunduğuna dair bir karine sunulabilir[302]. Risklerin doğru yönetilmesi için belgelere erişimde kullanılacak yöntemler, üstveri şemaları, e-imza ve zaman damgası gibi politika ve prosedürlerle belirlenen süreçlerde bilgi güvenliğinin korunduğunu gösteren dokümantasyon oluşturulmalıdır[303].

Delil değerinin korunmasına yönelik olarak, belgelerin paylaşımıyla ilgili hususlar içeren ISO 14721 Açık Arşivsel Bilgi Sistemi Standardı'na (Open Archival Information Systems [OAIS]) da başvurulduğu görülmektedir[304]. Bu standartta, elektronik ortamda oluşan her türlü bilginin uzun dönemli korunması ve paylaşımı üzerine çeşitli modeller geliştirilmiştir[305]. Elektronik dergi, elektronik kitap, fotoğraf hatta arkeolojik bir buluntunun görsel sunumu için kullanılmak üzere geliştirilen OAIS, arşivlenen kurumsal belgeler için de kullanılabilir. OAIS'de belge yönetimi ve arşivciliğin provenans ve orijinal düzen gibi temel uygulama prensiplerinin değerlendirildiği görülmektedir. Örneğin belgelerin neden üretildiği ve diğer belgelerle olan ilişkisi kontekst bilgisi[306], belgenin kaynağı, üretildiğinden bu yana geçirdiği değişimler ve kime ait olduğu gibi bilgiler ise provenans bilgisi olarak ifade edilmektedir. OAIS'de geçen bu açıklamalara göre, belgeyi üretenler, belgenin üretilip sisteme kaydedildiği andan itibaren provenans bilgisini oluşturmalı ve korumalıdır[307]. O hâlde, belgelerin delil değerinin analizinde önemli bir referans olan provenans

302 ISO, **27001 Information Security Management Systems: Requirements**, Cenevre[İsviçre], ISO, 2013, s. 2-14.

303 **a.g.e.**, s. 14-18. ; ISO, **10789 Information and Documentation Management**, **a.g.e.**, s. 13-14.

304 Açık Arşivsel Bilgi Sistemi Standardı'nın alanyazınında "Açık Arşiv Bilgi Sistemi Standardı" olarak da kullanıldığı görülmektedir (Bahattin Yalçınkaya, "E-Arşiv Uygulamalarına Teknolojik ve Altyapı Kapsamında Yaklaşımlar: Güvenilir E-Arşivleme Koşulları Yol Haritası", ed.: Fahrettin Özdemirci vd., **e-BEYAS 2015 Sempozyumu: Kurumsal Belleklerin Geleceği, Dijitalleştirme-Elektronik Arşiv-Elektronik Belge Yönetimi**, 21-22 Ekim Ankara, Ankara, Ankara Üniversitesi, 2012. ; Tolga Çakmak, "Türkiye'de Kültürel Bellek Kurumlarında Dijitalleştirme ve Dijital Koruma Politikaları: Bir Model Önerisi", Yayınlanmamış Doktora Tezi, Ankara, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı, 2016. ; Mehmet Oytun Cibaroğlu, "Elektronik Belge Yönetim Sistemi'nde Belgelerin Uzun Süreli Korunmasına Dair Bir Yaklaşım Değerlendirmesi: Açık Arşiv Bilgi Sistemi Referans Modeli (OAIS)", ed.: Fahrettin Özdemirci ve Zeynep Akdoğan, **Bilgi Sistemleri ve Bilişim Yönetimi: Beklentiler ve Yeni Yaklaşımlar**, Ankara, Ankara Üniversitesi, 2017). Arşivsel bilgi sistemi ifadesiyle arşivsel değerin daha iyi yansıtıldığı düşünülmektedir. Standartta vurgulanan hususun arşiv malzemesinin erişime sunulmasına ilişkin yaklaşımlar getirmek olduğu düşünülmektedir.

305 ISO, **14721 Open Archival Information System (OAIS)**, Cenevre[İsviçre], ISO, 2012, s. 1.

306 **a.g.e.**, s. 20.

307 **a.g.e.**, s. 25.

bilgisi, her dönem korunmalıdır. OAIS'de yer alan ve belgenin delil değerini kritik etmek için kullanılabileceği düşünülen diğer unsurlar ise sunuma ilişkin format, belge bileşenlerini gösteren yapı ile semantik bilgileridir. Sunum bilgisi, belgenin anlaşılabilmesi için gerekli olan JPEG ve PDF gibi format ve bu formatı kullanıcıya yansıtabilmek için gerekli olan yazılım bilgilerini içerir. Yapı bilgisi, belge bileşenlerinin nasıl bir araya getirildiğini açıklar. Semantik bilgisinde ise belgenin anlamlı olabilmesi için ihtiyaç duyulan kontekste, üstverilere ve arşivsel bağa ilişkin hususlar belirtilebilir[308].

OAIS'de belgelerin paylaşımı için üç farklı türde paket oluşturulur. Bunlardan ilki, belgenin üreticisinin oluşturduğu gönderim paketidir (submission information package [SIP]). Sonraki aşamada gönderim paketi, arşiv paketine (archival information package [AIP]) dönüştürülür. Yeni tanımlama bilgileri ve veri modellerinin uygulanması neticesinde paket, arşiv malzemelerinin bulunduğu alana gönderilir. Burada son kullanıcının istek ve ihtiyaçları doğrultusunda erişim için dağıtım paketleri (dissemination information package [DIP]) hazırlanır[309]. Arşiv paketi, belgenin delil değerine esas teşkil edecek bilgileri içerir. Bu pakette, içerik ve uzun dönemli korumaya ilişkin bilgiler mevcuttur. Diğer paketlerde bu bilgiler yer almayabilir[310]. Bu paketin, arşivlenmiş belge ve dosyadan[311] müteşekkil olduğu görülmektedir. Bu şekilde, kendilerine ait tanımlama bilgilerine sahip olan dosyalar, barındırdıkları belgelerin de tanımlama bilgilerini ihtiva eder. Böylece, dosyada uzun dönemli korumaya ilişkin tanımlama bilgileri bulunur[312]. Bunun yanı sıra, paketlerin muhtevası ve mahiyeti gereği göreceği muamelelerin aynı olmayacağı belirtilmektedir. Mesela, gönderim paketlerinin içeriğinin yetkililer tarafından değiştirilme ihtimali varken arşiv paketlerinin değiştirilmesi söz konusu değildir. Ancak, arşiv paketinde bir değişiklik yapılacaksa değişimden önceki özellikleri kayıt

308 **a.g.e.**, s. 25-26.

309 **a.g.e.** Bu paketler (AIP, SIP, DIP) sırasıyla arşiv bilgi paketi, gönderim bilgi paketi ve dağıtım bilgi paketi olarak da adlandırılabilir.

310 OAIS'de önce gönderim paketi sonra arşiv paketi oluşturulmaktadır. Gönderim paketinden arşiv paketi oluşturulduğu durumlarda, bazı üstveriler belgenin ilk üretildiğinden beri belgede yer almayabilir. Bu durumda belgenin kontekstini açığa çıkarmak için eksiklikler yaşanabilir. Bunun için her gönderim paketinin arşiv paketi gibi oluşturulması önerilmektedir (**a.g.e.**, s. 34, 35, 45).

311 OAIS'de dosyanın, arşivsel belge koleksiyonu olarak izah edildiği düşünülmektedir (**a.g.e.**, s. 85-86).

312 **a.g.e.**, s. 85-86.

altına alınır[313]. Bu durum, gönderim paketleriyle arşiv paketlerini depolama ünitelerinde aynı ortamda tutmak, format değişikliği, e-imza ve zaman damgası algoritmalarının güncellenmesi gibi teknolojik göç işlemlerini ayırmayı zorlaştırabilir. O hâlde, arşiv paketleri, diğer paketlerden ayrı bir yerde saklanmalıdır. Bununla birlikte, teknolojik göç neticesinde güncellenen arşiv paketinin bozulmadığını gösteren kayıtlar kontrol edilmelidir. Çünkü bu işlem sırasında paket, teknolojik nedenlerle aslına sadık kalınarak yeniden üretilebilir. Bu aşamada, içerik ve koruma bilgisinin değişmemesine dikkat edilir. Bilgi kaybının olmaması ve malzemenin arşivdeki saklanma sürecinde veya veri transferi sırasında bozulmamasına yönelik önlemler alınır[314].

Belgelerin delil değeri kritik unsurlarıyla ilgili olan e-belgelerin paylaşımı ve güvenliği, teknolojik koşullar ile e-belgelerin oluşumuna kaynaklık eden hususların yer aldığı bu standartların yanı sıra belgelerin delil değerine yönelik standartlar da bulunmaktadır. Burada, British Standard (BS - İngiliz Standardı) 10008, ISO 27037, 27042, 27043 ve 30121 gibi standartlar öne çıkmaktadır. Bu standartlar doğrudan arşivcilik ve belge yönetimiyle ilgili olmadığından müstakil bir alt bölümde ele alınmıştır.

1.4.4. Farklı Standartlarda E-Belgelerin Delil Değeri

Literatür taraması sırasında doğrudan belgelerle ilgili olmasa da elektronik ortamda oluşan bilgilerin delil değerini değerlendirme ve elektronik delil elde etme yöntemlerine ilişkin hususları içeren standartlar olduğu görülmüştür. Bu standartlarda risk yönetimine dikkat edilmesi, delil değeriyle ilgili stratejiler geliştirilmesi, bunlara yönelik dokümantasyonların oluşturulması, delillerle ilişkili olduğu düşünülen cihazların incelenmesi, aidiyet zincirinin kurulması, delillerin bütünlüğünün muhafazası ve saklama koşullarının nasıl olması gerektiği gibi konularda çeşitli kriterler yer almaktadır[315]. Her ne kadar, bu standartlarda elektronik ortamdaki bilginin delil değerine yönelik kriterler yer alsa da bilgi kadar kıymetli olan diğer bir odak

313 **a.g.e.**, s. 96-97.

314 **a.g.e.**, s. 52-53.

315 ISO, **British Standart Institute [BSI] 10008: Evidential Weight and Legal Admissibility of Electronic Information**, Londra[Birleşik Krallık], BSI, 2020, s. 2-7. ; ISO, **27043 Incident Investigation Principles and Process**, Cenevre[İsviçre], ISO, 2015. ; ISO, **30121 Governance of Digital Forensic Risk Framework**, Cenevre[İsviçre], ISO, 2015. s. V. ; ISO, **27050-1 Electronic Discovery Part 1: Overview and Concepts**, Cenevre[İsviçre], ISO, 2019, s. 9.

nokta ise onun taşındığı ortamdır. Başka bir deyişle, bilginin varlığına yokluğuna, transferine orijinalliğine bütünlüğüne bulunduğu kayıt ortamına bakarak karar verilebilir. O hâlde, bilginin delil değeriyle alakalı kritik unsurları belgeler için de kullanılabilmelidir.

Standartlarda ilk olarak, belgelerin delil değerini olumsuz etkileyecek risklerin değerlendirilip sonuçlarının tanımlanması önerilmektedir. Risklere ilişkin tanımlanan bu sonuçların nasıl çözümlenebileceğiyle alakalı olarak belge yönetimi fonksiyonları için politikalar belirlenmesi gerekmektedir[316]. Çünkü politikalarda, üretim, transfer, saklama ve imha gibi fonksiyonlarda belgelerin delil değerini tehdit edecek riskler tanımlanarak alınacak önlemler belirtilir[317].

Standartlarda riskler kadar delil değeriyle ilişkili bir husus da süreçlere ilişkin dokümantasyonun hazırlanmasıdır. Bu dokümantasyonda belgelerin üretiminden arşive devrine, sistem bakımlarından teknolojik göç ettirmeye kadar olan süreçlerin nasıl gerçekleştirildiği açıklanır[318]. Böylece süreçler gerçekleştirilirken politikalara uyulup uyulmadığı, ortaya çıkan dokümantasyonlar incelenerek anlaşılabilir. Fakat, bundan önce politikalar ışığında yapılan işlemlerin kayıt altına alınması gerektiği bilinmelidir. Bu kayıtların ardından dokümantasyon açığa çıkar. İşte, belgelerin delil değerini korumakla görevli olduğu düşünülen arşivciler ve belge yöneticileri politikaları, buna uygun kayıt işlemlerini ve ortaya çıkan dokümantasyonu çok iyi değerlendirmelidir[319].

Oluşan dokümantasyonun bulunduğu elektronik cihazlar da incelenmelidir[320]. Çünkü elektronik ortamdaki bir delil incelenirken, delil dosyası tek başına analiz edilmez. Onun ilişkili olabileceği diğer deliller de araştırılmalıdır. Hâliyle bu durum delilin bulunduğu akıllı telefon, sabit disk ve sunucu gibi cihazların da tetkik edilmesini gerektirir.

Bu süreçte dokümantasyon ve cihazlar kadar dikkat çeken bir durum da belgenin paydaşı olduğu diğer malzemelerdir. Belgelerin delil mahiyeti bazı durumlarda tek bir belge gözden geçirilerek anlaşılamayabilir; belgenin ilişkili olduğu

316 ISO, **BSI 10008: Evidential Weight and Legal Admissibility of Electronic Information**, **a.g.e.**, s. 12.
317 **a.g.e.**, s. 7-9.
318 **a.g.e.**, s. 13-17, 21-25.
319 ISO, **27037 Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence**, Cenevre[İsviçre], ISO, 2012, s. 6-8.
320 **a.e.**

diğer belgeleri de incelemek gerekir. Bunun için organik bağ tetkik edilmelidir[321]. Bu bağ dosyaların oluşumuna kaynaklık ettiğinden e-belgelerin delil değeri, dosya incelenerek de değerlendirilmelidir.

İncelenen standartlarda bu hususların yanı sıra, delillerin bütünlüğüne yönelik açıklamalar da yer almaktadır. Mesela, elektronik ortamdan delil elde edilirken delilin ana kaynağının korunması amacıyla replika düzenlenir. Delil kopyası olarak da bilinen bu replika, delillerin analizinde kullanılır. Delilin ana kaynağı ve replikanın bütünlüğünden bahsedebilmek için bunların zaman içerisinde değişmediği gösterilmelidir[322]. Burada ana kaynak ve replikadan farklı tarihlerde alınan özet değerlerinin birbiriyle eşleşmesi yöntemi benimsenmektedir. Öncelikle, ana kaynaktan elde edilen ilk özet değeriyle bu kaynağa dayanarak oluşturulan replikanın özet değeri karşılaştırılır. Bu değerler arasında eşleşme sağlanıyorsa bütünlüğün korunduğu ileri sürülebilir. Ancak, oluşturulan replikanın taşıyıcı ortamın kırılganlığı ve gerekli teknolojik koşulların uygulanmaması gibi nedenlerle zaman içerisinde bozulabilme ihtimali söz konusudur. Bundan dolayı, replikadan farklı tarihlerde alınan özet değerlerin karşılaştırılmasında eşleşmeme durumu söz konusu olursa delil değeriyle alakalı şüphe oluşabilir. Mevcut değerlendirmeler belgelerin delil değerinin analizi için de düşünülebilir.

Delillerin aidiyet zinciri de sahihlik için kullanılabilecek bir araçtır. Bu zincirin kopmaması, olduğu gibi korunması gerekir. Aidiyet zincirinde öncelikle belge yönetimi fonksiyonlarının düzenli işletilip işletilmediği değerlendirilir. Bunun için belge üretiminden tasfiyesine kadar olan tüm fonksiyonların aidiyet zinciri kaydı oluşturulur. Bu kayıtta tek biçim delil tanımlayıcı, delile kimin ne zaman ve nerede eriştiği, hangi işlemleri gerçekleştirdiği gibi bilgiler bulunur[323]. Mesela, belgelere verilen tek biçim referans numarası, belgeye erişim geçmişinin log kayıtlarında tutulması gibi işlemler bu tür bilgilerdendir.

Bu standartlarda delillerin bütünlüğünün korunması ve yedeklenmesi ile felaket kurtarma planlarının oluşturulması gibi süreçlerin açıklandığı arşivleme

321 Çiçek, **Kurumsal Bilgi ve Belge Yönetimi**, **a.g.e.**, s. 155.

322 ISO, **27037 Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence**, **a.g.e.**, s. 9.

323 **a.g.e.**, s. 10-11. ; ISO, **27042 Guidelines for the Analysis and Interpretation of Digital Evidence**, Cenevre[İsviçre], ISO, 2016, s. 5-8.

stratejisi önerilmektedir[324]. Önerilerden biri de bu stratejide belgelerin özniteliklerinin muhafaza edilmesine yönelik önlemlerin alınmasıdır. Bu amaçla üstveriler ve üstveri şemalarından yararlanılabileceği belirtilmektedir[325].

Belgelerin saklama koşullarının delil değerinin korunmasında önemli bir etken olduğu belirtilmektedir. Mesela, ISO 27050 Elektronik Keşif Standardı'nda (Electronic Discovery) elektronik ortamda saklanan bilgilerin etkin ve etkin olmayan şeklinde sınıflandırıldığı görülmektedir. Etkin olanlara güncel belgeler, etkin olmayanlara ise arşivlenmiş malzemeler örnek verilmektedir. Bu iki kategorideki belgelerin birbirinden farklı yerlerde saklanması önerilmektedir[326]. O hâlde, güncel kullanımda olanlarla arşivlenenler birbirinden ayrı yerlerde muhafaza edilmelidir. Böylece, arşivlenmiş belgeler için yapılacak format değişikliği ve e-imza ile zaman damgası algoritmalarının güncellenmesi gibi muamelelerin güncel belgelerin delil değerini etkilemesinin önüne geçilebilir.

Ancak, adı geçen Standart'ta kurumların belgelerin kontekstini açığa çıkarmak yerine daha çok saklama sürelerine odaklandıkları ve bunlarla ilgili sorumluluklarda asgari şartları sağlamak eğiliminde oldukları dile getirilmektedir. Bunun neticesinde, kurumların belgelerin delil değeri konusunda yeteri kadar kapsamlı bir anlayışa sahip olmadıkları ileri sürülmektedir. Sağlıklı olmayan belge yönetimi uygulamalarının sebep olduğu sonuçların doğuracağı maliyeti henüz tam kavramadıkları ifade edilmektedir. Çünkü belgeler, süresi dolduğunda imha edilmek yerine saklama süreleri uzatılmakta ya da imhaları geciktirilmektedir. Bunun neticesinde belgeler üzerinde entelektüel kontrolün sağlanamadığı; aksine, bir yığın oluşturulduğu düşünülmektedir. Bu yığınlar arasında konteksti açığa çıkarmanın güç olduğu dile getirilmektedir[327]. Bu olumsuz durum, belgelerin delil değerinin anlaşılamamasına neden olabilir.

---

324 ISO, **30121 Governance of Digital Forensic Risk Framework**, **a.g.e.**, s. V, 3.
325 ISO, **27050-1 Electronic Discovery Part 1: Overview and Concepts**, **a.g.e.**, s. 18-19.
326 **a.g.e.**, s. 13.
327 **a.g.e.**, s. 12.

İKİNCİ BÖLÜM
E-BELGELERİN GÜVENİLİRLİK UNSURLARI VE TEHDİTLER

2.1. Güven ve Güvenilirlik

2.1.1. Belgede Güven

İnsanlar, günlük yaşamda ticaretten sigortacılığa, haberleşmeden ulaşıma kadar çeşitli sektörlerde faaliyet gösterirken birbirleriyle ilişki içerisindedir. Bu ilişkide tarafların birbirlerine zarar vermeyecek faaliyetler sergilemeyeceğine inanılması "güven" olarak ifade edilmektedir[1]. Güvenin, tarafların faaliyet gösterdikleri sahada belirlenen değerler sistemine uygun davrandıklarının paylaşılmasıyla oluştuğu ileri sürülmektedir[2]. Bu değerler sistemi, örneğin bir tüccarın faaliyetlerini eksiksiz kaydetmesi, bir sigortanın devreye girme koşullarının belli olması ile bir işin vaat edilen zaman içerisinde gerçekleşmesi gibi hususları içerir.

Ancak, bu faaliyetler sürdürülürken taraflardan birinin güveni suistimal etme ihtimali her zaman bulunabilir. Bundan dolayı, mevcut hukuk düzeni içerisinde önlemler geliştirilmesi tabii bir durumdur. Hâliyle, güveni korumak amacıyla çeşitli kurallar benimsenmiştir[3]. Bu kurallar, tarafların ilgili sahada belirlenen değerler sistemine uygun hareket ettiğinin nasıl kanıtlanacağını belirler. Mesela, bir tüccarın faaliyetlerinin eksiksiz bir biçimde ticari defterlere nasıl kaydedileceği, bir araba sigortasının devreye girme koşullarının nasıl beyan edileceği gibi hususlar bu kurallarda açıklanır. Böylece sözler, sorumluluklar, yükümlülükler yazılı olarak açıkça beyan edilerek taraflar arasında güvenin tesis edilmesi hedeflenir. Taraflar arasında güvenin yazılı olarak tesisi belge ile sağlanır.

Yürütülecek idari işlemin belirlenen kurallara uygun yapılıp yapılmadığı, ilgili sahada gerçekleştirilen faaliyetlerin birer delili olan belgeler incelenerek anlaşılır. Çünkü belgeler içerikleri ve sahip oldukları form özellikleriyle faaliyetlerin nasıl gerçekleştiği gösteren izler taşır. Örneğin, ticari defterler incelenerek defterlerin

---

1 Hatun Boztepe, "Halkla İlişkiler Perspektifinden Güven Kavramı: Katılımcılık, Şeffaflık ve Hesap Verebilirlik İlkelerinin Kamu Kurumlarına Yönelik Güveninin Oluşmasındaki Rolü", **İstanbul Üniversitesi İletişim Fakültesi Dergisi**, No: 45, 2013, s. 55.

2 INTERPARES, **Terminology Web Sayfası**, **a.g.e.**

3 Francis Fukuyama, **Güven: Sosyal Erdemler ve Refahın Yaratılması**, çev.: Ahmet Buğdaycı, 3. bs., İstanbul, İş Bankası Yayınları, 2005, s. 41.

düzenlenmesini belirleyen kurallara uygun davranılıp davranılmadığı analiz edilebilir; haberleşme ve ulaşım kayıtları incelenerek faaliyetlerin zamanında yapılıp yapılmadığı kontrol edilebilir. Belgede sorumluyu gösteren antet, düzenleyeni işaret eden imza başlıca güven ve güvenilirlik tesis eden özelliklerden birkaçıdır. O hâlde, günlük yaşamda işlemler gerçekleştirilirken kullanıldığı sahaya göre gerekli form özelliklerine sahip belgeler, güveni tesis eden başlıca araçlardır.

Her ne kadar kullanıldığı sahada geçerli olan hukuk normlarının belirlediği kurallara göre belgeler, form özellikleri, kullanılan üstveriler ve format gibi farklı hususiyetler taşıyabilse de özgünlük, gerçeklik ve tamlık nitelikleri her tür belge için temel güvenilirlik unsurlarıdır. Hâliyle, bu nitelikleri haiz olan belge güvenilir olarak kabul edilmektedir[4]. O hâlde, güvenilirlik bir hususun kendisinden beklenen niteliklere sahip olması şeklinde ifade edilebilir. Bir belge üzerinde bu niteliklerin varlığı gizlenmeden üçüncü kişilerle paylaşıldıkça belgeye olan güvenin daha da arttığı söylenmektedir[5]. Bunlar korunduğu sürece belgeye olan güvende devamlılık sağlanmış olur[6]. Ancak e-imza doğrulamasının yapılamaması gibi şüpheli bir durum ortaya çıkarsa belgeye duyulan güven de zedelenir.

2.1.2. Güvenilirlik

2.1.2.1. Hukukun Güvenilirliği

Hukuk, finans ve mühendislik gibi farklı alanlarda yapılan çalışmalar incelendiğinde bir hususun güvenilirliğinin kendisinden beklenen niteliklerin sağlanması şeklinde ifade edilebileceği görülmektedir. Mesela bir uçağın güvenilirliği, onun belirlenen koşullar altında arıza yapmadan çalışmasıyla ilişkilidir[7]. Ülkelerde

---

4 Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**

5 Fukuyuama, **a.g.e.**, s. 26, 41, 169.

6 Luciana Duranti, "Preservation in the Cloud: Towards an International Framework for a Balance of Trust and Trustworthiness", **APA/C-DAC International Conference on Digital Preservation and Development Trusted Digital Repositories**, Yeni Delhi[Hindistan], 5-6 Şubat 2014, ed.: Dinesh Katre ve David Giaretta, yayım yeri yok, yayımcı yok, 2014, s. 33-34. ; G. Shabbir Chema, "Building Trust in Government: An Introduction", **Building Trust in Government: Innovations in Governance Reform in Asia**, ed.: G. Shabbir Chema ve Vesselin Popovski, New York[ABD], United Nations University Press, 2010, s. 4-6.

7 Şenol Kasap, "F-16 Uçaklarında Uçuş Güvenliğinin Güvenilirlik Mühendisliği ile Araştırılması", Yayınlanmamış Doktora Tezi, Eskişehir, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü İşletme Sayısal Yöntemler Anabilim Dalı, 2020, s. 5.

merkez bankalarının güvenilir olduğu düşünüldüğünde dış tesirlerin etkisinde kalmaksızın bu bankaların önceden belirlenen kurallara riayet ederek kendisinden beklenen güveni sağlamaya ilişkin nitelikleri taşıdıkları değerlendirilmektedir[8]. Hukukun güvenilirliği ise adaletin tesisi için hukuk kuralları (kanun, yönetmelik, tebliğ, genelge ve tebligat gibi düzenleyici işlemler) ve mahkeme kararlarının kendisinden beklenen belirlilik, istikrar ve öngörülebilirlik gibi niteliklere sahip olması şeklinde ifade edilmektedir[9].

Belirlilik, hukuk kuralları ve mahkeme kararlarının açık ve anlaşılabilir olmasını ifade eder. Anlaşılabilir olmak için anlam bütünlüğü içermesi gereken bu kural ve kararlar, dil bilgisi kurallarına uyumlu bir şekilde yazılmalı ve ifadeler birbiriyle çelişmemelidir[10]. Yazılı metinde anlaşılır bilgi bulunmalı, ne söylendiği, ne karar alındığı veya ne talep edildiği net ve belirli olmalıdır. Mesela, kurumlarda oluşan belgeler söz konusu olduğunda onların form özellikleri ve kullanılacak üstverilerin önceden bir hukuk kuralı olarak tanımlanmış, açık ve tüm kullanıcılar tarafından bilinir olması gerekir. Bu durumda arşivlenen e-belgelerin gerek güncel dönemde üretilirken gerekse yarı güncel dönemde yönetilirken ve aynı zamanda arşive devredildikten sonra güvenli bir şekilde muhafazasının ve sürdürülebilirliğinin sağlanmasında uygulanması gereken kurallar önceden açıkça ortaya konmalı ve herkes tarafından anlaşılabilmelidir.

İstikrar, hukuk kuralları ve kararlarına dayanılarak kazanılan hakların her zaman ve her ortamda korunacağı güvencesinin verilmesi olarak açıklanmaktadır. Bundan dolayı, hukuk normlarının sık sık ve keyfi olarak değiştirilmemesi, kazanılmış hakların korunması gerekir. Burada kazanılan hakların belirli bir süre için aynı

---

8 Mustafa Salim Erek, "Merkez Bankası Bağımsızlığı ve Mali Güvenilirlik İlişkisi: Gelişmekte Olan Ülkeler Örneği", Yayınlanmamış Doktora Tezi, İstanbul, Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü Bankacılık Anabilim Dalı, 2019, s. 45.

9 "Anayasa Mahkemesi Kararı", Karar No: 2011/3, Esas No: 2008/96, tar. 06.01.2011, **R.G.**, S 27934, tar. 14.05.2011, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2011/ 05/20110514-6.htm, 19 Mayıs 2020. ; Arşivsel güvenilirlik analizinde kullanılan hukuki güvenilirlik yaklaşımı, arşivlenen belgelerin delil değerinin incelenmesine yönelikken; burada ifade edilen hukukun güvenilirliği, hukukla ilgili kural ve kararların taraflara güven duygusu vermesiyle alakalıdır.

10 İsmail Köküsarı, "Anayasa Hukukunda Hukuki Güvenlik İlkesi", Yayınlanmamış Doktora Tezi, Ankara, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, 2020, s. 53, 56-60. ; Elif Yılmaz, "Hukuki Güvenlik İlkesinin Bir Gereği Olarak Vergi Hukukunda Geriye Yürümezlik İlkesi", Yayınlanmamış Doktora Tezi, Ankara, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, 2014, s. 14.

kalacağı ve geleceğin öngörülebilirliğine dair bir güvenin tesis edilmesi hedeflenir[11]. Hâliyle, arşivlenen e-belgelerin de ilk üretildiği gibi özniteliklerinin korunarak muhafaza edilmesi hukukun güvenilirliği ilkelerinden istikrar konusuyla ilişkilidir. Öznitelikleri zedelenen belgeler, istikrarı koruyamadığından hukukun güvenilirlik koşullarını da sağlayamamış olur.

Öngörülebilirlik ise hangi eylemlerin nasıl bir hukuki sonuç meydana getireceğinin bilinmesi olarak ifade edilmektedir[12]. E-belgelerin yönetimi ve arşiv işlemleriyle alakalı süreçleri açıklayan prosedürlerdeki normların uygulanması ya da uygulanmaması durumunda nasıl bir hukuki sonuç doğacağının önceden bilinmesi öngörülebilirlik olarak değerlendirilebilir. Dolayısıyla belge işlemleriyle alakalı hukuki düzenlemeler, hangi işlemin ne tür sonuçlar doğuracağını belirgin bir şekilde açıklamalıdır. Böylece, belgenin yaşam döngüsüne ilişkin safhalarla ilgili hükümler, açık ve bu uygulamalarla alakalı doğacak hukuki sonuçlar da öngörülebilir olmalıdır.

Hukukun güvenilirliğinin belirlilik, istikrar ve öngörülebilirlik nitelikleri, hukuki düzenlemelere ilişkin ilkeler içermektedir. Ancak, sadece bu hususlara yönelik ilkeler belirlenmesi ticaret, sigorta ve haberleşme ile ulaşım gibi farklı alanlarda faaliyet gösteren kurumlara güven duyulması için yeterli değildir. Çünkü bu kurumların faaliyetlerini belirlenen değerler sistemine göre gerçekleştirmesi gerekir. Bu değerler, kurumlar özelinde hesap verebilirlik, şeffaflık ve katılımcılık olarak değerlendirilmektedir. Bundan dolayı söz konusu niteliklere sahip olmak, kurumların güvenilirliği bakımından öne çıkmaktadır.

2.1.2.2. Kurumların Güvenilirliği

Kanunlara uygun olarak kurulan örgütler, TMK'ya göre tüzel kişi olarak adlandırılmaktadır. Tüzel kişi, prosedürlere göre meydana gelmiş gerekli organlara sahip olan toplulukları ifade etmektedir[13]. Örgütlü bir yapının teşekkül edip, tüzel kişi statüsü elde etmesi neticesinde tabii olarak güven duygusu gelişmektedir. Kamu güveni[14] olarak da adlandırılan bu kanaat, kurumların varlıklarının toplumsal sözleşme

---

11 **a.g.e.**, s. 23.

12 **a.g.e.**, s. 26.

13 TMK, **a.g.e.**, madde 49.

14 Kamu güveni, hukukun kanıtlama gücü tanıdığı unsurlara toplumun beslediği güven duygusu olarak tanımlanmaktadır (Cemal Elitaş, Oğuzhan Aydemir ve Bilge Leyli Elitaş, "Muhasebe

neticesinde geliştirilen kuralların yine bu sözleşme sonucunda tesis edilen kurullar tarafından onaylanmasından kaynaklanmaktadır. Her ne kadar kaynaklarda kamu güveni, özel ya da kamu ayrımı yapılmaksızın her türlü örgütlü yapı için ifade edilse de yaygın olan şekli daha çok kamu kurumlarına yöneliktir[15].

Toplumsal sözleşme olarak ifade edilen anayasa, devletin varlığını, birliğini ifade edip, sosyal düzen kurallarını açıkladığı gibi gerçek kişi hakları yanında örgütlü yapı olarak kurumların faaliyetlerini düzenleyen hukuk kaidelerine kaynaklık eder. Kanun, tüzük, yönetmelik ve genelge gibi düzenlemeler olan bu hukuk kaideleri, idari işlemlerin nasıl olması gerektiğini açıklarken üretilecek belgeleri de belirler. Yine, bu kaidelerden yetki alan organlar belirlenen bu belgeleri düzenler. Hâliyle, belgenin sorumlusu kamu idaresi, düzenleyeni kamu yetkilisi olduğundan belgelere güven duyulması doğal bir refleks olarak gelişir. Bundan dolayı, kamu kurumlarında üretilen belgelerin güvenilir olduğu kabul edilir. Bu belgelerin güvenilirliklerinin sorgulanmasına pek ihtiyaç duyulmaz.

Ancak, zaman içerisinde yaşanan kişisel veri içeren bilgi sızıntıları, kurumun fonksiyonlarını layıkıyla yerine getirdiğini belgeleyememesi ve yolsuzluk gibi olumsuz durumlar, kurumlara duyulan güveni zedelediğinden üretilen belgelerin güvenilirliği de sorgulanır hâle gelmiştir. Ekonomik Kalkınma ve İşbirliği Örgütü (Organisation for Economic Co-operation and Development - OECD) tarafından yapılan çalışmalarda 1980'li yıllardan itibaren tüm dünyada kamuya duyulan güvenin gittikçe azaldığı ileri sürülmektedir[16]. Bu kanaat, çeşitli kaynaklarda yaygın bir şekilde paylaşılmaktadır[17]. Durum böyle olunca, kurumların güvenilir olduğunu göstermek

---

Açısından Kamu Güveni: Türk Ceza Kanunu'nun İncelenmesi", **Mali Çözüm Dergisi**, No: 93, 2009, s. 38). Belgede sahtecilik üzerine çalışmalarıyla bilinen hukukçu Ahmet Gökcen ise kamu güvenini hukuk düzeninin ispat yeteneği tanıdığı, doğruluk ve gerçekliğine herkes tarafından güvenilmesini emrettiği araçların sahtekârlıktan korunmalarını hedefleyen genel ve toplumsal bir hak ve menfaat olarak tanımlamaktadır (Ahmet Gökcen, **Belgede Sahtecilik Suçları (m. 204-212)**, 5. bs., Ankara, Adalet Yayınevi, 2018, s. 135).

15 Ayşe Atılgan Yaşa ve Kamil Tüğen, "İlişkisel Sözleşmeler Bağlamında Vatandaş Güveni ve Devlet Bütçesi", **Yönetim ve Ekonomi**, C. 26, No: 3, 2019, s. 746. ; Lokman Çilingir, "Locke'un Toplum Sözleşmesi Kuramı", **Temâşâ Felsefe Dergisi**, No: 11, 2019, s. 35.

16 Organisation for Economic Co-operation and Development [OECD], **Government at a Glance**, Paris[Fransa], OECD, 2013, s. 9, (Çevrimiçi) https://doi.org/10.1787/gov_glance-2013-en, 20 Mayıs 2020.

17 Birol Akgün, "Türkiye'de Siyasal Güven: Nedenleri ve Sonuçları", **Ankara Üniversitesi SBF Dergisi**, C. 56, No: 4, 2001, s. 18. ; Erhan Örselli ve Esra Banu Sipahi, "Türkiye'de Vatandaşların Kamu Kurumlarına Güveni", **Uluslararası Sosyal Araştırmalar Dergisi**, C. 9, No: 45, 2016, s. 849. ; Pew Research Center, **Public Trust in Government: 1958-2021**,

gibi bir sorumluluğunun ortaya çıktığı yapılan çalışmalarda açıklanmıştır[18]. Çalışmalarda bu durum, "kurumların faaliyetlerini gerçekleştirirken hedeflerine ulaşabilmeleri ve varlıklarını sürdürebilmeleri için güven kazanmaları gerekir" şeklinde ifade edilmektedir[19]. Bundan dolayı, Türkiye'de de Kamu Malî Yönetimi ve Kontrol Kanunu ile Bilgi Edinme Hakkı Kanunu gibi prosedürler çıkarılmış, kurumların hesap verebilirlik, şeffaflık ve katılımcılık ilkelerine göre hareket etmesi gerekliliği doğmuştur.[20]

Şeffaflık, kurumlara ilişkin bilgilerin ulaşılabilir, basit, açık, anlaşılır, doğru ve eksiksiz olmasını ifade eder. Hesap verebilirlik, kurumların kendisinden başka bir otoriteye de açıklama yapmasını, sorumlulukların nasıl yerine getirildiğinin paylaşılmasını işaret eder. Katılımcılık ise kurumların karar alma ve politika oluşturma süreçlerinde diğer paydaşlar, meslek kuruluşları ve vatandaşların da söz hakkına sahip olması anlamına gelmektedir[21]. Hâl böyle olunca, kurumların güvenilirliği (kurumsal güvenilirlik), hesap verebilirlik, katılımcılık ve şeffaflık ilkeleriyle son derece ilişkilidir.

Elektronik ortamda oluşan bilginin güvenilirliği üzerine çalışmalar yürüten Kelton ve arkadaşlarına göre, söz konusu ilkelerin benimsenip benimsenmediği -kurumların güvenilir olup olmadığı- gerçekleştirilen faaliyetlerin birer delili olan belgeler incelenerek kontrol edilebilir[22]. Kurumların faaliyetlerini nasıl yürüttüklerine ilişkin yayınlayacakları prosedürler, hem denetim mekanizmasının işletilebilmesi hem de üretilecek belgelerin mevzuata uygun hazırlandığının gösterilebilmesi bakımından hesap verebilirlik ve şeffaflık ilkeleriyle son derece ilişkilidir. Bundan dolayı, kurumsal güvenilirlik analizinde belge yönetimi politika ve prosedürleri hazırlanmış mı, gerekli teknolojik koşullar sağlanmış mı ve belgeler mevzuata ve standartlara

(Çevrimiçi) https:// www. pewresearch. org/ politics/ 2021/ 05/ 17/ public-trust-in-government-1958-2021/, 20 Mayıs 2020. ; OECD, **Trust in Government Web Sayfası**, (Çevrimiçi) https:// www.oecd.org/gov/trust-in-government.htm, 20 Mayıs 2020.

18 Türk Sanayicileri ve İşadamları Derneği [TÜSİAD], **Kamu Hizmetinde Etik: Güncel Konular ve Uygulamalar**, İstanbul, Lebib Yalkım Yayınları, 2003, s. 17, 24.

19 Boztepe, **a.g.e.**, s. 54.

20 "Kamu Malî Yönetimi ve Kontrol Kanunu [KMYKK]", Kanun No: 5018, **R.G.**, S 25326, tar. 24.12.2003, (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2003/12/20031224.htm#1, 19 Mayıs 2020. ; "Bilgi Edinme Hakkı Kanunu", **a.g.e.**

21 Boztepe, **a.g.e.**, s. 61-63.

22 Kari Kelton, Kefnneth Fleischmann ve William A. Wallace, "Trust in Digital Information", **Journal of the American Society for Information Science and Technology**, C. 59, No: 3, 2008, s. 367.

uygun bir şekilde üretilip yönetiliyor mu gibi sorular sorulabilmektedir. Bu sorulara verilecek müspet cevaplar, kurumsal güvenilirliğin tesis edilmesine katkı sağlayabilir.

Belge yönetimiyle ilgili politika ve prosedürler hazırlanırken diğer paydaşların da fikrinin alınması imkânı oluşur. Mesela, arşivcilik dernekleri gibi meslek kuruluşlarının görüşüne başvurulabilir. Böylece, katılımcılık söz konusu olacaktır. Bununla birlikte, bu politika ve prosedürlerde belgelerin nasıl üretileceği, saklanıp arşive devredileceği ve imha edileceği açıklanır. Bunun için gerekli teknolojik koşullar tesis edilerek mevzuat ve standartlar ışığında belgelerin sahip olması gereken nitelikler kararlaştırılır. Hâliyle, bu adımlar sorumlulukların nasıl yerine getirildiğini gösterdiğinden hesap verilebilirliği de sağlar.

Kurumsal güvenilirliğin son ilkesi olan şeffaflık, belgelerin erişilebilir olmasını ifade eder. Ancak, burada erişime açılacak belgelerin birtakım özelliklere sahip olması beklenir. Mesela, erişim bir belge yığını içerisinde değil ihtiyaca uygun olan belgeler içerisinde gerçekleşmelidir. Bununla birlikte, erişime açılan belgelerin tam ve doğru olması gerekir[23]. Durum böyle olunca, politika ve prosedürler hazırlanarak ihtiyaç duyulan teknolojik koşullar sağlanır ve belgeler bir yığın içerisinde değil, özgün, gerçek ve tam olarak erişime sunulur.

2.2. E-İmzalı Belgelerin Güvenilirliğini Tesis Eden Araçlar

2.2.1. Elektronik Kimlik Tespiti Araçları

2.2.1.1. Basit (Temel) E-İmza

EİK, ilgili yönetmelikler, e-imza usul ve esasları ile idarenin çıkardığı teknik rehberler ve uygulamalarda çeşitli e-imza türleriyle karşılaşılmaktadır. Bunlar, basit

23 Hale Biricikoğlu, "Yerel Yönetimlerde Hesap Verebilirlik (Marmara Bölgesi Örneği)", Yayınlanmamış Doktora Tezi, Sakarya, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı, 2011, s. 22.

imza[24], zaman damgalı imza, ESHS'ye ait kök sertifikaları[25], sertifika iptal listesi (SİL) ve Çevrimiçi Sertifika Durum Protokolü (ÇiSDuP) (Online Certificate Status Protocol - OCSP)[26] cevaplarını içeren X-Long imza ile arşiv imzadır[27]. Bunlardan X-Long imza ile arşiv imza, yapısı gereği BTK tarafından çıkarılan Elektronik İmza Kullanım Profilleri Rehberi'ne göre uzun dönemli doğrulamaya elverişlidir[28].

Zaman damgası bulunmayan sadece düzenleyenin kimlik tespitini açıklayan imza çeşidi basit e-imza olarak tanımlanmaktadır. Bu imza, e-imza sertifikasının (elektronik sertifika) süresi kadar geçerlidir[29]. Sertifikanın süresi dolduktan sonra imza

---

24 KAMU SM'nin hazırladığı rehber ve yayınlarda ETSI tarafından basic electronic signature (BES) olarak ifade edilen imza türü, basit imza olarak açıklanmaktadır (KAMU SM, **E-İmza Teknolojileri Test Suit**, Web Sayfası, (Çevrimiçi) https :// yazilim. kamusm. gov. tr/ eit-wiki/ doku. php?id, 23 Eylül 2020. ; Işıl Hasırcıoğlu, "Elektronik İmza Oluşturma ve Doğrulama Standartları", **Ulusal Elektronik İmza Sempozyumu**, Ankara, Gazi Üniversitesi, 2006, (Çevrimiçi) http:// www. kamusm. gov. tr/ dosyalar/ makaleler/ Elektronik% 20Imza% 20Olusturma%20ve%20Dogrulama.pdf, 29 Şubat 2020. ; Selçuk, **a.g.e.**). Ancak, AB'nin çıkarmış olduğu çeşitli rehberlerden kişinin e-postasının altına yazdığı adı soyadı, ıslak imzanın sayısallaştırılmış hâli gibi imzaların "simple electronic signature" olarak tanımlandığı görülmektedir (Connecting Europe Facility [CEF], **eSignature Documentation**, (Çevrimiçi) https :// ec. europa. eu/ cefdigital/ wiki/ display/ CEFDIGITAL/ Introduction+to+e-signature, 12 Mayıs 2020). Hâliyle, nitelikli bir elektronik sertifikaya dayanmayan imzaları ifade ettiği için buradaki simple kavramının Türkçe karşılığının basit olabileceği; BES'in ise temel imza olarak değerlendirilebileceği düşünülmektedir. Buna rağmen, KAMU SM'de BES için basit imza açıklaması getirildiğinden bu terimin kullanılması tercih edilmiştir.

25 Kök sertifikalar, ESHS'nin kimlik bilgilerinin yer aldığı dosyadır (KAMU SM, **Temel Kavramlar**, (Çevrimiçi) https :// kamusm. bilgem. tubitak. gov. tr/ dokumanlar/ belgeler/ kitaplartemel_kavramlar.jsp, 24 Şubat 2020).

26 İptal durumunu öğrenmek için SİL ve ÇiSDuP incelenir. SİL, ESHS'lerden alınan ve içerisinde iptal edilmiş sertifikaların seri numarasını içeren listedir. "Bir sertifika için iptal kontrolü yapılacağı zaman sertifikanın seri numarası SİL içerisindeki listede aranır. Eğer seri numarası listede bulunuyorsa sertifika iptal edilmiş demektir, listede yoksa sertifika SİL'e göre geçerlidir". ÇiSDuP ise sertifika iptal bilgisinin çevrimiçi olarak sorgulanabildiği bir protokoldür (Gülen Çelebi Başçi, **Sertifika Geçerlilik Kontrolündeki Sorunların Giderilmesi**, (Çevrimiçi) https :// kamusm. bilgem. tubitak. gov. tr/ dosyalar/ makaleler/ Sertifika %20 Gecerlilik %20 Kontrolundeki %20 Sorunlarin % 20 Giderilmesi.pdf, 30 Nisan 2020).

27 KAMU SM, **E-İmza Teknolojileri Test Suit**, **a.g.e.**

28 Bilgi Teknolojileri Kurumu [BTK], **Elektronik İmza Kullanım Profilleri Rehberi**, s. 11, (Çevrimiçi) https://www.btk.gov.tr/uploads/pages/elektronik-imza-kullanim-profilleri-rehberi-5a33ff5b59f93.pdf, 5 Nisan 2020.

29 "Elektronik İmza Kanunu", **a.g.e.;** Selçuk, **a.g.e.** ; ESHS tarafından oluşturulan nitelikli elektronik sertifikanın geçerlilik süresi en fazla 3 yıl, ESHS'ye ait imza oluşturma ve doğrulama verilerinin geçerlilik süresi ise 10 yıl olarak belirlenmiştir. EİK'in ilgili Yönetmeliğinde ESHS'lerin nitelikli elektronik sertifikalar ve zaman damgaları ile ilgili işlemlere ilişkin kayıtları en az 20 yıl süreyle saklaması emredilmiştir. Kurumlar, saklama planlarında bu hususu göz önünde bulundurmalıdır (KAMU SM, **Nitelikli Elektronik Sertifika İlkeleri**, 2020, s. 49, (Çevrimiçi) http:// www. kamusm. gov. tr/ BilgiDeposu/ KSM_ NES_ SI/KSM_NES_SI.pdf, 15 Mart 2020. ; "Elektronik İmza Kanunun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik", **R.G.**, S 25692, tar. 06.01.2005, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/2005/01/20050106-15.htm, 22 Mayıs 2018).

doğrulanamaz[30]. Kullanım ömrü, bir sonraki iptal bilgisinin yayınlanmasından daha kısa olduğundan anlık imza olarak da ifade edilmektedir. Ancak, basit imza yapılacak eklentilerle uzun dönemli doğrulanabilir imza türlerine dönüşebilmektedir[31].

Basit imza oluşturulurken her bir imzacının sertifikasındaki özet algoritması kullanılarak imzalanacak içerik üzerinden mesaj özeti elde edilir. Bu özet imzacının özel anahtarı ile imzalanır ve imzalı bir veri elde edilir. Bu imzalar, sertifikanın geçerlilik süresi içerisinde cari olduğundan çevrimiçi işlemlerde veya imzanın geçerliliğinin kısa süreli ispat edilmesine ihtiyaç duyulan sistemlerde kullanılmalıdır[32].

2.2.1.2. Zaman Damgalı İmza

E-imza çeşidi olarak en yaygın kullanılan tür, zaman damgalı e-imzadır. Zaman damgası, bir elektronik verinin üretildiği veya gönderilip alındığı zamanın tespit edilmesi amacıyla ESHS tarafından e-imza ile doğrulanan kayıttır. Bundan dolayı, EBYS'lerde e-imzanın atıldığı zamanı öğrenmenin yanı sıra, belgenin de düzenlenme tarihini gösterebilmesi bakımından zaman damgasından yararlanılmaktadır[33].

Zaman damgasından dolayı basit imzadan farklı olarak sertifika kullanım süresi dolsa dahi belgenin doğrulama imkânı bulunmaktadır. KAMU SM'nin hazırladığı E-İmza Teknolojileri Test Suit adlı rehberde e-imzanın geçerliliği ve doğrulanması şu ifadeyle adeta zaman damgasına bağlanmıştır:

"Zaman damgası ile imzanın oluşturulma zamanı güvence altına alınır. İmza oluşturulma zamanı güvence altına alındığı için imza oluşturulduğu anda sertifika ve imza geçerliyse sertifika iptal olduktan ya da süresi dolduktan sonra da imza geçerlidir."[34]

E-imzalı belgelerin zaman damgası kontrol edilirken, bu damganın geçerli olup olmadığı cevabını verecek sertifikanın da doğrulanması gerekir. Zaman damgası

---

30 KAMU SM, **E-İmza Teknolojileri Test Suit**, **a.g.e.** ; Basit imzanın bu özelliğinden kaynaklanıyor olacak ki RYY Kılavuzu'nda bu imza türünün kullanılmaması gerektiği ifade edilmektedir (Türkiye Cumhuriyeti Cumhurbaşkanlığı İdari İşler Başkanlığı Destek ve Mali Hizmetler Genel Müdürlüğü Bilgi ve Belge Yönetimi Daire Başkanlığı, **Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik Kılavuzu (RYY Kılavuzu)**, 2020, s. 50, (Çevrimiçi) https://www.tccb.gov.tr/assets/dosya/resmiyazisma/dosyalar/kilavuz.pdf, 20 Mayıs 2021).

31 BTK, **Elektronik İmza Kullanım Profilleri Rehberi**, **a.g.e.**, s. 8.

32 Hasırcıoğlu, **a.g.e.** ; Selçuk, **a.g.e.**

33 KAMU SM, **E-İmza Teknolojileri Test Suit**, **a.g.e.**

34 KAMU SM, **E-İmza Teknolojileri Test Suit**, **a.g.e.**

doğrulama işlemleri olarak adlandırılan bu süreçte, öncelikle sunucudan gelen cevabın imzası kontrol edilir. Sunucuya gönderilen zaman damgalı belgenin özet değeri ile gelen cevap içerisindeki özet değer karşılaştırılır. Sonrasında bu damganın sertifikasının doğrulaması yapılır[35].

Zaman damgasına ilişkin uygulama esasları KAMU SM tarafından yayınlanmıştır. Uzun dönemli korunacak e-imzalı belgeler için kullanılan zaman damgaları, burada belirtilen tek biçim tanımlayıcılara ve en az 20 yıl saklanmak gibi özelliklere sahip olmalıdır[36]. Ancak, bir e-imzanın uzun dönemli doğrulanabilmesi için bu damganın da yeterli olmadığı düşünülmektedir. Çünkü doğrulama için damgayla birlikte imzanın atıldığı tarihteki SİL ve ÇiSDuP verilerinin imzada bulunması gerekir. Bu veriler, e-imzaların uzun dönemli doğrulamasında daha kullanışlı olan Extended Long Electronic Signature with Timestamp (X-Long imza) ve arşiv imzada yer almaktadır[37].

2.2.1.3. X-Long İmza ve Arşiv İmza

X-Long imza, zaman damgalı imzanın üzerine kurulu olan fakat bundan fazla olarak içerisinde ESHS'ye ait kök sertifikaları, SİL ve ÇiSDuP cevaplarını içeren imza türüdür. İmza doğrulanırken bu veriler kullanıldığından uzun dönemli doğrulamaya imkân tanır. KAMU SM'nin hazırladığı E-İmza Teknolojileri Test Suit'te belirtildiğine göre doğrulama yapılırken herhangi bir yerden doğrulama verilerinin edinilmesine gerek yoktur; ihtiyaç duyulan doğrulama verileri imza dosyasında mevcuttur[38].

Kurumlarda kullanılacak X-Long imzanın sahip olması gereken özellikler, 2012 yılında BTK tarafından Elektronik İmza Kullanım Profilleri Rehberi'nde yayınlanmıştır. Buna göre, e-imzaların oluşma ve doğrulama verilerine ilişkin ilkeler, imzanın içerisinde yer almalıdır[39]. X-Long imza, söz konusu özellikleri barındırdığından uzun dönem doğrulanabilmektedir. Ancak, sertifikaların kullandığı algoritmaların kırılabilmesi ihtimali nedeniyle arşivlenen e-belgelerdeki e-imzaların

---

35 **a.g.e.**

36 KAMU SM, **Zaman Damgası Uygulama Esasları**, (Çevrimiçi) https :// kamusm. bilgem. tubitak.gov.tr/BilgiDeposu/KSM_ZDUE/YON.01.02_02_KAMU_SM_ZAMAN_DAMGASI_UYGULAMA_ESASLARI.pdf, 11 Mayıs 2020.

37 BTK, **Elektronik İmza Kullanım Profilleri Rehberi**, **a.g.e.**, s. 11.

38 KAMU SM, **E-İmza Teknolojileri Test Suit**, **a.g.e.**

39 Bu rehberde çeşitli profiller belirlenmiş ve uzun dönemli korumaya elverişli imzaların P4 profiline sahip olması için gerekli özellikler açıklanmıştır (BTK, **Elektronik İmza Kullanım Profilleri Rehberi**, **a.g.e**).

doğrulanmasında X-Long imza yeterli gelmeyebilir. Buna bir çözüm olması amacıyla arşiv imza kullanılmaktadır[40].

X-Long imzadaki verileri içeren, fakat ESHS'ye ait kök sertifikaların ve zaman damgalarının geçerlilik süresinden daha uzun bir süre saklanması gereken belgeler için kullanılan imza türü, arşiv imzadır. Burada sertifikaların geçerlilik süresi bitmeden zaman damgası eklenmektedir. Arşiv imza, resmî yazışmalarla ilgili yönetmelikte şöyle tanımlanmaktadır:

"İmzaya imzadaki tüm eklentileri kapsayacak şekilde ve imzadaki zaman damgalarından daha güçlü bir özetleme algoritması kullanılarak bir zaman damgası eklenmesidir. Eklenen bu damga, arşiv zaman damgası olarak adlandırılmaktadır."[41]

Arşiv imza, belgedeki kriptografik algoritmalar zayıflamadan daha güçlü bir algoritmaya sahip zaman damgasının eklendiği imza türüdür[42]. Zaman damgası, belgeye imza ve damga geçerlilik sürelerinin bitiminden önce eklenmelidir[43]. Buna rağmen, eklenen bu damga da süreç içerisinde güçsüzleşebileceğinden imzaya birden fazla damga bağlanabilir[44].

---

40 KAMU SM, **E-İmza Teknolojileri Test Suit**, **a.g.e.** ; RYY Kılavuzu'na göre belgelerin Cryptographic Message Syntax (CMS - Kriptografik Mesaj Sözdizimi) Electronic Signature [CADES] X-Long imza türü ile imzalanıp, sonrasında arşiv imzaya dönüştürülmesi gerekmektedir (Türkiye Cumhuriyeti Cumhurbaşkanlığı İdari İşler Başkanlığı Destek ve Mali Hizmetler Genel Müdürlüğü Bilgi ve Belge Yönetimi Daire Başkanlığı, **RYY Kılavuzu**, **a.g.e.**, s. 50).

41 **a.g.e.** ; 2020 yılında güncellenen RYY'ye göre kamu kurum ve kuruluşlarında kullanılacak güvenli e-imzaların arşiv imzaya dönüştürülebilir olması gerekir. EBYS'ler, belgede yer alan imzanın dayanağı olan ve teknik standartta belirtilen arşivleme metodunu destekleyerek imzanın ilgili standarda göre "arşiv imzası" tipine dönüştürülebilmesini ve uzun dönemli doğrulanabilmesini sağlamalıdır (**a.g.e.** ; BTK, **Elektronik İmza Kullanım Profilleri Rehberi**, **a.g.e.**).

42 Tamer Ergun ve Vural Çelik, "E-Arşiv ve Uzun Süreli Doğrulama", **e-Beyas 2015 Sempozyumu Kurumsal Belleklerin Geleceği: Dijitalleştirme-Elektronik Arşiv-Elektronik Belge Yönetimi**, 21-22 Ekim 2015, ed.: Fahrettin Özdemirci vd., Ankara, Ankara Üniversitesi, 2016.

43 KAMU SM, **E-İmza Teknolojileri Test Suit**, **a.g.e.**

44 Selçuk, **a.g.e.** ; European Telecommunications Standard Institute [ETSI], **TS 119 312: Electronic Signatures and Infrastructures: Cryptographic Suites**, 2017, s. 16, (Çevrimiçi), https:// www. etsi. org/ deliver/ etsi_ ts/ 119300_ 119399/ 119312/ 01.02.01_60/ ts_119312v010201s.pdf, 29 Şubat 2020.

Ancak, e-imzalarda kullanılan kriptografik algoritmaların zayıflaması[45], güvenlik açıkları[46], uygulama yazılımlarının eksikliği[47] gibi belgenin bütünlüğünün ve gerçekliğinin korunamamasına neden olabilecek problemlerden dolayı belgelerin delil değeri riske girebilmektedir. Konuyla ilgili yapılan çalışmalarda arşiv imzaya zaman damgası eklemenin uzun süre saklanacak e-imzalı belgeler için oldukça hacimli veri boyutu oluşturabileceği ileri sürülmektedir. Aynı zamanda, belgenin formatı değiştirildiğinde sürecin nasıl yönetileceğiyle ilgili belirsizlikler de giderilmiş değildir[48]. Bunların yanı sıra, KAMU SM ve BTK gibi otoriteler ilerleyen zamanlarda e-imza algoritmalarının güncellenmesi, zaman damgası sunucularının bakımı gibi görevlerini layıkıyla sürdüremezse belgelerin geçerliliği riske girebilir[49]. Durum böyle olunca, sadece zaman damgası güncellemesiyle e-imzalı belgelerin delil değerinin yeteri kadar korunamayacağı, ek tedbirler almak gerekeceği öngörülmektedir.

---

45 E-imzaların ilk zamanlarında SHA1 algoritması kullanılmaktayken, günümüzde SHA2 ve SHA3'ün 256, 384 ve 512 bitlik algoritmalarından yararlanılmaktadır ("Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliğ", **R.G.**, S 25692, tar. 06.01.2005, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2005/ 01/ 20050106-19.htm, 5 Nisan 2020. ; "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik", **a.g.e.** ; Cevat Manap ve A. Murat Apohan, "Özet Fonksiyonlarındaki Zayıflıklar ve Elektronik İmzalara Etkisi", **Ulusal Elektronik İmza Sempozyumu**, Ankara, Gazi Üniversitesi, 2006, (Çevrimiçi) http :// www. kamusm. gov. tr/ dosyalar/ makaleler/ Ozet % 20Fonksiyonlarindaki % 20 Zayifliklar %20 Ve % 20Elektronik %20Imzalara%20Etkisi.pdf, 29 Şubat 2020. ; **Shattered Web Sitesi**, (Çevrimiçi) https://shattered.io/, 29 Şubat 2020. ; Gianluca Lax, Francesco Buccafurri ve Gianluca Caminiti, "Digital Document Signing: Vulnerabilities and Solutions", **Information Security Journal: A Global Perspective**, No: 24, 2015. ; Greg Casemento ve Patrick Hatfield, "The Essential Elements of An Effective Electronic Signature Process", **Digital Evidence and Electronic Signature Law Review**, No: 6, 2009. ; Chet Hosmer, "Providing the Integrity of Digital Evidence with Time", **International Journal of Digital Evidence**, C. 1, No: 1, 2002. ; Mason, **a.g.e.**, s. 368).

46 Güvenlik açıkları şöyle belirtilebilir: Belgedeki e-imza bilgilerinin değiştirilmesi, e-imzalı belgeye imzalandıktan sonra içeriği değiştirebilecek bir kod eklenmesi, kriptoanaliz ile imzanın geçerliliğini etkilemeden yeni bir belge üretilmesi, özet değeri hatası oluşturulması, e-imzanın oluşturma ve doğrulama verilerinin ele geçirilmesi, sertifika bilgilerinin bozulması, zaman damgasında tahrifat yapılması (Ardieta v.d., **a.g.e.**, s. 69, 74-78).

47 KAMU SM, **Elektronik Belgeleri Açık Anahtar Altyapısı Kullanarak Güvenli İşleme Rehberi**, Sürüm 1.4, 2015, (Çevrimiçi) http:// kamusm. bilgem. tubitak. gov. tr/ dosyalar/ rehberler/REHB-001.001_1.4.pdf, 23 Eylül 2020.

48 Bralic, Kules ve Stancic, **a.g.e.**, s. 101. ; Martin A. Gagliotti Vigil v.d., "Assessing Trust in the Long-term Protection of Documents", **2013 The Institute of Electrical and Electronics Engineers [IEEE] Symposium on Computers and Communications**, 7-10 Temmuz 2013, Split[Hırvatistan], IEEE, tarih yok, s. 185-188.

49 Bralic, Kules ve Stancic, **a.g.e.**, s. 91-92.

2.2.1.4. İmza Doğrulama Süreci

E-imzalarda, her kullanıcının bir açık bir de özel (gizli) anahtarı bulunur. Açık anahtarla doğrulama, özel anahtarla imza atma yani belgeyi düzenleme işi yapılır. Kişinin e-imza oluşturmak için kendine ait şifresi demek olan özel anahtar, sadece imza sahibinin kullanabildiği şifreleme algoritmasıdır. Atılan bir e-imzanın doğrulanabilmesi için özel anahtarın eşleniği olan açık anahtar gerektiğinde doğrulama yapabilmek için herkesle paylaşılabilir.

İmzalama yapılırken, öncelikle e-belgelerin boyutu küçültülür ve özeti elde edilir[50]. Bu özet, düzenleyenin özel anahtarıyla şifrelenir. İmzayı doğrulamak isteyen taraflar, açık anahtarı doğrulayarak imzayı kontrol edebilir. Bundan dolayı, e-imza doğrulama verilerinin imzalama yapan sertifikaları, iptal durum bilgisi cevaplarını ve zaman damgası sunucusundan alınan güvenilir zaman damgalarını içermeleri gerekir.

İmza doğrulama sonucunda ortaya çıkabilecek üç farklı durum söz konusudur. İlki e-imzanın geçerli olduğunu, doğrulama işleminin başarıyla gerçekleştiğini gösterir. İkincisi, sertifikanın imzayı doğrulamaması nedeniyle imzanın geçersiz olmasıdır. Oluşabilecek üçüncü ve son durum ise eksik doğrulamadır. Eksik doğrulama, imzanın geçerli veya geçersiz olduğunu kesin bir şekilde ifade edememekte, ulaşılamayan veya eksik olan verilerden dolayı imzanın doğrulanma işleminin tamamlanamadığını göstermektedir[51].

Bir belgedeki e-imzanın doğruluğunu kontrol etmek için elektronik sertifika ve zaman damgası kullanılmaktadır[52]. EİK'e göre, imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı ifade eden sertifika, teknolojik eskimeye ve şifrelemenin çözülmesine önlem almak amacıyla belirli bir zaman aralığında geçerlidir[53]. Bu süre bittikten sonra aynı sertifikayla imza atılamaz; yeni bir sertifika edinmek gerekir. Aynı şekilde zaman bilgisinin ispatı amacıyla kullanılan zaman damgası sertifikaları da belirli bir süre zarfında caridir. Bu süre bittikten sonra o sertifika ile zaman damgası üretilemez.

---

50 Manap ve Apohan, **a.g.e.**

51 Hasırcıoğlu, **a.g.e.**

52 Tamer Ergun, "Security Analysis of Electronic Signature Applications and Test Suite Study", Yayınlanmamış Doktora Tezi, Ankara, Ortadoğu Teknik Üniversitesi Uygulamalı Matematik Enstitüsü Kriptografi Anabilim Dalı, 2013, s. 4-5. ; KAMU SM, **Temel Kavramlar**, **a.g.e.**

53 "Elektronik İmza Kanunu", **a.g.e.**

E-imzalı bir belgenin uzun ömürlü olabilmesi için doğrulama verisini kendi içerisinde taşıyacak bir şekilde zaman damgasına sahip olması gerekir[54]. Ancak, şifrelemenin çözülmesine önlem almak amacıyla zaman damgası sertifikalarının da belirli bir geçerlilik süresi vardır. Bu nedenle arşiv imza formatı geliştirilmiştir. Uzun dönemli doğrulamanın sıhhati için belgedeki imza, bu formata dönüştürülerek belirli zaman aralıklarıyla güncellenmelidir. Bu dönüştürme işlemi, son kullanılan zaman damgası sertifikasının süresi bitmeden yeni bir sertifika alınarak arşivlenen belgelere zaman damgası eklenmesi yoluyla yapılmaktadır[55]. Aksi takdirde, ilerleyen yıllarda şifresi çözülmüş bir sertifika ile imzalanan belge doğrulanamazsa acaba belge tahrif mi edilmiş şüphesi doğabilecektir. Durum böyle olunca zaman damgası, belgenin geçerliliğinin korunduğuna yönelik bir karine olarak kullanılmaktadır.

Ancak, konuyla ilgili yapılan çalışmalarda zaman damgasının sürekli güncellenmesinin oluşturacağı hacimli veri boyutu ve teknolojik göç sürecine ilişkin belirsizliğin henüz giderilememesi gibi sorunların yanı sıra[56], e-imzalı belgelerin uzun dönemli doğrulanmasında çeşitli sorunlarla karşılaşılabileceği dile getirilmektedir. Bunlar, e-imza doğrulamasında üstveri, kontekst ve arşivsel bağ gibi belgenin form elemanlarının yeteri kadar dikkate alınmaması, özet değerlerinin birbiriyle eşleşememesi ve e-imzalı belgelerin teknolojik göç işlemlerinde yaşanabilecek problemlerdir. Bu sebeple belgelerin delil değerinin korunmasında sadece e-imza incelemesi yapılmasının her zaman başarılı sonuçlar veremeyebileceği dile getirilmektedir[57]. Ancak, e-imzanın belgenin form elemanlarını dikkate almak gibi bir görev tanımı yapılmamıştır. Çünkü, asıl görevi düzenleyeni belirlemek olduğu için elektronik ortamda oluşturulan herhangi bir yazılı kayıttaki irade beyanının kimliğini tespit etmek amacıyla geliştirilmiştir. Buna rağmen, özet değerlerinin birbiriyle eşleşmemesi ve teknolojik göç problemleri e-imzalı belgelerin güvenilirliğini tehdit eden sorunlar olarak değerlendirilebilir.

E-imzalı belgelerde farklı tarihlerde oluşturulan özet değerlerinin birbiriyle eşleşmesi beklenir. Böylece, bütünlüğün muhafaza edildiğine dair bir karine sunularak

54 BTK, **Elektronik İmza Kullanım Profilleri Rehberi**, **a.g.e.**, s. 11.
55 KAMU SM, **E-İmza Teknolojileri Test Suit**, **a.g.e.**
56 Bralic, Kules ve Stancic, **a.g.e.**, s. 101. ; Martin A. Gagliotti Vigil v.d., **a.g.e.**
57 Philip Boudrez, "Digital Signatures and Electronic Records", **Archival Science**, C. 7, No: 2, 2007, s. 182-183.

delil değerinin korunduğu gösterilir. Fakat, aksi bir durum belgenin gerçekten tahrif edildiği anlamına gelmez. Belgedeki bit akışı değişse de belgenin hukuki geçerliliği devam edebilir. Örneğin, kullanılan donanımlar yenilendiğinde belgelerin özet değeri birbiriyle eşleşmeyebilir. Hâliyle belgenin özniteliklerinde herhangi bir değişim yaşanmasa da bütünlüğünden şüphe edilebilecektir[58].

Özet değerleriyle ilgili bu problemlerin yanı sıra, e-imzalı belgelerin teknolojik göçüne yönelik sorunlarla da karşılaşılmaktadır. Bunlar, belgenin format değişikliğinde izlenecek adımlar ve kök sertifikaların uzun dönemli korunmasıyla ilgilidir. Formatla ilgili sorun, belgenin formatı değiştikten sonra e-imzanın doğrulama fonksiyonunun geçerli olamamasından kaynaklanmaktadır. Çünkü, belgenin formatı değiştirildiğinde yeni bir belge ve özet değeri söz konusudur. Bundan dolayı, format değişikliği gibi teknolojik göç işlemleri sonrasında belgelerin yeniden imzalanmasına ihtiyaç duyulmaktadır. Fakat belgenin düzenleyeni artık hayatta olmayabilir veya belgenin üretildiği kurumda o fonksiyonu gerçekleştirmekle ilgili bir görevi bulunmayabilir[59]. O hâlde, yeni formattaki belgenin eski formata göre üretildiği nasıl gösterilecek, doğruluğu nasıl kontrol edilecektir? Burada belgenin kim tarafından yeniden düzenlendiğini gösterecek ve bütünlüğü muhafaza edecek bir araca ihtiyaç duyulmaktadır. Durum böyle olunca, bu amaçla geliştirilen elektronik mühürden (e-mühür)[60] yararlanılabileceği düşünülmektedir. E-mühür, teknolojik göç sonrası oluşan belgelerin doğrulanmasında kullanılabilir.

E-imzalı belgelerin teknolojik göçünde karşılaşılan bir diğer sorun ise kök sertifikaların uzun dönemli korunup korunamayacağı meselesidir. Kök sertifikalar korunamazsa belgedeki imzalar doğrulanamayacaktır. Bundan dolayı kurumlarda e-

---

58 **a.g.e.**, s. 183-184.

59 **a.g.e.**, s. 188.

60 "Elektronik mühür, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve mühür sahibinin bilgilerini doğrulama amacıyla kullanılan elektronik veridir. Elektronik mühür, elektronik belgenin veya verinin mühür sahibi tarafından oluşturulduğunu, belgenin veya verinin kaynağını ve bütünlüğünü garanti eden delil kaydıdır" ("Elektronik İmza Kanunu", **a.g.e.**). Ancak, e-mührün kullanılması henüz zorunlu değildir (Vural Çelik vd., "Elektronik Yazışma Projesi Güvenlik Katmanları ve Uygulama Geliştirme Esnasında Dikkat Edilmesi Gereken Hususlar", **Bilgi Sistemleri ve Bilişim Yönetimi: Beklentiler ve Yeni Yaklaşımlar**, ed.: Fahrettin Özdemirci ve Zeynep Akdoğan, Ankara, Ankara Üniversitesi, 2017, s. 114. ; "2017/21 sayılı Başbakanlık Genelgesi", **R.G.**, S 30210, tar. 14.10.2017, (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2017/10/20171014-11.pdf, 20 Ağustos 2020).

imzalı belgelerin doğrulama işinin başarıyla gerçekleştiğinin kayıt altına alınması önerilmektedir. Bunun için belgedeki imza, hem ilk oluşturulduğu gibi hem de belirli aralıklarla otonom olarak doğrulanmalı ve bu işlemin yapıldığı üstverilere eklenmelidir. Bu süreç, teknolojik göç işlemlerinden sonra da tekrar edilmelidir. Böylece, belirli bir tarihten sonra kök sertifikalara erişim mümkün olmasa da o tarih öncesinde belgedeki imzanın doğrulandığı gösterilebilir[61].

Kök sertifika ve imza doğrulama verilerinin saklanmaması, e-imzaların doğrulanmasıyla ilgili çeşitli sorunlara sebep olmaktadır. Bu sorunların çeşitli ülkelerde yaşandığı bilinmektedir. Bunun en son örneklerinden birinin Hırvatistan'da yaşandığı Hrvoje Stancic'in yayımladığı raporda görülmektedir. Hırvatistan Merkez Bankası ve Vergi İdaresinde yapılan incelemelerde belgelerin e-imzalı olarak saklandığı fakat artık doğrulanamadığı belirtilmektedir[62]. Çünkü belgelerin düzenlendiği tarihteki SİL gibi imza doğrulamasına yönelik veriler merkezi otorite tarafından saklanmamıştır. Bundan dolayı, belgedeki imza sertifikasının iptal edilip edilemediği bilgisine ulaşmak mümkün olamamaktadır. Durum böyle olunca, belgenin delil değerinin korunamaması riski doğacaktır[63].

Söz konusu sorunlara blokzincir teknolojisi ve üstverilerin kayıt altına alınması gibi yöntemlerle çeşitli çözümler getirilmek istenmiştir. Hırvatistan'da geliştirilen TRUSTCHAIN uygulamasında sertifika bilgileri blokzincirlere yüklenmekte; e-imzalı belgelerin geçerlilikleri yüklenen bu sertifikalar üzerinden kontrol edilmektedir[64]. İsveç'te ise imza doğrulama bilgileri bir üstveri olarak kayıt altına alınmıştır[65].

---

61 Boudrez, "Digital Signatures and Electronic Records", **a.g.e.**, s. 186-188.

62 Hrvoje Stancic, **Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records**, 2018, s. 27-29, (Çevrimiçi) https :// interparestrust. org/ assets/ public/ dissemination/ TRUSTER Preservation Model (EU31)-Finalreportv_ 1_ 3. pdf, 12 Nisan 2020.

63 **a.g.e.**

64 Vladamir Bralic, Hrvoje Stancic ve Mats Stengard, "A Blockchain Approach to Digital Archiving: Digital Signature Certification Chain Preservation", **Records Management Journal**, C. 30, No: 3, 2020, s. 354-355.

65 Stancic, **Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records**, **a.g.e.**, s. 27-29.

2.2.1.5. Kurumsal Şifreleme ve Elektronik Mühür

Kurumlar, elektronik ortamdaki belge paylaşımlarında -şifreli EYP gönderiminde- gizlilik sağlamak amacıyla e-imzanın yanı sıra şifrelemeye de ihtiyaç duyabilmektedir. Belgenin kriptografik yöntemler kullanılarak gizliliğinin sağlanmasını mümkün kılan şifreleme, şifre verilerinin erişilememesi durumunda belgelerin okunamayacağı ihtimalinden dolayı delil değeri kritik unsuru olarak değerlendirilmektedir. Şifrelemeye ilişkin hükümler mevzuatta da yer almakta; 2017/21 sayılı Başbakanlık Genelgesi'nde şifrelemeyle ilgili hususlar bulunmaktadır. Buna göre, kurumların elektronik ortamdaki yazışmalarında kullanılacak şifreleme sertifikaları, gerçek kişiler adına üretilemeyecek; belgelerin uzun süreli saklanması veya e-imzalama gibi amaçlarla kullanılmayacaktır[66].

Şifrelemeye ilişkin usul ve esaslar BTK tarafından belirlenmiştir. Buna göre, şifreleme, "bir elektronik verinin, kriptografik yöntemler kullanılarak değiştirilmesi suretiyle gizliliğinin sağlanmasına olanak veren tekniği", şifreleme sertifikası ise "Kamu SM tarafından üretilen ve kamu kurum ve kuruluşları arasında elektronik ortamdaki belge paylaşımında şifreleme yapmak amacıyla kullanılan açık anahtarı içeren elektronik sertifikayı" ifade etmektedir. Şifreleme sertifikalarının geçerliliği bir yıldır[67].

2017/21 sayılı Başbakanlık Genelgesi'nde belirtilen bir diğer güvenilirlik aracı da elektronik mühürdür. Elektronik ortamda yapılan yazışmalarda, yazışma yapan tarafların kimliklerinin tanımlanıp doğrulanabilmesi gerekir. Bu ihtiyacın karşılanması amacıyla kamu kurumları için e-mühür sertifikaları oluşturulmaktadır. Bunlar, gerçek kişiler adına üretilememekte; şifreleme amacıyla kullanılamamaktadır[68].

E-mühre ilişkin usul ve esaslar yine BTK tarafından belirlenmiştir. Burada e-mühür, "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve elektronik mühür sahibinin kimliğini doğrulama amacıyla kullanılan elektronik veri" olarak açıklanmıştır. E-mühür sertifikası ise "KAMU SM tarafından üretilen ve kamu kurum ve kuruluşları arasında elektronik ortamdaki belge paylaşımında yazışma yapan tarafların kurumsal kimliklerini güvenli bir şekilde

66 "2017/21 sayılı Başbakanlık Genelgesi", **a.g.e.**

67 BTK, **Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar**, 2019, (Çevrimiçi) https :// www. btk. gov. tr/ uploads/ boarddecisions/ kurumsal- sifreleme- ve- elektronik- muhur- sertifikalarina- iliskin- usul- ve- esaslar/ 160-2019-web.pdf, 11 Mayıs 2020.

68 "2017/21 sayılı Başbakanlık Genelgesi", **a.g.e.**

tanımlamak ve doğrulamak amacıyla kullanılan elektronik sertifikayı" ifade etmektedir. Mühür sahibi, elektronik mührü oluşturan kamu kurum veya kuruluşudur[69].

Ancak, EİK'te kurumsal şifreleme açıklanmamışken e-mührün tanımlandığı görülmektedir. BTK'nın konuyla ilgili yayınladığı usul ve esaslardan farklı olarak e-mühür, elektronik belgenin veya verinin mühür sahibi tarafından oluşturulduğunu gösterir. Belgenin veya verinin kaynağını ve bütünlüğünü garanti eden delil kaydıdır şeklinde açıklanmaktadır[70]. Bundan dolayı, yazışma yapan tarafların kimliklerini tanımlamak ve doğrulamak amacıyla çıkarılsa da daha geniş bir işlevinin olabileceği düşünülmektedir. Mesela, teknolojik göç sonrası yeni formattaki bir belgenin özniteliklerinin korunduğunu teyit etmek için e-mühür kullanılabilir.

2.2.2. Belge Doğrulama Kodu

E-imzalı belgelerin güvenilirliğinin incelenmesinde kullanılabilecek bir diğer araç belge doğrulama kodudur. Bu kod aracılığıyla belge görüntülenebilmektedir. 2020 yılında güncellenen RYY ile kamu kurumlarının ürettiği belgeleri, belgedeki doğrulama kodu aracılığıyla e-Devlet Kapısı üzerinden doğrulamak zorunlu hâle getirilmiştir[71].

Ancak, bu güncellemeye rağmen her kurumun henüz bu uygulamayı benimsemediği görülmektedir. E-Devlet üzerinden doğrulama imkânı sunmayan kurumların ürettiği belgeler, kurumların kendi sistemleri üzerinden yine belgede yer alan doğrulama kodu aracılığıyla kontrol edilebilmektedir. Kendi sistemleri üzerinden sorgulama yapılmasına imkân tanıyan bazı kurumlarda doğrulama yapmayı mümkün kılan bağlantı ya da Quick Response [QR] kod (karekod) ekleme gibi uygulamaların tercih edildiği görülmektedir. Hangi uygulama benimsenirse benimsensin belgenin doğrulanması gerekmektedir. Ancak, sahadaki uygulamalarda ciddi sorunlarla karşılaşılmaktadır. Özellikle doğrulama kodu uygulamasının resmî olarak yürürlüğe girdiği tarihten önce kurulup işletilen EBYS'lerde uyum problemi yaşandığı bilinmektedir. Bununla birlikte, teknik ve teknolojik koşullarla aynı zamanda ağ bağlantılarından kaynaklanan sebepler, belge doğrulama süreci için riskler barındırmaktadır.

---

69 BTK, **Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar**, **a.g.e.**

70 "Elektronik İmza Kanunu", **a.g.e.**

71 "Belge doğrulama işlemi, doğrulama kodu ve karekod ile Dijital Türkiye (e-Devlet) üzerinden sağlanır" ("RYY", **a.g.e.**).

Her ne kadar doğrulama koduyla alakalı zaman zaman problemler yaşansa da kurumsal çözüm olarak karşılaşılan barkod uygulaması, belge doğrulamak için yeterlidir. İstanbul Üniversitesindeki örneklerde belgedeki doğrulama bağlantısı açıldığında belgedeki doğrulama barkodu ile giriş yapılarak belge görünmektedir (Şekil 48, 49 ve 50). Belgede bulunan doğrulama barkodu dikkat çeken bir uygulamadır.

Bu farklı uygulamalar, kanun yapıcıların da dikkatini çekmiş olacak ki, 2020 yılında güncellenen RYY'de çözüm için birtakım öneriler getirilmiştir. Bu önerilerden öne çıkan doğrulama kodu yanı sıra karekod uygulamasıdır (Şekil 51). Yönetmelik'e konuyla ilgili olarak şu hüküm eklenmiştir:

"Elektronik ortamda güvenli elektronik imza ile imzalanan belgelerde, "İletişim bilgileri" alanının üst sınırını belirleyen çizginin üzerinde iki satırlık alanın ilk satırında "Bu belge, güvenli elektronik imza ile imzalanmıştır." ibaresi bulunur. Belge doğrulama bilgilerini içeren "belge doğrulama kodu" ikinci satırda, "karekod" ise "İletişim bilgileri" alanının en sağ kısmında yer alır." [72]

Adı geçen Yönetmelik ve bunu açıklayan Cumhurbaşkanlığı Resmî Yazışma Kılavuzu'na göre bu karekod içerisinde belgeyi üreten idare, belge sayısı, belge doğrulama adresi ve belge doğrulama kodu bilgileri yer almalıdır[73]. Aynı zamanda EYP 2.0 ile doğrulama kodu zorunlu üstveriler olarak benimsenmiştir. Buna göre, belgenin doğrulama kodu, EYP'de "belgeId" ve "Core" bileşenlerinde yer alan belgenin tekil numarasıdır. Belgenin doğrulama adresi ise EYP'de "doğrulama bilgisi" üstverisinde bulunmalıdır[74].

2.2.3. Elektronik Yazışma Paketi

Kurumlar, e-belge üretirken birbirinden farklı uygulama yazılımları kullanabilmektedir. Bu yazılımlarda üretilen belgelerin başka yazılımlarda da erişilebilir olması gerekir. Bundan dolayı, kurumlarda oluşan belgelerin standart bir yapıya sahip olması gerektiği fikri gündeme gelmiştir. Birleşik Krallık'ta Oxford

72 "RYY", **a.g.e.**

73 **a.g.e.** ; Türkiye Cumhuriyeti Cumhurbaşkanlığı İdari İşler Başkanlığı Destek ve Mali Hizmetler Genel Müdürlüğü Bilgi ve Belge Yönetimi Daire Başkanlığı, **RYY Kılavuzu**, **a.g.e.**, s. 69.

74 Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO), **e-Yazışma Projesi**, (Çevrimiçi), https://cbddo.gov.tr/projeler/e-yazisma/, 30 Ağustos 2020.

Common File Layout (OCFL - Oxford Müşterek Dosya Düzeni), Amerika Birleşik Devletleri'nde BagIt gibi araçlarla belgelerin üstverileriyle birlikte bir paket olarak kurgulanabildiği görülmektedir[75]. Böylece, belgeler üretildikleri uygulama yazılımlarına bağımlı olmaksızın bu paket yapısıyla iletilebilmekte, hatta arşivlenebilmektedir.

Türkiye'de ise kamu kurum ve kuruluşlarının kendi aralarındaki resmî yazışmaların elektronik ortamda güvenli bir şekilde yapılmasını sağlamak amacıyla başlatılan E-Yazışma Projesi dikkat çekmektedir. Bu proje kapsamında 2012 yılında hazırlanan e-Yazışma Teknik Rehberi ile resmî yazışmalar, bunların üstverileri ve e-imzalarını taşıyacak bir paket yapısı (EYP) belirlenmiştir. EYP, kurumların EBYS'lerine eklenebilir bir yapıdadır[76]. Belirtilen tarihte uygulamaya alınan EYP'nin bütün kamu kurumlarının EBYS'lerinde aynı şekilde benimsenip entegre edilebilmesi için 2017/21 sayılı Başbakanlık Genelgesi ile kullanılması kurala bağlanmıştır. Aynı zamanda, adı geçen Genelge ile tüm kamu kurumlarının EBYS yazılımlarını e-Yazışma Teknik Rehberi'ne uyumlu hâle getirmesi kararlaştırılmıştır[77]. 2020 yılında güncellenen RYY ile dışarıya gönderilmeyip kurum içerisinde kalan belgeler için de EYP oluşturulması zorunlu hâle getirilmiştir[78].

EYP, resmî bir yazışmaya ait üst yazı, ek, üstveri, imza ve mühür gibi bileşenleri tanımlanan kurallar neticesinde tek bir elektronik dosyaya dönüştürür. Paket olarak adlandırılan bu dosya, kendisine ait tanımlayıcı bilgiler içerir. Böylece, teknoloji ve platformdan bağımsız bir paket elde edilmesi hedeflenmiştir. Paketin tasarlanmasında açık bir standart olan Open Packaging Conventions (OPC - Açık Paketleme Kuralları) yapısı kullanılmıştır. EYP ile resmî yazışmalara ait üstyazı ve ekler bir bütün olarak tek seferde e-imza ile imzalanabilmektedir. Böylece, farklı kurumlara gönderilecek paketler için yeniden imza atılmasına ihtiyaç duyulmamaktadır.

Bunun yanı sıra, EYP'de pakete eklenmesi düşünülen yeni bileşenler paketin bütünlüğü bozulmadan eklenebilmektedir. Çünkü paket içerisindeki bileşenler hem ayrı ayrı hem de paketle ve kendi aralarında ilişkilendirilerek saklanmaktadır. Bundan

---

75 **Oxford Common File Layout (OCFL) Web Sitesi**, (Çevrimiçi) https://ocfl.io/, 1 Mayıs 2020. ; **The BagIt File Packaging Format Web Sitesi**, (Çevrimiçi) https://tools.ietf.org/html/draft-kunze-bagit-17, 1 Mayıs 2020.

76 CBDDO, **e-Yazışma Projesi**, **a.g.e.**

77 "e-Yazışma Projesi hakkında Genelge", **a.g.e.**

78 "RYY", **a.g.e.**

dolayı, bileşenlerin ayrıştırılması ve tekrar bir bütün hâline getirilmesi pakete atılan imzaları bozmamaktadır[79].

EYP'nin belgenin kendisi ve ekleri, üstveriler ve imza gibi bileşenleri içermesi onun delil değeri analizinde kullanılabileceğini düşündürmektedir. Ancak, pakette kullanılması zorunlu olan üstveriler[80], nitelikleri açısından delil değerini korumak noktasında yeterli başarıyı sağlayamayabilir. Çünkü, belgelerin hangi faaliyet ve fonksiyon kapsamında üretildiği ile ait olduğu dosya bilgisinin zorunlu bir üstveri olarak benimsenmediği görülmektedir. Halbuki bunlar, belgenin dosyalanmasına kaynaklık ettiğinden delil değeri unsurlarından biri olarak değerlendirilmektedir. O hâlde, EYP'deki zorunlu üstveriler bileşenine işlem, faaliyet, fonksiyon ve birim ile dosya kodu bilgileri eklenebilir. Bununla birlikte, kamu kurumlarının yürüttüğü faaliyetlerin süreçler düzeyinde açıklandığı Hizmet Envanteri Yönetim Sistemi (HEYS) ile kurumlarda oluşan belgeler arasında bir ilişki kurularak belgenin türü ve ait olduğu süreç gibi bilgiler zorunlu üstveriler olarak kurgulanabilir[81].

Bunların yanı sıra, belgenin delil değeri unsurlarından olan erişilebilirliği sağlamak için ihtiyaç duyulan yazılım ve donanım koşulları gibi asgari gereksinimler ile belgenin üretildiği EBYS yazılımı ve sürüm numarası zorunlu üstveriler olarak benimsenebilir. Aynı zamanda, üstverilerde EBYS'nin oluşumuna kaynaklık etmesi nedeniyle yazılımın kaynak kodunun referans numarasının da yer alması önerilebilir. Çünkü, bu konuyla alakalı olarak UNESCO'nun destekleriyle Software Heritage Project'in (Yazılım Mirası Projesi) yürütüldüğü bilinmektedir[82]. Bu üstveriler elle

---

79 CBDDO, **e-Yazışma Teknik Rehberi**, Ankara, Sürüm 2.0., 2020, (Çevrimiçi) https:// cbddo. gov. tr/ SharedFolderServer/ Projeler/ File/ EYP _ 2.0/ EYP 2.0 _ teknik-rehberi.pdf, 30 Ağustos 2020.

80 EYP'de bulunan zorunlu üstveriler şöyle belirtilebilir: Belge referans numarası, belgenin konusu, tarihi ve sayısı, güvenlik derecesi ve tasnif kodu (gizli, çok gizli, kişiye özel gibi), belgedeki imzalar ve oluşturan, üstyazı bileşeninin formatı, dağıtım listesi, üstyazı bileşeninin dosya sistemindeki adı (**a.g.e.**, s. 34). Bu üstverilerin zenginleştirilmesine duyulan ihtiyaç Yalçınkaya'nın doktora tezinde de ifade edilmiştir (Bahattin Yalçınkaya, "E-devlet Üstveri Standardının Oluşturulması ve Türkiye için Modellenmesi", Yayınlanmamış Doktora Tezi, İstanbul, Marmara Üniversitesi Türkiyat Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı, 2014).

81 "HEYS, merkezi ve yerel yönetim kuruluşları tarafından, vatandaşlara, özel sektör kuruluşlarına, sivil toplum kuruluşlarına ve diğer kamu kurumlarına sunulan kamu hizmetleri ile kurumlarda yürütülen diğer tüm faaliyetlerin "süreçler" düzeyinde tespit edildiği ve bu süreçlerin birbirleriyle ilişkilendirilmesinin sağlanarak tüm kamu hizmetlerine yönelik genel süreç haritalarının çıkarıldığı KAYSİS alt sistemidir" (CBDDO, **e-Yazışma Teknik Rehberi**, **a.g.e.**, s. 14. ; CBDDO, **Hizmet Envanteri Yönetim Sistemi Web Sayfası** (Çevrimiçi), https :// envanter.kaysis.gov.tr, 30 Nisan 2020).

82 UNESCO, **Software Heritage Web Sitesi**, **a.g.e.**

eklenmemeli, belge tanzim edilirken otomatik olarak oluşmalıdır. Böylece, e-imzalı belgeler EYP ile birlikte arşivlenebilir.

2.2.4. Kayıtlı Elektronik Posta

KEP, elektronik iletilerin, gönderimi ve teslimatı da dâhil olmak üzere kullanımına ilişkin hukukî delil sağlayan nitelikli elektronik posta olarak tanımlanmaktadır. Bu e-postanın kullanımı için mevzuatta belirtilen şartları taşıyan KEPHS tarafından geliştirilmiş KEP sistemleri kullanılır. Burada yapılan işlemler sonucunda KEPHS işlem sertifikası kullanılarak imzalanıp, zaman damgası aracılığıyla hangi işlemin ne zaman meydana geldiğini gösteren KEP delilleri oluşmaktadır[83].

KEPHS'ler, KEP ile ilgili kayıtların, güvenliğini, gizliliğini ve bütünlüğünü sağlamakla yükümlüdür. Söz konusu kayıtlar, bu özellikleri korunarak en az 20 yıl saklanmalıdır. Bununla birlikte, KEP iletileri ile delilleri anlaşılabilir ve okunabilir olmalı, kullanılan sistem arayüzlerinin de engelli dostu olması gerekmektedir[84].

KEP işlemlerinin nasıl yönetileceğine ilişkin teknik bir tebliğ hazırlanmıştır. Bu tebliğde KEPHS'lerin ETSI Technical Specification (TS - Teknik Özellikler) 102 640 Standardı'na uygun hareket etmesi kararlaştırılmıştır[85]. Bununla birlikte bu tebliğde KEPHS'lerin kullandığı imzaların Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'e uyumlu olması gerektiği belirtilmiştir[86]. BTK'nın hazırladığı usul ve esaslara göre KEP iletisi, paketleri ve işlem loglarının CMS Archival Electronic Signature (CADES-A, CMS Arşiv Elektronik İmza), kep delillerinin ise XADES-A ile imzalanması gerekmektedir. Bunlar, sertifika süreleri bitmeye yakın arşiv imza ile yeniden imzalanmalıdır[87]. Böylece, KEP'in gönderim, kabul, teslim ve okunmasına ilişkin inkâr edilemez deliller oluşur.

---

83 "Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik", **a.g.e.**

84 **a.g.e.**

85 "Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ", **R.G.**, S 28036, tar. 25.08.2011, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2011/ 08/ 20110825-21.htm, 10 Mart 2019.

86 "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliğ", **a.g.e.**

87 BTK, **Kayıtlı Elektronik Posta Hizmet Sağlayıcılarının Birlikte Çalışabilirliğine İlişkin Usul ve Esaslar**, 2014, s. 26, (Çevrimiçi) https:// www. btk. gov. tr/ uploads/ pages/ kephsbirliktecalisabilirlikusulesas-5a3406e891d77.pdf, 10 Mart 2019.

KEP sistemi üzerinden düzenlenen ileti, güvenli e-imza ile imzalanarak gönderici KEPHS'e yönlendirilir. Bu KEPHS, iletinin mevzuatta belirtilen standartlara uygunluğunu kontrol eder. Bir aykırılık tespit edilmemesi durumunda ileti "KEPHS tarafından kabul edildi" delili üretilir. Bu delil, KEP iletisinin ekine konur ve gönderici KEPHS tarafından imzalanarak göndericiye iletilir. Sonrasında göndericinin oluşturduğu ileti, KEP paketinin içine konularak gönderici KEPHS tarafından imzalanır ve alıcıya iletilir. Ancak, oluşturulan ileti, gönderici KEPHS tarafından reddedilirse "KEPHS tarafından reddedildi" delili göndericiye tebliğ edilir[88]. Bu işlem adımlarından sonra KEP iletisinin alım süreci başlamaktadır.

KEP iletisinin alımında alıcı KEPHS, gönderinin mevzuatta belirtilen standartlara uygunluğunu kontrol eder. Bir aykırılık tespit edilmemesi durumunda "alıcı KEPHS tarafından kabul edildi" delili üretilir. Bu delil, KEP iletisinin ekine konur ve alıcı KEPHS tarafından imzalanarak göndericiye iletilir. Ancak, bir aykırılık tespit edilirse "Alıcı KEPHS tarafından kabul edilmedi" delili üretilir ve bu delil KEP iletisinin ekine konulup alıcı KEPHS tarafından imzalanarak geri gönderilir. Bu işlem sonucunda KEP başarılı bir şekilde alıcıya teslim edilirse "teslim edildi delili" oluşturulur. Yine bu delil, KEP iletisinin ekine konur ve alıcı KEPHS tarafından imzalanarak göndericiye tebliğ edilir[89].

İletinin gönderilmesi ve kabul edilmesinden sonra okundu delili oluşturulur. Alıcı KEPHS, KEP'in alıcı tarafından okunup okunmadığını kontrol eder. Bu kontrolü gerçekleştirirken KEP'in teslim edilmesinden sonraki iş gününe kadar alıcı tarafından açılması hâlinde "alıcı tarafından okundu" delili üretilir. Bu delil, KEP iletisinin ekine konularak göndericiye iletilir. Belirtilen süre içerisinde alıcının iletiyi açmaması durumunda ise "alıcı tarafından okundu kabul edildi" delili oluşturulur. Bu delil, KEP iletisinin ekine konularak alıcı KEPHS tarafından imzalanıp göndericiye teslim edilir[90].

Görüldüğü üzere KEP delilleri, iletinin sisteme gönderilmesi, kabul edilmesi ve okunması gibi süreçlerle ilişkilidir. E-belgelerin özniteliklerinin zaman içerisinde korunmasına ihtiyaç duyulduğundan KEP, mevcut yapısıyla belgelerin güvenilirliğinin korunmasında yeterli olmayabilir. Hâl böyle iken, en az 20 yıl

88 **a.g.e.**, s. 4-5.
89 **a.g.e.**, s. 5-7.
90 **a.g.e.**, s. 8-10.

saklanacak KEP delilleri nasıl bu amaçla kullanılabilir sorusu akla gelmektedir. Ancak, KEP'in belgelerin özniteliklerini korumak gibi bir işlevi söz konusu değildir, esas görevi belgenin güvenli bir şekilde iletilmesini sağlamaktır.

Durum böyle olunca, belgeye ait KEP delilinin güvenilirliği tesis edebilecek EYP gibi başka bir araçla ilişkilendirilebileceği düşünülmektedir. Her ne kadar, EYP içeren KEP iletilerinde EYP'nin özet değeri yer alsa da sadece özet değer üzerinden bir inceleme yapmak yeterli olmayabilir. Çünkü, kamu kurumlarında zenginleştirilerek kullanılması önerilen EYP'deki üstveriler aynı zamanda KEP delili olarak değerlendirilebilir. Belge, başka bir kuruma KEP aracılığıyla gönderildiğinde EYP'deki üstveriler KEP delilinin içerisinde yer alabilir. Böylece bu delil, EYP'deki üstverilerin sahihliği için bir teyit mekanizması olarak benimsenebilir ve e-imzalı belgelerin delil değeri analizinde kullanılabilir.

2.2.5. Güvenilirliği Tesis Eden Diğer Araçlar

E-imza ve e-mühür benzeri elektronik kimlik tespiti araçları, belge doğrulama kodu, EYP ve KEP gibi güvenilirlik araçlarının yanı sıra[91], RYY'de yer aldığından güvenilirliği tesis ettiği düşünülen log kayıtları ve olağanüstü belge kayıt defteri gibi araçlar da bulunmaktadır. Her ne kadar bu araçlar, kurumlarda oluşan yazışma türündeki belgeler için benimsenmiş olsa da farklı türdeki belgeler için de geçerli olabilecek mahiyettedir.

Yazılımlarda sistem performansı ve kullanıcı etkinliklerini ayrıntılı olarak sunan log kayıtları oldukça çeşitlidir. Örneğin sistemlerde açılan oturumların başlangıç ve bitişini, eriştiği internet adreslerini gösteren trafik logu, sistem güvenliğini aşmaya yönelik eylemleri belirten tehdit logu ile sistemdeki her bir olay ve hareketi kaydeden sistem logu gibi pek çok log türü vardır. EBYS'lerde ise belgeyi hazırlama süreçleri, paraflama ve imzalama aşamaları, havale ile dosyasına kaldırma işlemlerine ait bilgilerin log kayıtlarında yer aldığı görülmektedir[92].

---

91 RYY'de e-imza, e-mühür, EYP ve KEP gibi araçların kullanımına ilişkin hususlar açıklandığından burada tekrar açıklanmayacaktır.

92 Bahattin Yalçınkaya, Muhammet Emin Gedikli, Mehmet Oytun Cibaroğlu, "Elektronik Belge Yönetim Sisteminde Log Analizi: İstatistiksel Bir Değerlendirme", **Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ**, ed.: Bahattin Yalçınkaya vd., Ankara, Ankara Üniversitesi, 2019, s. 64-65.

Log kayıtlarına ilişkin hususlar, RYY'de de yer bulmaktadır. Buna göre, parafların elektronik onay ile atılabileceği ve bu onayların günlük raporlarda yer alacağı ifade edilmektedir. Bu raporlar, günlük olarak zaman damgasıyla damgalanmalıdır. Oluşturulan günlük raporların saklama süresi ilişkili olduğu belgenin saklama süresinden daha kısa olamamaktadır[93]. Yönetmelik Kılavuzu'nda ise bu raporlar aynı zamanda log olarak adlandırılmaktadır. Log kayıtlarının belgelerin saklama planları çerçevesinde imha edilebileceği belirtilmektedir[94]. Ancak, Yönetmelik'te ya da Kılavuz'da log kayıtlarının içerdiği bilgiler hakkında bir açıklama görülememektedir. Bu durum, kamu kurum ve kuruluşlarının elektronik belge yönetimi uygulamaları gerçekleştirirken bağlı kalmaları gereken[95] TS 13298 Standardı'nda EBYS'lerde oluşturulacak loglarda bulunacak asgari bilgilerin yer almasından kaynaklanabilir[96].

Log kayıtlarının yanı sıra benimsenebilecek bir diğer güvenilirlik aracı ise olağanüstü durumlarda oluşturulan belgeler için hazırlanan "olağanüstü durum belge kayıt defteri"dir. Olağanüstü durum, gerçekleşmesi hâlinde kurumları olumsuz etkileyebilecek veya güvenlik zafiyeti oluşturabilecek durumları ifade etmektedir. Bunlar, uzun süreli elektrik kesintileri ile donanım ve yazılım sorunları gibi teknik ve teknolojik sorunlar nedeniyle EBYS'lerin çalışamamasından kaynaklanabilir. Bu durumlarda, belgelerin fiziksel ortamda hazırlanması gerekir. EBYS'ye erişim sağlandığında ise bu belgeler üstveri bilgileriyle birlikte sisteme kaydedilir[97].

Olağanüstü durumlarda hazırlanan belgeler, -paraflı nüsha onu oluşturan kurumda kalacak şekilde- en az iki nüsha olarak düzenlenmektedir. Bu belgelerin sayı kısmında "O" ifadesi yer alır (O-İdari birim kimlik kodu-Dosya kodu-Evrak kayıt

---

93 "RYY", **a.g.e.**

94 Türkiye Cumhuriyeti Cumhurbaşkanlığı İdari İşler Başkanlığı Destek ve Mali Hizmetler Genel Müdürlüğü Bilgi ve Belge Yönetimi Daire Başkanlığı, **RYY Kılavuzu**, **a.g.e.**, s. 51.

95 "2008/16 sayılı Başbakanlık Genelgesi", **R.G.**, S. 26938, tar. 16.07.2008, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/2008/07/20080716-7.htm, 8 Haziran 2020.

96 Bunlar, sistemde kayıt ekleme, değiştirme ve arama gibi gerçekleştirilen işlemler, işlemin kim tarafından hangi EBYS elemanı üzerinde hangi tarih ve saatte gerçekleştirildiği bilgileridir. Log kayıtları aracılığıyla dokümanların belgeye dönüşme tarih ve saati, EBYS elemanları üzerinde yapılan işlemler ile saklama planı ve süresinde yapılacak değişiklikler takip edilebilmektedir. Bu bilgilerin sistem yöneticisi dâhil kimse tarafından değiştirilemez ve silinemez şekilde korunması gerekir. Log kayıtları, gerekli olduğu durumlarda kurum dışındaki yetkililer tarafından incelenebileceğinden anlaşılabilir bir format ve açıklıkta olmalıdır (TSE, **13298 Elektronik Belge Yönetim Sistemi Standardı**, **a.g.e.**, s. 23-24).

97 "RYY", **a.g.e.**

numarası gibi). Olağanüstü durumlarda belgenin kayıt numarası kurumsal belge kayıt sistemi üzerinden alınır. Bu sistem, "mevzuat sebebiyle EBYS kullanamayan idare tarafından ya da "çok gizli" nitelikteki belgeler ile olağanüstü durumlarda hazırlanan belgelere sayı almak için kullanılan defter ve benzeri fiziksel veya EBYS harici tutulan elektronik kayıt" olarak tanımlanmaktadır[98].

RYY Kılavuzu'nda olağanüstü durumlarda hazırlanan belgeler için "olağanüstü durum belge kayıt defteri"nin hazırlanması gerektiği ifade edilmektedir. Bu defterde, her belge için kurumsal belge kayıt sisteminden alınan belge kayıt numarası, belgenin sayısı, belgenin tarihi[99], ek bilgisi ve gideceği yer yazılmalıdır[100]. Bu bilgiler, belgenin öznitelikleri olarak değerlendirilebilir.

Ancak, olağanüstü durumlarda hazırlanıp sonrasında e-imza ile ya da sadece üstverileriyle EBYS'ye kaydedilen belgelerin teknolojik eskime veya e-imza sertifikalarının doğrulanamaması gibi nedenlerle ilerleyen dönemlerde güvenilirlikleri sorgulanabilir. Durum böyle olunca, bu belgeler, gerçekten olağanüstü durumda mı üretilmiş, öznitelikleri korunmuş mu şüpheleri oluşabilecektir. Bu şüpheleri gidermenin araçlarından biri belgenin özniteliklerinin kaydedildiği olağanüstü durum belge kayıt defteridir. Bu defterdeki bilgilerle EBYS'deki bilgiler karşılaştırılır ve özniteliklerin ne kadar korunduğu analiz edilebilir. Eşleşme sağlanıyorsa belgenin güvenilir olduğuna dair bir karine sunulabilir.

E-imzalı belgelerin güvenilirliğini tesis etmek için e-imza ve e-mühür gibi elektronik kimlik tespiti araçlarının yanı sıra EYP ve KEP delili gibi mekanizmalardan yararlanmak mümkün olsa da bunlar tek başına yeterli değildir. Çünkü güvenilirliği tehdit eden risklerin de giderilmesine ihtiyaç duyulmaktadır. Bunlar, dosyalamanın layıkıyla yapılamaması gibi güncel belge sürecinde oluşan riskler, bit akışının bozulması ve belge ile bileşenlerinin arasındaki ilişkinin kopması gibi teknolojik koşullardan kaynaklanan riskler ve güncel dönemde belgelerin başarılı bir şekilde yönetilmesini engelleyecek sürdürülebilirlikle ilgili riskler olarak öne çıkmaktadır.

---

98 **a.g.e.**

99 E-imzalı belgelerde son imzacının imzaladığı tarihi gösteren zaman damgasındaki tarih bilgisi, belge tarihi olarak esas alınırken, olağanüstü durumlarda hazırlanan belgeler imzalandığında kayıt altına alındığından bunların tarihi onun imzalandığı zamanı belirtir (**a.g.e.**).

100 Türkiye Cumhuriyeti Cumhurbaşkanlığı İdari İşler Başkanlığı Destek ve Mali Hizmetler Genel Müdürlüğü Bilgi ve Belge Yönetimi Daire Başkanlığı, **RYY Kılavuzu**, **a.g.e.**, s. 20.

2.3. Güvenilirliği Tehdit Eden Unsurlar

2.3.1. Güncel Belge Yönetim Sürecinde Riskler

2.3.1.1. Belge Formatının Korunamaması

E-belgeler, günümüzün bilgi teknolojisi yazılım ürünlerinin sunduğu endüstri standardına sahip JPEG, TIFF ve PDF, PDF/A, PDF/X gibi format yapılarında üretilmekte ve kullanılmaktadır. EBYS'lerde belgeler bu formatlarda üretilirken güvenli e-imza, EYP, üstveriler ve KEP entegrasyonuyla bir bütünlük arz ederler. Belgenin varlığı, bütünlüğü ve delil değeri bütün bunlarla anlam kazanır.

E-belgeler üretilirken doğru formatın tercih edilmemesi ve kullanılan formatları korumak için gerekli önlemlerin alınmaması durumunda belgelere uzun dönemde erişim sorunu yaşanabilir. Bu sorunlar, kurumun onaylanmış bir dosya formatı listesinin bulunmaması, belgenin endüstri standardı ya da özgür bir formatta üretilmemesi, formatın zaman içerisinde bozulması ve kullanılan yazılımın formatı açamaması gibi nedenlerden kaynaklanmaktadır[101]. Bu hususlar, e-belgelerin özgünlüğünün bozulması riskini taşımaktadır. Mesela, ABD'de bazı devlet başkanlarının görevleri boyunca ürettikleri e-belgelerin (resmî e-yazışma, e-posta, fotoğraf vb.) NARA'ya devrinde bazı problemlerle karşılaşılmıştır. 2008 ve 2009 yıllarında NARA'ya transfer edilen George Bush dönemine ait 267 milyon belgenin 65 milyonunda virüslü, içeriksiz, okunamayan vb. gibi farklı sorunlar saptanmıştır. Bu çalışmalar sırasında nasıl açılıp okunacağı tespit edilemeyen formatlarda belgeler görülmüştür[102]. Bundan dolayı, belgeler üretilmeden önce hangi format ve kurallarda üretileceğinin belirlenmesinin gerekli olduğu anlaşılmıştır. Böylece, bilgi ve belge güvenliği olmayan ve sürdürülebilirliği sağlanamayan formatta belge oluşumunun önüne geçilebilir. Belgenin hangi format ve şartlarda üretileceği, nasıl korunacağı ve transfer edileceğinin belirlenmesi güvenilirliğin korunmasında önemli bir aşama olarak değerlendirilmektedir.

Ancak, kullanılacak ortam endüstri formatı olarak belirlense de bazılarının sahtelerinin kolay üretilmesi, karmaşık bit yapısına sahip olması gibi sebeplerden

---

101 TNA, **Managing Digital Contunity Loss**, **a.g.e.**, s. 7.

102 Kenneth Thibodeau, "The Perfect Archival Storm: The Transfer of Electronic Records from the G. W. Bush White House to the National Archives of United States", **The Memory of the World in the Digital Age: Digitization and Preservation**, 26-28 Eylül 2012, ed.: Luciana Duranti ve Elizabeth Shaffer, Vancouver[Kanada], UNESCO, 2013, s. 732.

dolayı güvenilirliği tehdit eden sorunlarla karşılaşılmaktadır. Mesela Türkiye'deki Birlikte Çalışabilirlik Esasları Rehberi gereği metin tabanlı belgeler PDF/A formatında olmalıdır. Fakat, bu formatın çeşitli sorunları olduğu ileri sürülmektedir. Bunlar, karmaşık bir yapıya sahip olmak (11 farklı dizilim (sentax), en az 20 farklı bit yapısı, 2 şifreleme algoritması gibi), destek verilebilirliğin kısıtlılığı, sahtelerinin üretilebilirliği ve JSTOR/Harvard Object Validation Environment (JHOVE - JSTOR/Harvard Nesne Doğrulama Ortamı) ve Digital Record Object Identification (DROID - Sayısal Belge Nesnesi Kimliklendirme) gibi doğrulama araçları tarafından doğrulanamaması olarak belirtilmektedir[103]. Bu sorunlara karşılık Open Preservation Foundation (OPF - Açık Koruma Vakfı), PDF Derneği ve Digital Preservation Coalition (DPC - Sayısal Koruma Koalisyonu) tarafından VeraPDF uygulaması geliştirilmiştir. Bu uygulama, PDF dosyalarının doğrulamasını gerçekleştirmekte; varsa eksik olan üstverileri eklemektedir[104].

Bu sorunlar yaşansa da çözümüne yönelik çeşitli çalışmaların yapıldığı bilinmektedir. Mesela ABD'de yapılan bir çalışmada 28 bin 313 adet karakter sorunu, sentax hataları, sayfa yapısı gibi problemler içeren PDF dosyasının %87,5'inin sorunlarının giderildiği belirtilmektedir. 28 bin 313 dosyanın %61,2'sinin ise PDF/A'ya dönüştürülerek JHOVE ile VeraPDF gibi araçlarla doğrulandığı ifade edilmektedir[105].

Format yapısından kaynaklanan sorunlar çıkabildiği gibi teknik destek yapısının bazı alanlarda kullanıcı tercihine bırakılması sebebiyle yanlış kullanıma neden olan problemler de yaşanabilmektedir. Örneğin Japonya'da yapılan bir analizde 1 buçuk milyon PDF dosyasından sadece 14 bininin PDF/A formatında olup uzun dönemli korumaya uygun olduğu ifade edilmektedir. Bu bir milyon beş yüz bin PDF dosyasının %30'unun kullanıcılar tarafından şifrelenmesi nedeniyle uzun dönemli koruma için elverişli bulunmadığı görülmüştür. Bununla birlikte, yaklaşık %50'sinin

---

103 Duff Johnson, "Achieving Canonical PDF Validation", **11. International Conference on Digital Preservation**, 6-10 Ekim 2014, ed.: Serena Coates vd., Melbourne[Avustralya], State Library of Victoria, 2014, s. 40-41, (Çevrimiçi) https:// phaidra. univie. ac. at/ detail_ object/ o:378066, 5 Mart 2020. ; Marco Klindt, "PDF/A Considered Harmful for Digital Preservation", **14. International Conference on Digital Preservation**, 25-29 Eylül 2017, Kyoto[Japonya], yayımcı yok, 2017, (Çevrimiçi) https://ipres2017.jp/wp-content/uploads/15.pdf, 31 Aralık 2019.

104 **VeraPDF Web Sitesi**, (Çevrimiçi) https://verapdf.org, 20 Şubat 2020.

105 Juha Lehtonen vd., "PDF Mayhem: Is Broken Really Broken?", **15. International Conference on Digital Preservation**, 24-27 Eylül 2018, ed.: Megan Potterbusch vd., Boston[ABD], yayımcı yok, 2018, (Çevrimiçi) https://osf.io/n85b9/, 5 Ocak 2020.

üreten, %20'sinin de başlık gibi üstverileri içermediği anlaşılmıştır. Ancak, bazı PDF'lerin zengin üstveri içerdiği de belirtilmektedir[106].

2.3.1.2. Dosya Yönetiminin Planlanmaması

Güncel belgelerin yönetim risklerinden olan dosya formatının doğru seçilememesinin yanı sıra karşılaşılan bir diğer sorun da dosyalamayla ilgili hatalı uygulamalardır. Çeşitli çalışmalarda, e-belgelerin dosyalanmasıyla ilgili risklerin 2008'de yaşanan küresel ekonomik buhran neticesinde daha iyi fark edildiği dile getirilmektedir. Buhran'ın sebep olduğu zararlar incelenirken finans kuruluşlarında oluşan belgelerin organik bağının kurulamadığı anlaşılmıştır. Belgelerin, aralarında organik bağ bulunduğu diğer belgelerle ilişkilendirilmesi yerine, daha çok tek başına bilgi içeren bir nesne olarak yönetildiği gözlenmiştir. Bundan dolayı, belgelerin konteksti açığa çıkarılamamış; belgelerle fonksiyon arasındaki ilişki kurulamamıştır[107]. Bu sorunlara bir çözüm olarak dosya bütünlüğünün ne kadar ehemmiyetli olduğu, aynı zamanda uygun dosya tasnif planının seçilmesi gerektiği bir kez daha fark edilmiştir. Bunun neticesinde özellikle mali kayıtlar için tasnif yöntemi geliştirilmeye çalışılmıştır. Tasnif planının fonksiyon odaklı olması gerektiği görülmüştür[108].

Plan oluşturulurken kurumun fonksiyonları analiz edilerek seriler saptanır[109]. Seriyi meydana getiren dosyaların türleri belirlenir. Aynı zamanda her bir dosyanın

---

106 Teru Agata, Yosuke Miyata ve Atsushi Ikeuchi, "Long-term Preservation of PDF Files in Institutional Repositories in Japan", **16. International Conference on Digital Preservation**, 16-20 Eylül, 2019, ed.: Marcel Ras, Sierman, Barbara ve Puggioni, Angela, Amsterdam[Hollanda], yayımcı yok, 2019, s. 423-425, (Çevrimiçi) https:// ipres2019. org/ static/ proceedings/iPRES2019.pdf, 5 Mart 2020.

107 Julian Cunningham-Day ve Marly Didizian, "Data Exchange and Confidentiality: An Asia Pacific Perspective", **Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra[Birleşik Krallık], Facet Publishing, 2011, s. 61. ; 2008'de yaşanan ekonomik buhranla birlikte belgeleri uzun süreli arşivlemenin ciddi emek isteyen bir süreç olduğu fark edilmiştir. Bunun nedenlerinden biri olarak arşivciler ile bilişim uzmanlarının meseleye farklı yaklaşması gösterilmektedir. Bilişim uzmanlarının, arşivlemeyi çevrimiçi çalışan sistemlerin daha sağlıklı yönetilebilmesi için güncel olmayan veriyi çevrimdışı ortamlara taşımak şeklinde anladığı ifade edilmektedir. Çevrimdışı ortamlara taşınan bu verilerin de sağlıklı yönetilmesi gerektiği kabul edilmiştir (Geoffrey Yeo, "Introduction", **Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra[Birleşik Krallık], Facet Publishing, 2011, s. xix-xx).

108 Aaron J. Loehrlein, Victoria L. Lemieux ve Michael Bennett, "The Classification of Financial Products", **Journal of the Association for Information Science and Technology**, C. 65, No: 2, 2014, s. 263-264, 277.

109 Jim Suderman, "Defining Electronic Series: A Study", **Archivaria**, No: 53, 2002, s. 35-36, 45.

karşılığı olan vaka ve konu olarak iş, bunun gerçekleşmesini sağlayan faaliyet ve işlemler açığa çıkarılır. Böylece, belge, işlem, faaliyet, iş, fonksiyon ve seri arasında belge hiyerarşisi mantığıyla ilişki kurulmaya çalışılır. Bu ilişkiyi oluşturacak organik bağ ve bunu ifade edecek dosya kodu ve tek biçim başlık gibi araçlar kullanılır. Bu sürecin sağlıklı şekilde akışını sağlamak için fonksiyon odaklı dosya planının kullanılması gerekir. Ancak, bazı EBYS uygulamalarında dosya planlarının yeteri kadar sağlıklı oluşturulmadığı; bu sebeple belgedeki dosya kodunun organik bağ kurmaya yönelik verilmediği; neticede belgeler arasında bütünlük sağlanamadığı bilinmektedir[110]. Bu sorunlar, bir vaka/konuya ait iş ve işlemlerle ilgili kopuklukların oluşmasına yol açabildiğinden[111], dosyadaki belge varlığının sorgulanması sonucunu doğurur. Her ne kadar bu olumsuz durum, belgenin tek başına özgünlüğünün sorgulanmasıyla alakalı bir sorun oluşturmasa da paydaşı olması gereken belgelerle organik bağ kurulamadığından fonksiyon ve faaliyetle ilgili kontekstte kopukluğa sebep olacaktır. Hâliyle, bir belgenin ait olduğu dosyada bulunmaması ya da yanlış dosyada bulunması güvenilirliği tehdit eden bir risk olarak karşımıza çıkabilir.

Bu risk, en başta e-belge yönetimi uygulamalarında işe göre dosya açılmamasından kaynaklanmaktadır. Dosya açılmadığı gibi, belgelere verilen dosya kodları paydaş belgeler arasında organik bağ kurmak yerine, sadece bir etiket olarak kullanılmaktadır. Yalnızca bu etiket ile veri tabanı arasında bir ilişki oluşturulmaktadır. Bundan dolayı belgeler, ait oldukları fonksiyona göre organik bağı kurulan diğer belgelerle aynı dosya içerisinde bulunmayıp, tek başına tutulmaktadır[112]. Bu tarz yanlış dosyalamalarda ilgili işe ait bilgi bütünlüğünün sağlanması güçleşmektedir[113].

Güncel kullanım safhasında sağlıklı dosyalanmayan belgeler, arşive de sağlıklı devredilememektedir. Devredilmesi durumunda ise arşiv depolarında dosyaların yeniden düzenlenmek zorunda kalındığı bilinmektedir. Hâliyle, dosyalar uygunluk

110 Çiçek, "Elektronik Belge Yönetimi Uygulamalarında Dosya Bütünlüğü Problemi", **a.g.e.**

111 Bahattin Yalçınkaya, "Belge Yönetim Sistemlerinde ve Süreçlerinde Risk Tanımları", **Arşiv Dünyası**, No: 16-17, 2014, s. 20-23.

112 Geoffrey Yeo, "Trust and Context in Cyberpsace", **Archives and Records**, C. 34, No: 2, 2013, s. 214-219.

113 Çiçek, "Elektronik Belge Yönetimi Uygulamalarında Bir Alt Sistem Olarak Dosya Yönetimi", **a.g.e.**, s. 435-436.

kontrolü yapılıp tekrar gözden geçirilerek konu ya da vakaya göre dosya bütünlüğü oluşturulduktan sonra arşive devredilmelidir[114].

Uygunluk kontrolü yapılarak arşive devredilen belgelerin güvenilirlik kontrolünde envanter listesinden yararlanılabilir[115]. Bu listede belgelerin dosyadaki sırası, yılı, konusu, sayısı, gizlilik derecesi ve dosya kodu gibi bilgiler yer alır[116]. Bunlar, dosyasında bulunması gereken ama yerinde olmayan ya da o dosyada bulunmaması icap eden belgelerin güvenilirliklerinden şüphe duyulduğunda bir kontrol mekanizması olarak işlev görür. Bundan dolayı, EBYS'lerde üretilip arşivlenen belgeler için envanter listesinin hazırlanması unutulmamalıdır.

EBYS'lerde dosyalamayla ilgili yaşanan sorunlar üzerine yapılan çeşitli çalışmalarda, kamu kurumlarında "099 Diğer" ya da "804 Gelen-Giden Evrak" gibi dosya koduna sahip milyonlarca belgelerin bulunduğu belirtilmektedir[117]. Durum böyle olunca, "099 Diğer" ve "804 Gelen-Giden Evrak" dosya kodları ile etiketlenen belgelerin ait oldukları iş ve faaliyetle ilişkilendirilmediği anlaşılmaktadır. Çünkü "804 Gelen-Giden Evrak" gibi etikete sahip belgelerin kurumlarla yapılan yazışmalardan teşekkül ettiği bilinmektedir. Bu belgeler, işlem gördüğü kurumunda girmesi gereken konu ya da vaka dosyasına kaldırılmalıdır. Bunun yapılmadığı belgelerin bir yığın oluşturduğu görülmektedir. Yığınlardan da kontekstin açığa çıkarılması pek mümkün olamamaktadır[118].

Organik bağı kurulup bütünlüğü sağlamak adına ait olduğu dosyasına giremeyen e-belgelerin güvenilirliğinin başarıyla korunamayacağı düşünülmektedir. Mesela ihale dosyasında bulunması gereken bir sözleşme, dosyada mevcut değilse dosyadan elde edilecek bilgi tam olmayacaktır. Bundan dolayı ihale konusu layıkıyla değerlendirilemeyecektir. Hâliyle belgelerin gerçekliğinin korunup korunamadığından

---

114 "Devlet Arşiv Hizmetleri Hakkında Yönetmelik", **R.G.**, S 30922, tar. 18.10.2019, (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2019/10/20191018-9.pdf, 22 Mayıs 2020.

115 Heather MacNeil, "Methods for Creating and Maintaning Reliable and Authentic Electronic Records", **Preservation of the Integrity of Electronic Records**, ed.: Luciana Duranti, Terry Eastwood ve Heather MacNeil, yayım yeri yok, Springer, 2002, s. 50.

116 "Devlet Arşiv Hizmetleri Hakkında Yönetmelik", **a.g.e.**

117 Solhan, **a.g.e.**, s. 52-53.; Hatice Gümüş, "Kurumlarda EBYS ve Arşiv Çalışmaları, Yaşanan Sorunlara Genel Bir Bakış", **e-Beyas 2015 Sempozyumu Kurumsal Belleklerin Geleceği: Dijitalleştirme-Elektronik Arşiv-Elektronik Belge Yönetimi**, 21-22 Ekim 2015, ed.: Fahrettin Özdemirci vd., Ankara, Ankara Üniversitesi, 2016, s. 98.

118 Çiçek, "Elektronik Belge Yönetimi Uygulamalarında Dosya Bütünlüğü Problemi", **a.g.e.**, s. 164.

şüphe duyulabilir[119]. Oysa bazı sektörlerde belgeleri ait oldukları iş ve faaliyete göre dosyalama, aynı zamanda hukuki bir normdur. Örneğin VUK'un 241. maddesine göre belgelerin dosyasında muhafaza edilmesi, TTK'nın 82. maddesi uyarınca da sınıflandırılmış bir şekilde saklanması gerekir[120].

Dosyalamayla ilgili bu sorunların kaynağı olarak sistemlerin uzman personel tarafından geliştirilmemesi, yanlış yapılan dosyalama işlemlerinin takip edilebileceği bir mekanizma kurulmaması, yazılımların dosyalamanın gerektirdiği mantığa sahip olmaması ve bu konudaki kurum kültürünün gelişmemesi gösterilebilir[121]. Bunun neticesinde dosyalama işi kurumlarda yanlış yerde başlatılabilmektedir. Belgenin onu kullanan birimde dosyalanması gerekirken, bu işlem genellikle evrak kayıt bürolarında yapılmaktadır. Evrak kayıt memurları, belgeye hızlıca bakıp bir dosya kodu atamakta ve kurumda belgenin dosyalandığı algısı oluşabilmektedir. Oysaki dosyalama, belgenin ait olduğu faaliyet ve fonksiyonla ilişkisinin yani organik bağının kurulmasıdır. Bunu en iyi gerçekleştirecek olanlar, belgeyi kullanan birimlerde bilgi ve belge uzmanı olarak çalışanlardır[122].

Belgeleri ait oldukları vaka ya da konu dosyasıyla ilişkilendirmemek yığın oluştururken bu durumun bir sebebi de elektronik ortamdaki her türlü kaydı tasfiye etmeden tutma gayretidir. Verilerin elektronik ortamda kolayca saklanabileceği düşüncesinin[123]; aynı zamanda teknolojik altyapı ve kurumsal destek eksikliğinin bunda etkili olduğu anlaşılmaktadır. Mesela, ABD'de 2008 yılında yapılan bir araştırmaya göre kurumların yüzde 60'ının adli bir vakayı aydınlatmak için yapılan elektronik keşif (e-discovery)[124] sürecini idame ettirebilecek bir teknolojik altyapıya,

---

119 Bu risk, aynı zamanda Uganda'da milyarlarca liralık kamu zararına sebep olmuştur. Çünkü ihalelerle ilgili sözleşmeler bulunamadığından ihaleyle ilgili tam bir bilgi elde etmek mümkün olmamıştır (Ronald Tumuhairwe ve Arthur Ahimbisibwe, "Procurement Records Compliance, Effective Risk Management and Records Management Performance: Evidence from Ugandan Public Procuring and Disposing Entities", **Records Management Journal**, C. 26, No: 1, 2016, s. 85).

120 "VUK", **a.g.e.**

121 Çiçek, "Elektronik Belge Yönetimi Uygulamalarında Bir Alt Sistem Olarak Dosya Yönetimi", **a.g.e.**, s. 437.

122 Çiçek, "Elektronik Belge Yönetimi Uygulamalarında Dosya Bütünlüğü Problemi", **a.g.e.**

123 Natasha Dow Schüll, "Digital Containment and its Discontents", **History and Anthropology**, C. 29, No: 1, 2018, s. 42, 44.

124 Elektronik keşif, davalı taraflar arasında uyuşmazlık konusu vakıayla ilişkili olduğu düşünülen delillerin duruşmadan önce incelenmesini mümkün kılan yasal bir süreçtir. Keşif sürecinde tarafların erişimine açılan kurumsal belgelerden incelenip uyuşmazlık konusu vakıayla ilişkili olduğu düşünülenler mahkemeye delil olarak sunulabilir (Sautter, **a.g.e.**, s. 20).

%53'ünün de bir saklama politikasına sahip olmadığı ifade edilmektedir[125]. 2015 yılında büyük ölçekli kuruluşlarda bu keşif sürecine önem verildiği görülse de orta ölçekteki şirketlerde söz konusu sürece yeteri kadar yatırım yapılmadığı gözlenmiştir[126]. 2018 yılında yayınlanan başka bir raporda ise araştırmaya katılan kurumların yüzde 77'si, kurumda oluşan tüm verileri sakladıklarını belirtmektedir[127]. Türkiye'deki kurumların e-belgeleri saklama ve imha uygulamalarına yönelik bir çalışma henüz görülemese[128] de sahadaki uygulamalar pek çok kurumun oluşturdukları tüm e-belgeleri sakladığını göstermektedir. Durum böyle olunca, kurumlarda yığın oluştuğu düşünülmektedir.

Avustralyalı bilgi ve belge uzmanı Sharyn Wise, verileri muhafaza etmenin onları yönetmek anlamına gelmediğini ileri sürmektedir[129]. Bu görüşe benzer bir şekilde, SALT Araştırma'nın kurucu direktörü Vasıf Kortun, elektronik ortamda arşiv değeri olmayan pek çok sayısal malzemenin bulunduğunu ve bunun sonucunda lüzumsuz olan malzemelerin gereksiz yere saklandığını dile getirmektedir. Bu düşünce, belgelerin yönetilmeyip yığın oluşturulduğunu düşündürmektedir[130]. Belge yönetiminde, belgelerin üstverilerle tanımlanarak birbirleriyle olan çok yönlü ilişkisinin açığa çıkarılması hedeflenirken; yığın oluşturma, belgeler üzerindeki bu entelektüel kontrolü azaltmaktadır[131]. Bundan dolayı, belgelerin kontekstinin açığa çıkarılamaması riski gündeme gelmektedir[132].

---

125 Burke Ward vd., "Electronic Discovery Rules for a Digital Age", **Boston University Journal of Science and Technology Law**, C. 18, No: 150, 2012, s. 24, (Çevrimiçi) https :// papers. ssrn. com/sol3/papers.cfm?abstract_id=2229408, 5 Mart 2020.

126 BDO Consulting, **Inside E-Discovery: The State of E-Discovery According to Corporate Counsel,** 2015, (Çevrimiçi) https://www.bdo.com/getattachment/Insights/Consulting/Inside-E-Discovery/2015-BDOC-E-Discovery-report-WEB.pdf.aspx, 5 Mart 2020.

127 Exterro, **The State of E-Discovery 2018**, 2018, yayım yeri yok, yayımcı yok, s. 23, 40.

128 Ceyhan Güler, Türkiye'deki bazı kurumların Kişisel Verilerin Korunması Kanunu kapsamındaki imha yöntemlerini incelemiştir (Ceyhan Güler, **Elektronik Belgelerin İmhası: Teori ve Uygulama**, İstanbul, Hiperlink Yayınları, 2020). Ancak, saha araştırması yapılarak kurumlarda oluşan e-belgelerin saklama süreleri ve koşullarını inceleyen bir çalışmaya ihtiyaç duyulmaktadır.

129 Kim Williams, **Twitter**, 26 Temmuz 2018, (Çevrimiçi) https :// twitter. com / thelibrarykim / status/1022280871259168768, 6 Mart 2020.

130 Vasıf Kortun, **Bu Bize Ne Anlatıyor**, (Çevrimiçi) https://www.unlimitedrag.com/post/bu-bize-ne-anlat%C4%B1yor, 26 Şubat 2020. ; Geoffrey Yeo, arşivcilerin elektronik ortamda yoğun bir belge akışıyla karşıya kaldığını dile getirerek bunun sağlıklı bir belge yönetimi işleyişini engellediğini ileri sürmektedir (Geoffrey Yeo, **Records, Information and Data: Exploring the Role of Record-keeping in an Information Culture**, Londra[Birleşik Krallık], Facet Publishing, 2018, s. 194).

131 David Weinberger, **Everything is Miscellaneous: The Power of the New Digital Disorder**, New York[ABD], Holt Paperbacks, 2008, s. 129-130.

132 ISO, **27050-1 Electronic Discovery Part 1: Overview and Concepts**, **a.g.e.**, s. 10.

Levent Erden, günümüzde insanların geleceği ve geçmişi öncelemekten ziyade, anı yaşamaya odaklandığını ileri sürmektedir. İnsanın, geçmişten bugüne kadar ölümsüzlüğü bulmaya ve anı korumaya yönelik hareket ettiğini dile getirmektedir. Buna imparatorlukların yaptığı heykelleri, tabloları ve fotoğrafları örnek göstermektedir[133]. Belgeler de bir bakıma kayıp, yok oluş ve ölüme karşı insanın devamlılığını sürdürme amacıyla oluşturulurlar[134]. Ancak, kurumların, ürettikleri belgeleri saklayıp korumak amacıyla hareket etmek yerine, yer sıkıntısı olmadığını düşündükleri için belge yığını oluşturmayı tercih ettiği görülmektedir.

Çeşitli ülkelerde yapılan araştırmalarda e-belgelerin ait oldukları faaliyetle olan ilişkilerinin müphem olduğu belirtilmektedir. Örneğin Belçika'da gerçekleştirilen Flaman Kurum ve Kuruluşlarında Elektronik Arşivleme (Digitale archivering in/voor Vlaamse instellingen en diensten - DAVID) Projesinde, kâğıt ortamında belge ile ait olduğu faaliyet arasındaki ilişkinin korunduğu fakat elektronik ortamda bu ilişkinin kaybolduğu belirtilmektedir. Halbuki, e-belgeler söz konusu olduğunda da belgelerin ait olduğu kurumsal fonksiyonla ilişkilendirilmesi gerekir. Bunu gerçekleştirmenin yöntemlerinden birinin dosyalama olduğu kabul edilmektedir. E-belgeler üretilmelerine sebep olan iş, konu ve faaliyetle ilişkilendirilerek dosyalanırsa ait olduğu kurumsal fonksiyonları yansıtabilecektir. Aksi takdirde kontekstin açığa çıkarılamaması riski söz konusu olduğundan belgelerin temel karakteristiği kaybolabilecek ve güvenilirlikleri sorgulanabilecektir[135].

2.3.2. Gerekli Teknolojik Koşulların Sağlanamaması

Bilgi teknolojisi ürünü olan yeni nesil taşıyıcı ortamlar, teknolojinin çok hızlı değişmesi ve ürünlerin kırılgan bir yapıya sahip olması nedeniyle kullanım ve muhafaza sırasında birçok risk barındırmaktadır. Sürekli yeni nesil ürünlerin piyasada kullanılmaya başlanması, belgelerin saklandığı depolama ortamları, kullanılan yazılımlar ve belge formatlarının da değişebilmesine sebep olmaktadır. Bu değişimler

133 Türkiye Radyo Televizyon Kurumu (TRT) 2, **Levent Erden: Anjelika Akbar ile Sesler**, (Çevrimiçi) https:// www. facebook. com/ watch/?v=556779264910717, 18 Şubat 2020.

134 Mehmet Torunlar, "Arşiv-Hafıza-Kamusal Ensefalizasyon", **Arşiv Dünyası**, C. 6, No: 2, 2019, s. 120-121.

135 Filip Boudrez vd., **Digital Archiving: The New Challenge?**. IRIS, Belçika, 2005, s. 77, 113.

neticesinde depolama ortamlarında bit kaybı oluşabilmekte[136], yazılım hatalarıyla karşılaşılabilmekte ve kullanılan cihazların ömrü kısalabilmektedir[137]. Durum böyle olunca, belgelerin güvenilirliği de sorgulanır hâle gelebilmektedir. Tüm bunlara kurumsal sürdürülebilirliğin sağlanamaması, yangın, sel gibi afetlere karşı planlar yapılamaması gibi yeni sorunlar eklenebilmektedir[138].

Bu sorunlardan dolayı, kurumların karşılaşabilecekleri riskleri belirleyerek çözüm yolları geliştirmesi gerekir. Bu riskler, belgedeki bit akışının bozulması, belge ile bileşenleri arasındaki ilişkinin kopması, belgelere yetkisiz kişilerin erişmesi, güvenilirliği korumak için gerekli olan yazılım ve donanım koşullarının sağlanamaması, şifrelemenin belgenin okunabilirliğini olumsuz etkilemesi, özet değerlerinin eşleşememesi ve teknolojik göç sürecinin layıkıyla gerçekleştirilememesi olarak öne çıkmaktadır. Belirtilen risklerin bir kısmının telafisi mümkünken bazılarının geri dönülemez sonuçlar doğurabileceği bilinmelidir.

Teknolojik koşullar kaynaklı risklerin başında bit akışının bozulmasının geldiği görülmektedir. Çünkü, radyasyon, sabit disklerin okuma ve yazma yapan kısımlarının birbiriyle çarpışması, depolama donanımının eskimesi gibi nedenlerle bit akışı bozulabilmektedir. Bunun sonucunda belgeyi oluşturan bileşenlere erişim

---

136 Elektronik malzemelerin korunması üzerine çalışan uzmanlardan David Rosenthal, Conseil Européen pour la Recherche Nucléaire (CERN - Avrupa Nükleer Araştırma Merkezi)'de disklere kaydedilen verilerin bir kısmının ısı, ışık ve nem gibi gerekli önlemlerin alınamaması nedeniyle altı ay içerisinde bozulduğunu ifade etmektedir (David S. Rosenthal, "Bit Preservation: A Solved Problem?", **5. International Conference on Preservation of Digital Objects: Joined Up and Working: Tools and Methods for Digital Preservation**, 29-30 Eylül 2008, Londra, The British Library, 2008, s. 277- 279, (Çevrimiçi) https://phaidra.univie.ac.at/detail_object/o:294190, 4 Mart 2020).

137 Optik ve manyetik ortamların ömürlerinin çok uzun olmadığı dile getirilmektedir (Yan Han ve Chi Pak Chan, "The Modeling System Reliability For Digital Preservation: Model Modification and Four-Copy Model Study", **5. International Conference on Preservation of Digital Objects: Joined Up and Working: Tools and Methods for Digital Preservation**, 29-30 Eylül 2008, Londra[Birleşik Krallık], The British Library, 2008, s. 281, (Çevrimiçi) https :// phaidra. univie.ac.at/detail_object/o:294190, 4 Mart 2020. ; Lauren J. Young, **Data Reawakening: The "File Not Found" Series: Part 3 of 3**, (Çevrimiçi) https :// apps. sciencefriday. com/ data/ reawakening.html, 4 Mart 2020). Brigham Young Üniversitesinde bazı verilerin 1995'ten beri yıllık olarak kompakt disklere (compact disk - CD) kaydedildiği ve bu CD'lerin yüzde beşine erişilemediği belirtilmektedir. Bununla birlikte, 8 terabyte boyutundaki bir ana görüntü kopyasının harici disklerde kaybolduğu ifade edilmektedir (Chris L. Erickson ve Barry M. Lunt, "Alternatives for Long-Term Storage of Digital Information", **12. International Conference on Digital Preservation**, 2-6 Kasım 2015, ed.: Christopher Lee, North Carolina[ABD], School of Information and Library Science University of North Carolina at Chapel Hill, 2015,s. 231-232, (Çevrimiçi) https:// phaidra. univie. ac. at/view/o:429524, 4 Mart 2020).

138 David S. Rosenthal vd., "Requirements for Digital Preservation Systems: A Bottom-Up Approach", **a.g.e.**

mümkün olamayabilir ve belge yeniden üretilemeyebilir. 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[139]. Belgenin yeniden üretilememe tehlikesini barındırdığından bit akışının bozulması riskinin tehdit gücü oldukça yüksektir.

Belge ile üstveri, ekleri ve e-imza gibi bileşenleri arasındaki ilişkinin kopma ihtimali de söz konusudur. Bu ihtimal, farklı işletim sistemleri arasında belge transferi yapılması ve 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, bu iki sistem arasında belge alışverişi yapıldığında belgeler okunamayabilir[140]. Bununla birlikte, belge ile üstveri dosyası gibi bileşenleri arasında ayrılmaz bir ilişki kurulamamış olabilir. Bundan dolayı, DROID ve JHOVE gibi format tanımlayıcıların kullanılarak işletim sistemlerinden bağımsız şekilde belgelerin standart bir yapıda üretilmesi[141] ve belge ile bileşenlerine tek biçim tanımlayıcılar atanması önerilmektedir[142].

E-belgelerin güvenilirliğini etkileyen unsurlardan biri de onun yönetildiği sistemlerle ilgilidir. Bu sistemler, mutlak erişim kontrolü gibi ilkeler ışığında çalışmazsa belgeler yetkisi olmayanlar tarafından görülüp kullanılabilir. Bunun neticesinde ticari sır ve kişisel verilerin gizliliği gibi mahremiyet kaygılarından dolayı EBYS'lerdeki belge alışverişinde dirençlerle karşılaşılabilir. Bu durum, faaliyetlerin yerine getirilmesini geciktirebilmekte ve iş verimliliğini de azaltabilmektedir. Aynı zamanda erişim kontrolleri uygulanmadığında mahremiyet içeren bilgilerin açığa çıkması gibi üçüncü şahısların hakları korunamadığından toplumsal sıkıntılar

---

139 Sarah Glassford, "Black Hole or Brave New World? Archivists, Historians and the Challenges of the Digital Age", **Emerging Library & Information Perspectives**, C. 1, No:1, 2018, s. 95-97. ; ISO, **27040 Security Techniques: Storage Security**, **a.g.e.**, s. 14-17.

140 Jinfang Niu, "Original Order in the Digital World", **Archives and Manuscripts**, C. 43, No: 1, 2015, s. 67.

141 Matthew G. Kirschenbaum vd., **Digital Forensics and Born-Digital Content in Cultural Heritage Collections**, Washington[ABD], Council on Library and Information Resources, 2010, s. 17-19.

142 TNA, **Migrating Information between Records Management Systems**, **a.g.e.**, s. 28-31.

oluşabilmektedir[143]. Söz konusu sorunlarla karşılaşmamak için EBYS'lerde erişim kontrolleri -kullanıcı profil ve rolleri- tanımlanarak hangi belgeye hangi yetki dâhilinde erişileceği belirlenmelidir[144].

E-belgelerin güvenilirliğini doğrudan etkileyen bir diğer husus da kullanılan donanımlar için uygun sıcaklık, nem ve ışık koşullarıdır. 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 bilişim sistemlerinde Redundant Array of Independent Disks (RAID - Bağımsız Disklerin Artıklık Dizisi) 10 gibi saklamada başarılı olduğu kabul edilen yöntemlere sahip saklama cihazlarının kullanılması önerilmektedir[145]. Bununla birlikte, teknolojik eskimeyle karşı karşıya kalmamak için yeni cihazlara periyodik olarak belge aktarımı yapılabilir.

E-belgelerin güvenilirliğini tehdit eden hususlardan biri de kullanılan yazılımlara zamanı geldiğinde gerekli yamaların yapılmamasıdır. Bunun neticesinde sistemden veri sızıntısı, belge yönetimi standartlarına uyum sağlayamamak ve belgelere uzun dönemli koruma yöntemlerinin uygulanmaması gibi sorunlar oluşabilir. Bunlar, belgelerin bütünlüğünü bozabilecek mahiyettedir. Oysa bütünlüğü korumak için yazılımların periyodik olarak güncellenmesi önerilmektedir[146].

E-belgeler, format, işletim sistemi ve yazılım dilleri gibi çeşitli teknolojik bileşenlere bağımlıdır. Sürdürülebilirlik için söz konusu bileşenlerin bilinçli olarak kontrollü bir şekilde yönetilmesi gerekir. Bu sebeple 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[147].

---

143 ISO, **17068 Trusted Third Party Repository for Digital Records**, **a.g.e.**, s. 4. ; James Manor, "The Potential -Constructive and Destructive- of Information Technology for Records Management: Case Studies from India", **A Matter of Trust: Building Integrity into Data, Statistics and Records to Support the Sustainable Development Goals**, ed.: Anne Thurston, Londra[Birleşik Krallık], University of London Press, 2020, s. 70.

144 TNA, **Migrating Information between Records Management Systems**, **a.g.e.**, s. 33.

145 ISO, **18492 Long-term Preservation of Electronic Document-based Information**, **a.g.e.**, s. 4.

146 TNA, **Managing Digital Contuinity**, 2017, s. 11-12, (Çevrimiçi) https :// nationalarchives. gov. uk/documents/information-management/managing-digital-continuity.pdf., 8 Aralık 2020.

147 **a.e.** ; TNA, **Mapping the Technical Dependencies of Information Assets**, 2017, s. 5-6, (Çevrimiçi) https :// www. nationalarchives. gov. uk/ documents/ information-management/ mapping-technical-dependencies.pdf, 8 Aralık 2020.

Teknolojik bileşenler tanımlanırken format, kullanılacak cihazlar, teknolojik göç planları gibi belgenin erişim ve saklamasını etkileyen hususlar ifade edilmektedir. Aynı zamanda, belgelerin üretilme koşulları ve onu meydana getiren bileşenler tanımlanıp, üstverilerle arasındaki ilişki kurulup, bütünlük ve tamlığın kontrolü sağlanırken, log kayıtlarında yer alacak hususlarla benimsenecek güvenlik önlemleri de açıklanır[148].

Güvenilirliğin korunması amacıyla e-belgeye kimin ne zaman nasıl eriştiğini gösteren log kayıtlarından oldukça faydalanıldığı görülmektedir. Bundan dolayı, bu kayıtların özgünlüğü korunarak belgeyle ilişkilendirilmeleri gerekir[149]. Bunlar, aynı zamanda yeni formatlara aktarılabilir olmalıdır.

Güvenilirliği tehdit eden diğer risklerden biri de şifrelemedir. Her ne kadar kurumsal şifreleme gibi mekanizmalar, güvenlik için çıkarılmış olsa da anahtarının unutulması, şifreleme sertifikasında kullanılan algoritmaların zayıflığı gibi durumlar belgeyi erişilemez kılabilir. KAMU SM'nin hazırladığı rehberde, zayıf ve yetersiz şifrelerin kullanılması, kriptografik anahtarların yanlış yöntemlerle üretilmesi ve bunların güvensiz bir ortamda saklanması riskler arasında gösterilmiştir. Ayrıca, EBYS'nin kriptografik anahtar ve sertifika kullanımıyla ilgili fonksiyonların değiştirildiğini fark edememesi diğer riskler arasında kabul edilmektedir[150]. Durum böyle olunca, şifreleme algoritmalarının standartlara uyumlu olması gerekir. Belgelerin, ne zaman ve nasıl şifrelendirildiğine dair bir kayıt, bunlara erişilemediğinde bir bozulma olup olmadığının denetlemesi için faydalı olabilir. Burada, şifreleme uygulamaları ve bu uygulamaların sonuçlarını gösteren log kayıtları da yer almalıdır[151].

Güvenilirliğin 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 özet değerleri farklılaşmakta ya da birbirleriyle eşleşememektedir[152]. Bunun

---

148 **a.g.e.**, s. 9-11.

149 Belgelerle ilgili oluşan log kayıtları ile belge ayrı dosyalardır. Bu dosyaların fiziki olarak bir arada tutulması ya da veri tabanında birbiriyle ilişkilendirilmesi gerekir (TNA, **Migrating Information between Records Management Systems**, **a.g.e.**, s. 32).

150 KAMU SM, **Elektronik Belgeleri Açık Anahtar Altyapısı Kullanarak Güvenli İşleme Rehberi**, **a.g.e.**, s. 7.

151 ISO, **27040 Security Techniques: Storage Security**, **a.g.e.**, s. 50-52.

152 Ragib Hasan vd., "Trustworthy Records Retention", **Handbook of Database Security**, ed.: Michael Gertz ve Sushil Jajodia, New York[ABD], Springer, 2008, s. 366.

neticesinde belgenin tahrif edilmiş olabileceği düşünülecektir. E-belgelerin güvenilirliği konusunda çalışmaları bulunan Corinne Rogers, teknolojik göç işlemleri sırasında oluşturulan özet değerleri korunursa sorunun hafifletilebileceğini dile getirmektedir[153]. Bununla birlikte, özet değeri oluşturulurken satır satır özet değeri (piecewise hashing) oluşturmanın daha sağlıklı sonuçlar verebileceği ifade edilmektedir[154].

Teknolojik koşullardan kaynaklı risklere karşı çözüm geliştirmek amacıyla belgenin üretildiği yazılımları korumak (öykünme/emulation)[155] ve teknolojik göç ettirme (migration) gibi çeşitli yöntemler tartışılmaktadır. Bilgisayar endüstrisinin hızla değişmesi, günümüz saklama ortamlarının veriyi kayıp yaşanmadan uzun süre saklayamaması, gelişen teknolojinin eski yöntemleri etkisiz kılması ve hizmet verilecek kitlenin bilgi birikiminin değişmesi yazılımları korumayı zorlaştıran unsurlar arasında kabul edilmektedir. Bundan dolayı, belgelerin üretildikleri formatın değiştirilmesi ya da bulundukları sistemin yenilenmesi gibi işlemler olarak karşımıza çıkan teknolojik göç ettirme sık kullanılan bir yöntem olmuştur[156].

Ancak, teknolojik göç sırasında belgelerin tek biçim tanımlayıcılarının değişmesi gibi güvenilirliği tehdit eden bazı risklerle karşılaşmak mümkündür. Bunun neticesinde kontekstin bozulabilmesi söz konusudur. Dolayısıyla teknolojik göç işlemleri sırasında belgenin içeriğiyle birlikte konteksti de muhafaza edilmelidir. Kontekstin muhafazası, diplomatik özellikler ile arşivsel bağın korunmasını gerektirir[157]. Bunun için önceden tanımlanmış standart form ve şablonlar oluşturmak, belge türü ve fonksiyona göre çeşitlenen yöntemlerle özgünlüğü tasdik etmek ve log kayıtları oluşturmak gibi çözüm önerileri

153 Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice", **a.g.e.**, s. 161.

154 Alex Garnett, Mike Winter ve Justin Simpson, "Checksums on Modern Filesystems, or: On the Virtuous Consumption of CPU Cycles", **15. International Conference on Digital Preservation**, 24-27 Eylül, ed.: Megan Potterbusch vd., Boston[ABD], yayımcı yok, 2018, (Çevrimiçi) https://osf.io/cxahf, 1 Ocak 2020.

155 Öykünme, elektronik nesnelerin oluşturuldukları ortamın yeniden tesis edilerek bunların ilk hâllerine dönüştürülmesidir. Farklı işletim sistemlerinin ilk hâllerine dönüştürülmesi, bilgisayar oyunlarının çalıştırılması gibi amaçlarla öykünmeden faydalanılmaktadır (Ross Harvey ve Jaye Weatherburn, **Preserving Digital Materials**, 3. bs., Londra[Birleşik Krallık], Rowman & Littlefield, 2018, s. 123-124).

156 ISO, **14721 Open Archival Information System (OAIS)**, **a.g.e.**, s. 100

157 The National Electronic Commerce Coordinating Council, **Creating and Maintaining Proper Systems for Electronic Record Keeping**, 2002, s. 21, (Çevrimiçi) https :// www. ctg. albany. edu/publications/reports/proper_systems/proper_systems.pdf, 4 Mart 2020.

geliştirilmiştir[158]. Bu tasdik işlemi, insan müdahalesine gerek duyulmadan otonom bir şekilde gerçekleşmelidir. Log kayıtları ise belgenin yaşam döngüsünde geçirdiği aşamaların dokümantasyonu olarak kullanılabilir[159].

Burada aynı zamanda üstverilerden de yararlanılmaktadır. "İşlemin kim tarafından gerçekleştiği, gerçekleşme tarihi, ortam yenilemesi öncesinde ve sonrasındaki döngüsel artıklık denetimi ve özet değerlerinin karşılaştırılması" gibi üstverilerin oluşturulabileceği ifade edilmektedir. Bununla birlikte, log kayıtlarında teknolojik göç işlemlerinde karşılaşılan sorunların da yer alması önerilmektedir. Böylece, sürecin benimsenen prosedürler dâhilinde yürütülüp yürütülmediği incelenebilir ve kalite kontrolü yapılabilir[160].

2.3.3. E-Belgelerin Sürdürülebilirlik Riskleri

Örgütlerde arşivlenen e-belgelerin güvenilirliğini tehdit eden faktörlerden biri uzun dönemde sürdürülebilirliğe ilişkin faktörlerin belirsizliğidir. Bu belirsizliklerin giderilip, arşiv döneminin sağlıklı yönetilebilmesi için sürdürülebilirlik stratejilerine ihtiyaç vardır. Bu stratejiler arasından belgelerin zaman içerisinde kullanılabilir kalmasını sağlama yeteneği olarak ifade edilen[161] sayısal süreklilik anlayışı öne çıkmaktadır. Sayısal sürekliliği diğer bir ifadeyle sürdürülebilirliği tehdit edebilecek riskler, formatın endüstri standardında olmaması ve kullanılan EBYS'lerin gerektiğinde güncellenmemesi şeklindedir.

Bu olumsuz durum, bir organizasyonun varlığını sürdürebilme yeteneği olarak tanımlanabilecek kurumsal kapasite geliştirmeyle[162] de ilgilidir. Kapasite geliştirme, örgütlerin fonksiyonlarını gerçekleştirmeyi sağlayacak sermaye, ham madde, insan kaynağı ve bilgi varlıklarını düzenleme, geliştirme ve yönetme yeteneği olarak tanımlanmaktadır[163].

---

158 Luciana Duranti, "Concepts and Principles for the Management of Electronic Records, or Records Management Theory is Archival Diplomatics", **Records Management Journal**, C. 20, No: 1, 2010, s. 82.

159 **a.g.e.**, s. 83.

160 ISO, **18492 Long-term Preservation of Electronic Document-based Information**, **a.g.e.**, s. 9-12.

161 Lale Özdemir ve Emine Cengiz, "Türk Kamu Sektöründe Dijital Süreklilik Ne Kadar Mevcut: Teorik Bir Çerçeve", **Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ**, ed.: Bahattin Yalçınkaya vd., Ankara, Ankara Üniversitesi, 2019. ; TNA, **Risk Assessment Handbook**, 2017, s. 7-9, 20, (Çevrimiçi) https :// www. nationalarchives. gov.uk/documents/information-management/risk-assessment-handbook.pdf, 6 Mart 2020.

162 Belgin Uçar Kocaoğlu, "Kamu Kurumlarında Yönetsel Kapasitenin Güçlendirilmesi", **Sayıştay Dergisi**, No: 114, 2019, s. 119.

163 Ali Şahin ve Adnan Söylemez, "Yerel Yönetimlerde Kurumsal Kapasitenin Ölçülmesi (Konya Örneği)", **ASSAM Uluslararası Hakemli Dergi 13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı**, 2019.

Organizasyonlarda belgelerin sürdürülebilirliğini sağlamak için kapasite değerlendirme sistemleri geliştirilmiştir. Burada, yasal düzenlemeler, kurumun fonksiyonları, mevcut bilgi teknolojileri ve insan kaynağı analiz edilerek belge yönetiminin üretim, tasnif, erişim ve uzun dönemli koruma gibi süreç adımlarında kullanılır[164].

Kapasite geliştirme, bu süreçlerle ilgili iyileştirmeleri sağlarken birtakım riskleri de beraberinde getirir. Süreçlerle alakalı yönergelerin belirlenmemesi ve nitelikli personelin istihdam edilmemesi öne çıkan riskler arasındadır. Yönergelerin eksikliği, hangi durumda ne yapılacağı konusunda doğru karar vermeyi güçleştirir[165]. Kararsızlık ise yasal ve idari gereksinimlerin sağlanamamasına, hesap verilebilecek denetim mekanizmasının oluşmamasına, hedeflerin gerçekleştirilip gerçekleştirilmediğini denetleyecek raporlamaların yapılamamasına, tekrarlanan işler ayıklanmadığından kırtasiyeciliğin devam etmesine ve verimliliğin düşmesine sebep olur[166]. Bu eksiklik, kurum düzeyinde belirtilen aksaklıklara sebep olurken, belge yönetimi düzeyinde ise belgelerin nasıl üretilip paylaşılacağı, nerede saklanacağı, nasıl organize edilip tanımlanacağı, tasfiye edileceği ve erişileceği hususunda çalışanların cevap bulmasını zorlaştırır[167].

Belge yönetimindeki ilk kurumsal kapasite geliştirme programının örneklerinden birinin çeşitli arşivcilik derneklerinde başkanlık yapmış Anne Thurston tarafından hazırlandığı görülmektedir. Burada yeteri kadar bilgi ve belge uzmanının istihdam edilmemesi bir diğer kurumsal kapasite geliştirememe riski olarak kabul edilmektedir. Thurston, karar vericilerin arşivciler ve belge yöneticilerinin değil bilgi teknolojilerinin sorunları çözeceğine inandığını dile getirmektedir. Bunun sonucunda kurumsal kapasite

---

164 International Records Management Trust [IRMT], **Records Management Capacity Assesment System: User Guide**, Version 1.4., 2005, s. 6, (Çevrimiçi) https:// www. nationalarchives. gov. uk/rmcas/documentation/rmcas_user_guide.pdf, 26 Mayıs 2020. ; Özgür Külcü ve Hande Külcü, "The Records Management Capacity Assessment System (RMCAS) as a Tool for Program Development at the Turkish Red Crescent Society", **International Journal of Information Management**, C. 29, No: 6, 2009, s. 485.

165 Naomi Hay-Gibson, "Risk and Records Management: Investigating Risk and Risk Management in the Context of Records and Information Management in the Electronic Environment", Yayınlanmamış Doktora Tezi, Northumbria University, Newcastle[Birleşik Krallık], 2011, s. 27.

166 Judith Ellis, "Embedding Records Management in the Business", **Managing Records Risks in Global Financial Institutions, Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra[Birleşik Krallık], Facet Publishing, 2011, s. 203.

167 Kofi Koranteng Adu ve Patrick Ngulube, "Key Threats and Challenges to the Preservation of Digital Records of Public Institutions in Ghana", **Information, Communication &Society**, C. 20, No: 8, 2016, s. 10-11. ; Noriyuki Takayama, "On Fifty Million Floating Pension Records in Japan", **The Geneva Papers on Risk and Insurance - Issues and Practice**, C. 34, No: 4, 2009, s. 632.

geliştirmede belge yönetimi merkezli değil, teknoloji odaklı bir yaklaşımın benimsendiğini ifade etmektedir[168]. Bundan dolayı, tanımlama, tasnif, transfer ve özgünlüğün korunması gibi belge yönetimi süreçleri başarıyla gerçekleşemeyebilir.

Benzer bir şekilde, Danimarka Kraliyet Kütüphanesinin sayısal koruma uzmanlarından Eld Zierau, her ne kadar belgenin bit yapısını korumak, replikaların birbirinden bağımsız olarak saklanması ve bütünlüğün düzenli aralıklarla kontrol edilmesi gibi işlemlerin daha çok bilgisayar mühendislerinin çalışma alanına girdiğini ifade etse de belgeler ne kadar süre ile saklanacak, arşivde nasıl muhafaza edilecek gibi hususların kararlaştırılması için arşivcilik ve belge yönetimi eğitimi almış uzmanların istihdamına ihtiyaç duyulduğunu dile getirmektedir[169]. Hâliyle bu uzman eksikliği, sürdürülebilirliği etkileyecek sorunlara neden olabilir. Mesela, İskoçya Milli Arşivinin Koruma ve Bilgi Yönetimi Müdürü Tim Gollins, bilgisayar mühendislerinin %10'luk bir veri kaybını kabul edilebilir gördüklerini ifade etmektedir[170]. Fakat, belge yönetiminde herhangi bir veri kaybı telafi edilemez sonuçlara yol açmaktadır. Durum böyle olunca, arşivcilik ve belge yönetimi bakış açısıyla mühendislik yaklaşımının birlikte değerlendirilmesi gerekmektedir. Belgelerin korunmasında hangi kuralların uygulanacağı ortak akılla belirlenmelidir.

İngiliz Milli Arşivinin sayısal süreklilikle ilgili çıkardığı rehberlerde risklerin, belgelerin okunup erişilememesi, fonksiyon analizinin layıkıyla yapılamaması ve kontekstin açığa çıkarılamaması gibi sonuçlara sebep olabileceği açıklanmaktadır[171]. Bu sorunlar, belgelerin tamlık ve özgünlüğüne zarar verebileceğinden güvenilirliklerini tehdit eden unsurlar olarak kabul edilmektedir[172]. Bundan dolayı, risk analizi yapılıp, önlemlerin belirlenmesi güvenilirliğin korunmasına yardımcı olabilir[173].

---

168 Thurston, "Digitization and Preservation: Global Opportunities and Cultural Challenges", **a.g.e.**, s. 32.

169 Eld Zierau, "The Rescue of Danish Bits: A Case Study of the Rescue of Bits and How the Digital Preservation Community Supported it", **15. International Conference on Digital Preservation**, 24-27 Eylül 2018, ed.: Megan Potterbusch vd., Boston[ABD], yayımcı yok, 2018, (Çevrimiçi) https://osf.io/2eazn/, 1 Ocak 2020.

170 Tim Gollins, **Twitter**, 3 Temmuz 2018, (Çevrimiçi) https:// twitter. com/ timgollins/ status/ 1014084416526802944?s=21, 6 Mart 2020.

171 TNA, **Understanding Digital Contunity**, **a.g.e.**, s. 6. ; TNA, **Managing Digital Contunity**, **a.g.e.**, s. 10-11.

172 TNA, **Migrating Information between Records Management Systems**, **a.g.e.**, s. 18. ; TNA, **Risk Assessment Handbook**, **a.g.e.**, s. 20.; ISO, **27050-2**: **Electronic Discovery, Part 2: Guidance for Governance and Management of Electronic Discovery**, Cenevre[İsviçre], ISO, 2018, s. 7.

173 Victoria L. Lemieux ve Ember D. Krumwied, "Managing Records Risks in Global Financial Institutions", **Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra[Birleşik Krallık], Facet Publishing, 2011, s. 93-94.

ÜÇÜNCÜ BÖLÜM
E-BELGELERİN GÜVENİLİRLİĞİNİN KORUNMASI YÖNTEMLERİ

3.1. Belge Yönetimi ve Arşivcilikte Güvenilirlik Yöntemleri

3.1.1. Gereksinimler

3.1.1.1. Belge Yönetimi Fonksiyonları

Belgelerin özgünlük, gerçeklik ve tamlık niteliklerine sahip olması olarak ifade edilen güvenilirlik, hem güncel dönemde hem de arşive devredildiğinde korunmalıdır[1]. Ancak, belge ve arşiv yönetimi sürecinde uygulama adımları aynı olmadığından birkaç çalışmada bu iki alan için güvenilirlik gereksinimlerinin birbirinden farklı olduğu belirtilmiştir[2]. Güncel dönemdeki gereksinimler, hangi dokümanların belgeye dönüşeceği, kimlerin belge düzenleme ve erişme yetkisine sahip olacağı, belgelerin sistemde ne kadar kalacağı ve nasıl tasfiye edileceği gibi hususlarla ilgili kuralları içerir. Arşiv yönetimi güvenilirlik gereksinimlerinde ise belgelerin hangi kurallar ışığında arşive devredileceği, güvenilirliklerinin ne şekilde korunacağı ve süreçlerin işletilme biçimini gösteren log kayıtları gibi dokümantasyonun nasıl yapılacağı açıklanır[3].

Örgütlerde belgeler oluşturulurken sorumlu, düzenleyen, kişi/tüzel kişi, arşivsel bağ, hukuki sonuca yönlenebilecek bir içeriğe sahip olmak ve düzenlenme tarihi, idari ve hukuki açıdan belgenin karakteristiği olarak ortaya çıkarken, bu hususiyetler aynı zamanda güvenilirlik gereksinimleri olarak da değerlendirilebilir. Başka bir deyişle hukukun bir belgede delil değeri olarak belirlediği bu özellikler, güvenilirlik unsurları olarak kabul edilebilir. Bazı saha uzmanlarına göre belirtilen bu unsurlar, belgenin tanımlanması ve bütünlüğüyle ilişkilidir[4]. Mesela, belgedeki kişiler, konu, belgenin kuruma geliş veya üretim tarihi, arşive devredilme tarihi ile arşivsel bağ ve ekler gibi belgenin tanımlanmasıyla ilgili hususlar bu özellikleri tamamlayan

---

1 Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**

2 Heather MacNeil, belgelerin güncel kullanım dönemindeki güvenilirlik gereksinimlerini "benchmark requirements"; arşiv safhasındakileri ise "baseline requirements" olarak ifade etmektedir (MacNeil vd., "Requirements for Assessing and Maintaning the Authenticity of Electronic Records", **a.g.e.**, s. 3).

3 **a.e.**

4 Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice**", a.g.e.** ; Luciana Duranti, "Diplomatics: New Uses for an Old Science", **Archivaria**, No: 28, 1989, s. 11.

parçalardır. Tanımlama bunlardan oluşurken bütünlük, belgenin türüne göre sahip olması gereken öznitelikleri barındırması ve bunların da zaman içerisinde değişmemesi anlamına gelmektedir. Bütünlük kritik edilirken belgedeki süreli olma ibaresi (günlüdür, acele), havale şerhi, düzeltme notu vb. açıklamalar ile zaman damgasının güncellenmesi ya da formatın yenilenmesi gibi teknolojik değişiklikler kayıt altına alınır[5].

Belirtilen bu hususiyetler, güvenilirlik gereksinimi olarak birinci aşamayı oluştururken, belge yönetiminde ikinci aşama erişim seviyelerinin belirlenmesidir. Erişim seviyeleri, kurumun yetkili organları tarafından görev tanımları yapılıp imza yetkileri yönergesi gibi prosedürlerle yetki ve sorumluluklara göre tayin edilir. Önceden belirlenmiş bu yetki ve sorumluluklara göre de belge yöneticisi, kimlerin hangi belgeleri hazırlayacağını ve kimlerin imzalayacağını, aynı zamanda işlem safhasında gerektiğinde havala şerhi ya da açıklama notunu kimlerin yazabileceğini EBYS'de yapılandırır. Bu erişim seviyeleri kullanıcı profillerine göre gruplandırılır. Mesela, bir profildeki kullanıcı sadece belgeyi görüntüleyebiliyorken, diğer profildekiler cevap hazırlama yani yeni bir belge düzenleme yetkisine de sahiptir. Tüm bu yetkiler ve işleyiş süreçleri EBYS'de log kaydı olarak tutulur. Erişim seviyelerinin sağlıklı çalışıp çalışmadığını denetlemek için bu log kayıtlarından yararlanılır[6].

Üçüncü aşamada belgelerin kaybolması ve bozulmasını önleyici prosedürler hazırlanır. Bunlar, belgelerin öznitelikleri korunarak düzenli yedeklemelerin yapılması, sistem yedeklerinin muhafaza edilmesi, düzenli yapılan yedeklemelerle son yedeklemeden bu yana yaşanan değişikliklerin saklanması gibi adımlardır[7].

Dördüncü aşamada belgelerin bulunduğu ortam ve kullanılan teknoloji ile ilgili prosedürler geliştirilir. Teknoloji yenilemelerini planlama, uygulama yazımı değiştirildiğinde belgeleri bulup getirme (retrieve), onlara erişme ve kullanabilme ile belgelerin taşıyıcı ortamını yenileme gibi teknolojik göç işlemlerinde yapılacaklar bu aşamada değerlendirilir[8].

---

5 MacNeil vd., "Requirements for Assessing and Maintaning the Authenticity of Electronic Records, **a.g.e.**, s. 5-7.

6 **a.e.**

7 **a.e.**

8 **a.e.**

Beşinci aşamada dokümanter form tanzim edilir. Diğer bir ifadeyle birinci aşamada belirlenen form özelliklerine göre belge şablonları oluşturulur. Yasal ve idari prosedürlerle ilişki kurularak belge türüne özgü dokümanter form hazırlanır. Fonksiyonlara göre iş akışı sürecinde belge oluşturan idari işlemlerde belge türü belirlenir. Türün belirlenmesi, belge formunun açıklanması demektir. Dolayısıyla bir iş sürecinde belge türü belirlenerek onu ortaya çıkaran işlem ile türe özel form hususiyetleri ilişkilendirilmiş ve tanımlanmış olur[9].

Türe özgü dokümanter formun oluşmasına dikkat edilerek tanzim edilen belgeler, idari işlemlerde kullanılmaya hazır hâle gelir. Bunlar, kurumsal iş ve işlem süreçlerini yansıtır. İşlemi biten belgeler, fonksiyonlarına göre dosya planları ışığında tasnif edilir. Bundan dolayı bir fonksiyon kapsamında ortaya çıkan iş (konu/vaka) bağlamında oluşan belgeler, aralarındaki organik bağa göre bir araya getirilir. Böylece işten kaynaklanan organik bağdan dolayı dosyada bütünlük sağlanır. Belgeleri aralarındaki organik bağa göre bir araya getirme işlemi, dosyalama olarak bilinmektedir[10]. Dosyadaki belgeler değerlendirilerek yürütülen işlemler anlaşılır. Bu yapılarak işlem adımları görülür. Neticede işe ait işlemlerin tamamlandığı anlaşılabilirken yapılmayan ya da atlanan bir işlem varsa o da açığa çıkarılır. Böylece, kurumda oluşan belgeler, dosya planı ışığında ait oldukları işe göre dosyalanırken aynı zamanda fonksiyona ilişkin işlemler de dosyalanmış olur.

Dosya planları ve dosyalama kadar belge yönetiminin temel fonksiyonlarından biri de saklama planlarıdır. Belgelerin saklama süresi, yasal, idari ve kültürel ihtiyaçlara göre değişiklik gösterebilmektedir. Bir belge türünün yasal prosedürler gereği oluşturulduğu birimde saklama süresi on yıl olabilirken, başka bir türün saklama süresi beş yıldır. Bu saklama süreleri daha belgeler oluşmadan tayin edilir. Böylece, yasal ve idari açıdan bir değişiklik olmadıkça bir belgenin ne kadar süre ile saklanacağı bellidir. Bu süre bittikten sonra belgenin tasfiye süreci başlar, arşive devredilip devredilmeyeceği kararlaştırılır.

Altıncı aşamada, arşive devredilme kararı verilmeden önce belgelerin güncel dönemdeki özniteliklerini koruyup korumadığı, dolayısıyla güvenilir olup olmadığı

---

9 **a.e.**

10 Çiçek**, Kurumsal Bilgi Yönetimi, a.g.e.**

değerlendirilir. Başka bir deyişle uygunluk kontrolünden geçirilir. Özniteliklerini koruduğu kanaati oluşunca da güvenilirliği onaylanır. Böylece, belge arşive devredilmeye hazır hâle gelir. Burada, tasfiye olarak adlandırılan belgelerin arşive devrine karar verildiği dönemde arşivcileri (ayıklama-imha komisyonu) bekleyen bir konu, belgeler güvenilirliğini devam ettiriyor mu sorusuna cevap vermektir. Henüz Türkiye'de e-belgelerin tasfiyesiyle alakalı örnek uygulamalar görülmediğinden bunun nasıl gerçekleşeceği çok netleşmese de bazı saha uzmanlarının birtakım öneriler getirdiği görülmektedir. Bu önerilerden biri arşiv malzemesi olduğuna karar verilen e-belgelerin güvenilir olup olmadığı değerlendirmesi yapılıp, hâlâ güvenilirliğini korudukları kanaati oluşunca da birtakım elektronik onay araçlarıyla bunu tasdik etmek şeklindedir. Bu işlemin e-imzalı belgelerde e-mühür gibi araçlarla gerçekleştirilebileceği değerlendirilmektedir[11].

E-belgelerin bit yapısının olduğu gibi muhafazası yerine belgedeki kişiler, faaliyet, kontekst, arşivsel bağ ve içerik gibi bileşenler korunup yeniden tanzim edilerek delil değerini hâlâ muhafaza eden ve hukukun kabul ettiği belgeler oluşturulur[12]. Yedekleme, teknolojik göç gibi işlemler nedeniyle birden fazla nüsha bulunabilir. Bundan dolayı belge yönetimi güvenilirlik gereksinimlerinin yedinci aşamasında, daha önceden belirlenen prosedürler ışığında hangi nüshanın delil olarak değerlendirileceği kararlaştırılır[13]. Değerlendirme kriterlerinin açıklandığı bu prosedürler, aynı zamanda log kaydı gibi dokümantasyonların zorunluluk olduğunu göstermektedir.

Sekizinci ve son aşama belgelerin dokümantasyonlarıyla birlikte arşive devredilmesidir. Çünkü belgeler tek başlarına değil güncel kullanımında gördüğü işlemleri de gösteren log kaydı ve denetim günlükleri gibi dokümantasyonlarla arşive transfer edilir[14]. Belge yönetimi süreklilik modeli gibi yaklaşımlarda (records continuum) belgelerin delil değeri özelliğinin güncel dönem ile arşiv sürecinde de devam etmesinden dolayı bu safhaların birbirinden kesin çizgilerle ayrılamayacağı

---

11 MacNeil vd., "Requirements for Assessing and Maintaning the Authenticity of Electronic Records, **a.g.e.**, s. 5-7.

12 Duranti, "Structural and Formal Analysis: The Contribution of Diplomatics to Archival Appraisal in the Digital Environment", **a.g.e.**, s. 80.

13 MacNeil vd., "Requirements for Assessing and Maintaning the Authenticity of Electronic Records, **a.g.e.**, s. 5-7.

14 **a.e.**

değerlendirilmektedir[15]. Ancak, bu safhalardaki uygulama adımları farklılık içerdiğinden güvenilirlik gereksinimlerinin ayrı olarak kurgulanması gerekliliği ortaya çıkmıştır. Durum böyle olunca, belge yönetimi güvenilirlik gereksinimlerinden sonra arşiv yönetimindeki gereksinimler gündeme gelmektedir.

3.1.1.2. Arşivcilik Uygulamaları

Kâğıt belgeler, arşive intikal ettiğinde onu üreten kurum ya da üretilmesine sebep olan hukuk kurallarının güvenilirliği gibi nedenlerle sahih kabul edilir. Arşivdeki varlığı süresince de belgelerin güvenilirliğine halel gelmediği düşünülür. Bundan dolayı, arşivcilerin, kâğıt belgelerin güvenilirliğini kontrol gibi etmek bir sorumluluğu olmamıştır. Mesela, bir araştırmacı, arşivcilerden bir belgenin güvenilir olduğunu göstermelerini istese bu talep, görevlerinin bir parçası olmaması nedeniyle kabul edilmeyebilir. Aynı zamanda geleneksel olarak bir belgenin güvenilirliğini sorgulamak daha çok araştırmacının yaptığı bir uygulamadır. Arşivcilerin belgelerin güvenilir olduğunun gösterilmesine yardımcı olabilecek belgeyi ait olduğu kontekste göre tanımlamak ve belgenin üreticisiyle olan ilişkisini göstermek gibi faaliyetleri söz konusudur[16].

Ancak, elektronik ortamda yaşanan hızlı teknolojik değişimler, kullanılan taşıyıcı ortamların kırılganlığı, e-imza ve zaman damgası sertifikalarının yenilenmesi gibi durumlar e-belgelerin arşive devredildikten sonra da güvenilirliğinin devam ettirilmesini gerektirir. Bu durum, aslında belgenin güncel dönemdeki özniteliklerinin korunmasıdır. Dolayısıyla özniteliklerin muhafazası, güvenilirliğin güncel dönemde olduğu gibi korunduğunu ifade eder.

Bu öznitelikler, arşivcilik uygulamalarındaki temel süreçler olan muhafaza, reprodüksiyon ve tanımlamayı kapsar. Bundan dolayı, üç aşamadan oluşan arşiv yönetimi güvenilirlik gereksinimleri hazırlanmıştır. Bunlar, belgelerin muhafazasına ilişkin kuralları belirlemek, reprodüksiyon sürecinin dokümantasyonunu oluşturmak ve üstverilerin bütünlük içerisinde arşivsel tanımlamada kullanılmasını sağlamaktır[17].

---

15 Frank Upward vd., **Recordkeeping Informatics for a Networked Age**, Victoria[Avustralya], Monash University Publishing, 2018, s. 192.

16 Duranti, "Structural and Formal Analysis: The Contribution of Diplomatics to Archival Appraisal in the Digital Environment", **a.g.e.**, s. 78-79.

17 MacNeil vd., "Requirements for Assessing and Maintaning the Authenticity of Electronic Records, **a.g.e.**, s. 7-11.

Birinci aşamada arşive transfer ve arşivdeki uygulamalar sırasında aidiyet zincirinin korunması ve belge hiyerarşisinin kopmadan muhafazasına ilişkin kurallar belirlenir. Bu aşamada arşivciler, erişim seviyelerinin tayin edilmesi, belgelerin bozulmaması ve aidiyet zincirinin kopmaması için belirlenen prosedürleri uygular. Her ne kadar, belge yönetiminde arşive devredilecek malzemeler belirlenirken aidiyet zincirinin korunup korunmadığı değerlendirilse de belge arşive devredildikten sonra bu değerlendirme tekrar gözden geçirilir. Aidiyet zincirinin kopmadığı, belge hiyerarşisinin muhafaza edildiği teyit edilir. Transfer süreci gözden geçirilip, arşiv uygulamaları başladıktan sonra belgenin içeriğinin, kontekstinin ve form elemanlarının zaman içerisinde korunmasına yönelik önlemler alınır. Örneğin bu önlemlerden biri teknolojik güncellemelerden dolayı formatın değiştirilmesidir. Ancak, bu gibi uygulamalar gerçekleştirilirken özniteliklerin korunduğu gösterilmeli, güvenilirlik de onaylanmalıdır. Durum böyle olunca, güvenilirliğin nasıl ve hangi araçlarla onaylanacağı önceden açıklanmalıdır.

İkinci aşamada var olan belgelerin bileşenleri olduğu gibi korunarak ikinci ya da daha fazla nüsha üretmek anlamına gelen reprodüksiyon oluşturma sürecinin dokümantasyonu hazırlanır. Burada teknolojinin gelişmesi, taşıyıcı ortamın değişmesi gibi nedenlerle bileşenleri korunmuş bir şekilde arşive devredilen belgeye dayanarak hukukun belge olarak kabul ettiği niteliklere sahip ikinci bir nüsha düzenlenir. Ancak, format değişikliğinden dolayı ilk nüsha kullanılmaz. Hâliyle bu ikinci nüsha esas belge yerine geçer. Bu sebeple reprodüksiyon oluşturma tarihi, bu işlemden sorumlu kişi ve arşive devredilen belgelerle oluşturulan reprodüksiyonlar arasındaki ilişki kayıt altına alınır. Eğer oluşturulan reprodüksiyonun form özellikleri, içeriği ya da kullanılabilirliği etkileyecek bir unsuru bileşenleri korunan belgeden farklılık arz ediyorsa bu bilgi de kaydedilmelidir. Bu süreçlerin dokümantasyonu son kullanıcının erişimine açılacağı bilinciyle hazırlanmalıdır.

Arşive devredilen belgelerin aidiyet zincirinin korunması ve reprodüksiyon işlemlerinin dokümantasyonu hazırlandıktan sonra arşiv yönetimi güvenilirlik gereksinimlerinin üçüncüsü olan tanımlama aşamasına geçilir. Arşivsel tanımlama, bir fondaki tüm belgelerin konteksti ve teknolojik geçmişiyle birlikte kapsam ve içeriğinin

açıklanması olarak ifade edilmektedir[18]. Burada, kontekst açığa çıkarılarak belge arşive devredildikten sonra gerçekleşen değişimlerle ilgili bilgiler sunulur.

Geleneksel tanımlamada belgelerin konteksti açığa çıkarılıp, aynı zamanda bunun zaman içerisinde değişmediği gösterilmektedir. Bugüne kadar kâğıt belgeler için değerlendirilen bu husus, e-belgelerin reprodüksiyonları oluşturulurken ilk format yapısındaki özniteliklerinin korunduğu ve yeni format kaynaklı değişiklikler olmuşsa da bunların kayıt altına alınarak belirlendiğinin gösterilmesiyle gerçekleştirilir. Hâliyle, tanımlama, belgenin reprodüksiyonları ve belgedeki değişimler gibi hususları içeren bilgilerin kaydedildiği yer olduğundan, güvenilirliğin değerlendirilmesinde oldukça kritik bilgiler sunar. Her ne kadar, tanımlamanın güncel yönetim safhası katılarak mı yoksa arşive devredildikten sonra mı yapılacağı tartışmaları[19] olsa da burada işlenen bilgilerin belgenin güvenilirliğinin onaylanmasında kullanılacağı gerçeği gözden uzak tutulmamalıdır[20].

3.1.2. Güvenilirlik Yöntemleri

Hukuk alanında, üniversitelerde ve ulusal/uluslararası araştırma merkezleri tarafından gerçekleştirilen projelerde e-belgelerin güvenilirliği konusunun ele alındığı görülmektedir. Bunlar içerisinde özellikle elektronik ortamdaki bilgi varlıklarının güvenilirlikleriyle ilgili projeler öne çıkmaktadır. Saha uygulamaları yapılıp, uygulanabilir vakaları değerlendirerek pratik sonuçlar ürettikleri düşünülen projeler, bu tezde kullanılan güvenilirlik analiz yönteminin geliştirilmesinde daha yönlendirici olmuştur.

---

18 Duranti, "Structural and Formal Analysis: The Contribution of Diplomatics to Archival Appraisal in the Digital Environment", **a.g.e.**, s. 78-79.

19 Bu tartışma, belgenin ait olduğu fonksiyon sonucunda üretildiğini gösterecek karinelerin ileri sürülmesi gerekliliğinden kaynaklanır. Bundan dolayı saha uzmanları, belgeler arşive devredildikten sonra yapılan tanımlamanın faaliyet ve fonksiyonları tam olarak yansıtamayabileceğini ileri sürmektedir (Millar, "An Obligation of Trust: Speculations on Accountability and Description", **a.g.e.**, s. 72). Tanımlamanın otonom araçlarla belge üretildiği gibi kurumsal faaliyetlerle ilişkilendirilerek başlatılması; bunun için üstverilerin kullanılması önerilmektedir (MacNeil, "Methods for Creating and Maintaning Reliable and Authentic Electronic Records", **a.g.e.**, s. 42). MacNeil'in bu önerisinden hareketle saha çalışmasında kurumlara tanımlama uygulamalarıyla ilgili sorular sorulmuştur. Ancak, tanımlamanın e-imzalı belgelerin güvenilirliğinin başarıyla korunmasında nasıl kullanılabileceğini incelemek belirli bir sürede bitirilmesi gereken bu tezin kapsamı dışında tutulmuştur. Bu incelemenin müstakil bir çalışmada ele alınmasının daha sağlıklı olacağı değerlendirilmektedir.

20 MacNeil vd., "Requirements for Assessing and Maintaning the Authenticity of Electronic Records, **a.g.e.**, s. 7-11.

INTERPARES, ERPANET, CASPAR, PLANETS ve APARSEN gibi araştırma projelerinin tamamlanıp sonuçlarının kamuoyuyla paylaşıldığı bilinmektedir. INTERPARES'in dışında adı geçen bu projeler, daha çok elektronik ortamdaki kültürel ve bilimsel mirasın korunması ve devamlılığı üzerinedir. INTERPARES ise özellikle arşivlenen e-belgelerin özniteliklerinin korunarak güvenilirliklerinin sağlanması konusuyla ilgilenmektedir. 20 yıldan fazla süredir çalışmalarını devam ettirmesi ve bu bağlamda 4. safhayı bitirmesiyle dikkat çekmektedir. Yaklaşık 28 ülkenin katkı sağladığı projenin bu uluslararası görünürlüğü ve yaygın etkisi, dünyanın pek çok yerinden ve farklı disiplinlerden üyelerinin bulunmasıyla ilişkilendirilmektedir[21]. Bu projenin yaygın etkisinden dolayı diğerlerine göre öne çıktığı görülmektedir.

Proje'de hem güncel hem de arşive devredilen belgelerin güvenilirliğinin korunma yöntemleri incelenmiştir. Proje sonucunda, üretilmesinden arşiv belgesi olana kadar geçen süreçte ve arşivlenen e-belgelerin teknolojik göç ettirilmesinde güvenilirliğin nasıl korunabileceği açıklanmıştır. Aynı zamanda bu süreçlerde kullanılan teknolojik yaklaşımların belgelerin güvenilirliğine zarar vermediğinin nasıl ortaya konacağı belirlenmeye çalışılmıştır. Tüm bunlar belge yönetimi, arşivcilik, hukuk, bilgisayar ve işletme mühendisliği gibi farklı disiplinlerin katılımıyla değerlendirilmiştir[22].

Projeden elde edilen bu sonuçlar neticesinde e-belgelerin güvenilirliğinin korunmasında modern diplomatik yöntemlerden faydalanılabileceği anlaşılmıştır. Modern diplomatik, e-belgelerin özgünlüğünü değerlendirebilmek için bir analiz metodu ortaya koymaktadır. Başka bir deyişle modern diplomatik, bilgi teknolojisi yeni taşıyıcı ürünlerin vasıflarını göz önünde bulundurarak çağdaş bir yorum geliştirmiştir. E-belgelerin sahip olması gereken hususiyetleri barındıran bu çağdaş yorumda, belge yönetimi ve arşivciliğin aynı zamanda geleneksel diplomatik inceleme usulünün kriterleri bulunmaktadır. Burada belgenin oluşumuna kaynaklık eden

---

21 Maria Guercio, "Digital Preservation in Europe: Strategic Plans, Research Outputs and Future Implementation. The Weak Role of the Archival Institutions", **The Memory of the World in the Digital Age: Digitization and Preservation. An International Conference on Permanent Access to Digital Documentary Heritage**, 26-28 Eylül 2012, ed.: Luciana Duranti ve Elizabeth Shaffer, Vancouver[Kanada], UNESCO,2013, s. 468.

22 Luciana Duranti, "Introduction", **The Long-term Preservation of Authentic Electronic Records: Findings of the International Research on Permanent Authentic Electronic Records [INTERPARES] Project**, (Çevrimiçi) http:// www. interpares. org/ book/ interpares_book_c_intro.pdf, 28 Aralık 2020.

bürokratik işlemleri şekillendiren yasal ve idari prosedürler güvenilirlikle ilişkilendirilir. Bunu yapmak için yazılım ve donanımda kullanılan bilgi teknolojileri ile diplomatik, belge yönetimi ve arşivcilik uygulamaları kullanılır. Böylece e-belgelerin hem güncel kullanım safhasında hem de arşive devredildikten sonra güvenilir olduklarını destekleyecek karineler açığa çıkarılır[23].

Bu projelerin yanı sıra bazı araştırmacıların konu hakkında incelemeler yaptığı gözlenmektedir. British Columbia Üniversitesinde Corinne Rogers tarafından hazırlanan doktora tezi benimsenen yöntemi açısından dikkat çekmektedir[24]. Rogers, e-belgelerin özgünlüğünü sosyal ve teknolojik göstergeler başlığı altında incelemiştir. Sosyal göstergeler, temel arşiv ve belge yönetimi uygulamalarından olan politikalar, tasnif şeması ve dosya planı, saklama ve imha süreleri, arşivsel tanımlama ile niteleyici üstverileri içermektedir. Bunlar, belgelerin üretimi, yönetimi ve korunması amacıyla kurumlar tarafından geliştirilerek belge yöneticileri ve arşivciler aracılığıyla uygulanır. Teknolojik göstergeler ise belge yönetim sistemlerinin teknolojik bileşenleri kullanılarak oluşturulan sistemsel üstveriler, log kayıtları, e-imza doğrulama teknikleri, erişim kontrolleri ve güvenlik önlemleri ile teknik dokümantasyonu içerir[25]. INTERPARES'de geliştirilen diplomatik analiz yöntemiyle benzerlik gösterdiği düşünülen Rogers'in bu sosyal ve teknolojik göstergeler tasnifinden arşivlenen e-imzalı belgelerin güvenilirliğinin incelenmesinde yararlanılabileceği düşünülmüştür.

Çeşitli bilimsel çalışmalarda belgelerde özgünlük anlayışının sosyal, ekonomik ve felsefi arka planı olduğu düşünülerek daha geniş perspektiften konuya yaklaşıldığı bilinmektedir. Bu yüzden özgünlüğü anlamak için tek bir çözüm yerine farklı bakış açılarını değerlendirmek gerektiği ortaya konulmuştur[26]. Bu anlayış, sosyal sistem içerisinde pozitif hukuk ve teknolojinin verileri ışığında bir değerlendirme olarak öne çıkmaktadır.

---

23 MacNeil vd., "Authenticity Task Force Report", **a.g.e.**, s. 1.

24 Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice**", a.g.e.**

25 Corinne Rogers, "Authenticity of Digital Records in Practice", **2015 Digital Heritage Conference**, 28 Eylül-2 Ekim 2015, ed.: Gabriele Guidi vd., Granada[İspanya], IEEE, 2015, s. 396.

26 David Bearman ve Jennifer Trant, "Authenticity of Digital Resources: Towards a Statement of Requirements in the Research Process", **D-Lib Magazine**, 1998, (Çevrimiçi) http :// www. dlib. org/ dlib/june98/06bearman.html, 31 Mayıs 2020. ; Clifford Lynch, **Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust**, Alexandria[ABD], CLIR, 2000, (Çevrimiçi) https :// www. clir. org/ pubs/ reports/ pub92/ lynch/, 31 Mayıs 2020.

Ancak, bu tez kapsamında e-imzalı belgelerin güvenilirliği arşiv boyutuyla ele alındığı için belirtilen sosyal alanları kapsayan geniş bir perspektif yerine belge yönetimi ve arşivcilik dinamikleriyle sınırlı kalınmıştır. Belgelerin özgünlük ve güvenilirliği, teknolojik yöntemler yanı sıra arşivcilik metodolojilerinden biri olan arşivsel bağ odaklı olarak incelenmiştir. E-imzalı belgelerin güvenilirliğini korumada benimsenebilecek arşivcilik kaynaklı yöntemler arşivsel bağ başlığı, teknoloji kaynaklı yaklaşımlar ise teknolojik yöntemler başlığı altında değerlendirilmiştir. Arşivcilik kaynaklı olanlar daha çok tanımlama, üstveri, diplomatik analiz gibiyken teknolojik yöntemlerde bütünlük kontrolleri, log kayıtlarının analizi, e-imza kullanımı gibi sistemsel yaklaşımlar bulunmaktadır[27].

E-belgelerin güvenilirliğinin korunmasına yönelik çalışmalarda kritik unsurlarından arşivsel bağa ilişkin olarak dosyalama, diplomatik analiz ve üstverilerin ön plana çıktığı görülmektedir. Gelişen bilişim sistemlerinin ortaya koyduğu yöntemler ve sunduğu teknolojik imkânlar günümüzde blokzincir, yapay zekâ ve derin öğrenme olarak karşımıza çıkmaktadır. Bundan dolayı, tezde e-delil elde etme yöntemleri, blokzincir teknolojisi, yapay zekâ ile derin öğrenme yaklaşımları ele alınmaktadır.

3.2. Arşivsel Bağ

3.2.1. Dosyalama

3.2.1.1. Organik Bağ ve Belge Hiyerarşisi

Dosyalama, belgeleri ait oldukları iş bağlamında organik bağ kurarak bir araya getirmek olarak bilinmektedir. Elektronik belge yönetimi uygulamalarında dosyalamanın belge hiyerarşisi[28] kurularak yapılması yaygın bir görüştür. Ancak, kullanıcıların belgeyi keşfetme yetisini kısıtlayabileceği nedeniyle buna ihtiyaç duyulmadığı, belgelerin ait oldukları işle olan ilişkilerinin üstverilerle kurulabileceği

---

27 Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice**", a.g.e.**

28 Belge hiyerarşisinin (TSE, **13298 Elektronik Belge Yönetim Sistemi Standardı**, **a.g.e.**, s. 9), yabancı dildeki literatürde dosya dizini (folder structure) olarak da kullanıldığı bilinmektedir (European Archival Records and Knowledge Preservation [E-ARK - Avrupa Bilgi ve Belgelerinin Korunması], **Common Specification for Information Packages**, (Çevrimiçi) https :// earkcsis. dilcis. eu/, 24 Mart 2020). Türkiye Bilimler Akademisi Türkçe Bilim Terimleri Sözlüğü'nde ise folder, dosya dizini olarak ifade edilmektedir. "Bilgisayarda, belirli bir bellek ortamında bulunan dosyaların birbirleriyle ilişkisini, adlarını ve alt dizinlerin listesini saklayan ve örgütleyen veri yapısı; eşanlam: klasör" şeklinde tanımlanmıştır (TÜBA, **Türkçe Bilim Terimleri Sözlüğü**, **a.g.e.**, 24 Mart 2020).

görüşü de tartışılmaktadır. Belge hiyerarşisinin gerekli olduğunu savunanlar, aralarında organik bağ kurularak belgelerin konu ya da vakaya göre bir araya getirilebileceğini ileri sürmektedirler[29].

Belge hiyerarşisini açığa çıkarmak için kullanılan iki temel araçtan biri arşivsel bağ, diğeri organik bağdır. Organik bağ daha çok mikro düzeyde ilişkileri değerlendirip, belgeleri bir araya getirerek dosya oluşturma çabasıyken, arşivsel bağ makro düzeyde olup belgeden fona buradan da provenansa giden bir süreç izler. Bundan dolayı dosyanın belge hiyerarşisindeki yerine daha çok arşivsel bağ aracılığıyla işaret edilir. Arşivsel bağ, belgelerin kim tarafından, hangi idari işlem ve fonksiyon kapsamında üretildiğini, kime devredildiğini, nasıl dosyalandığını ve hangi seride bulunduğunu açıklayıp, bu seri içerisinde ait olduğu dosya ve dosyadaki diğer belgelerle ilişkisini kurabilmek şeklinde ifade edilmektedir[30]. Bu bağ, sadece belgenin üretildiği ve kullanıldığı kontekstle ilişkili olmayıp dosya, seri ve fon gibi onun ait olduğu arşiv kümesini de tanımlamaktadır. Bundan dolayı arşivsel bağı incelemeden bir belgenin güvenilirliğini analiz etmeye çalışmak yeteri kadar başarılı sonuçlar vermeyebilir.

Bu bağ değerlendirilirken bir işin faaliyetleri sonucunda oluşan belgelerle, bunların üreticisi, muhafaza edeni ve aralarındaki ilişki analiz edilir[31]. Durum böyle olunca, "aynı fonksiyon kapsamında üretilen farklı tür ve formattaki belgelerin bir konu ya da vaka bağlamında bir araya getirilmesi arşivsel bağın kurulmasında önemli bir adım olarak" kabul edilmektedir[32].

Arşivsel bağ kurulurken her belge ait olduğu fonksiyon kapsamında değerlendirilir. Birbiriyle ilişkili olan belgeleri ait oldukları işe göre bir araya getirip dosya oluşmasını sağlayan fonksiyon, aynı iş akışı sürecinde yürütülen farklı işlere ait benzer yapıdaki dosyaları toplayarak serinin meydana getirilmesine yardımcı olur.

---

29 E-ARK, **Common Specification for Information Packages**, **a.g.e.** ; Çiçek, "Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme", **a.g.e.** ; Victoria L. Lemieux, "Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework", **Future Technologies Conference**, 29-30 Aralık 2017, Vancouver[Kanada], The Science and Information Organization, 2017.

30 Çiçek, "Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme", **a.g.e.**, s. 98-99.

31 Lemieux, "Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework", **a.g.e.**, s. 44.

32 Çiçek ve Sağlık, "E-Belgelerin Arşivsel Bağının Elektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme", **a.g.e.** s. 262.

Hâliyle, arşivsel bağ, işlem, faaliyet, iş ve fonksiyona göre şekillenir. Bu durumda belgenin ilişkilendirildiği konu ya da vaka tamamlanana kadar organik bağ göz önünde bulundurulurken, tasfiye, arşive devir ve muhafaza adımlarından sonra belge arşiv malzemesi olduğu dönemde kontekstin tamamı açığa çıkarılacağından bu sefer arşivsel bağ kurma süreci işletilir[33].

Örgütlerde belgeler üretildikleri bağlama göre birbirleriyle ilişkilendirilerek bir araya getirilir. Bu işlem organik bağ kurma olarak adlandırılır. Bunun dosyalama ile sağlanabildiği bilinmektedir. Burada kullanılan en temel mekanik araç ise dosya kodunun verilmesidir[34]. Bu kod aracılığıyla belgelerin organik bağı kurulurken dosya bütünlüğüne yaptıkları katkı incelenir. Böylece, dosyadaki her belgenin diğer belgelerle bütünlük arz etmesi sağlanır[35]. Burada amaç, ister konu ister vaka olsun bir iş bağlamında birbiriyle ilişkili belgeleri bir araya getirmektir.

Belgeler arasında organik bağ kurmak, bir akıl yürütme faaliyetidir. Belgelerle üretildikleri bağlam arasında entelektüel bir ilişki olduğundan dosyalamanın fiziksel bir eylemin de ötesinde düşünsel bir boyutu vardır[36]. Bu ilişki organik bağın kurulmasıyla ortaya çıkarılır. İyi ve doğru dosyalamanın kaynağı olan organik bağ, belgenin kontekstinin anlaşılmasına da yardımcı olur. Bunun neticesinde belge ile üretildiği fonksiyon arasında ilişki kurularak arşivsel bağa giden fon, alt fon, seri ve dosya yolu tespit edilir.

Bir belgenin ait olduğu fonksiyon ortaya çıkarılamıyorsa organik bağın zarar gördüğü düşünülebilir. Bu durum, belgenin dosyadaki varlığının sorgulanmasına sebebiyet verirken; diğer taraftan antet, imzalayan, sayı gibi form özelliklerinin de problemli olabileceğini gündeme getirir. Dolayısıyla organik bağ kuran araçların kuşkulu olması, belgenin delil değeriyle alakalı şüpheler uyandırabilir[37].

Belgeler üzerinde entelektüel kontrol sağlamak olan dosyalama, vaka ve konuya göre oluşur. Bu oluşum sürecine dosyaya girecek olan belgelerin üretim,

---

33 Duranti, "The Concept of Electronic Record, Preservation of the Integrity of Electronic Records", **a.g.e.**, s. 11.

34 Çiçek, **Kurumsal Belge Yönetimi**, **a.g.e.**, s. 154-156.

35 Çiçek ve Sağlık, "E-Belgelerin Arşivsel Bağının Elektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme", **a.g.e.**, s. 263.

36 Çiçek, "Elektronik Belge Yönetimi Uygulamalarında Bir Alt Sistem Olarak Dosya Yönetimi", **a.g.e.**, s. 439.

37 Çiçek ve Sağlık, "E-Belgelerin Arşivsel Bağının Elektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme", **a.g.e.**, s. 263.

yönetim ve koruma süreçlerindeki kurallar etki eder[38]. Örneğin belgeye dosya kodu verilmesi bir form özelliği olup belgeyi tamamlayan unsurlardan biri olduğu kadar; aynı zamanda belgenin konusunu ifade ettiği için nasıl dosyalanmasını gerektiğini açıklar. Bu kodun verilmemesi ya da yanlış uygulanması belgenin dosyalama sürecinin hatalı başlamasına sebep olabilir. Hâliyle sadece dosyaya işaret eden bir form özelliği gibi gözüken dosya kodu meselesi, belgenin güvenilirlik unsurlarından olan tamlık ve gerçekliğe ilişkin fikir veren araçlardan biri olarak karşımıza çıkmaktadır. Aynı zamanda, dosya kodu ve dosyalama belgenin tanımlanmasıyla ilişkili olduğundan özgünlüğe de katkı yapar[39].

Ancak, organik bağın kurulmasında önemli bir aşama olan dosyalama yapılırken belge hiyerarşisinin kurulup kurulamadığı yönünde bir tartışma söz konusudur. Belge hiyerarşisinde, belgeler birim, seri, dosya, alt dosya, iş ve belge şeklinde hiyerarşik olarak tasnif edilir. Bu yapı, ağacın dallarına benzetildiğinden "ağaç yapısı" olarak da bilinir. Söz konusu yapının benimsenmemesi gerektiğini ifade eden diğer görüş ise bunun kullanıcı ihtiyaçlarını karşılamadığını dile getirmektedir. Bu görüşü savunanlar, belge hiyerarşisi kurulmadan, belgelere üstveriler aracılığıyla erişilebileceğini ileri sürmektedir.

Belge hiyerarşisinin gerekli olduğunu ifade eden görüşlere çeşitli akademik çalışmalar ve projelerde rastlanmaktadır. Bu projelerden biri olan E-ARK'da belge hiyerarşisinin benimsenmesiyle dosyası yani kaynağı belli olan bir belgede taşıyıcı ortam hakkında risk analizi yapmak gibi arşivcilik işlemlerinin kolayca gerçekleştirilebileceği ileri sürülmektedir. Bu yapı benimsenmezse ihtiyaç duyulan arşivcilik işlemlerini gerçekleştirmek için tüm belgeler üzerinde bir sorgulama yapmak gerekecek ve ciddi emek harcanabilecektir[40]. Belge hiyerarşisinde ise birim, seri ve dosya seçilerek ilgili belge üzerinde ihtiyaç duyulan arşivcilik işlemleri yapılabilecektir.

Belge hiyerarşisini fiziki olarak oluşturmanın yanı sıra, bu yapının üstveriler aracılığıyla tesis edilebileceğine ilişkin görüşlerle de karşılaşılmaktadır. Örneğin Norveç'te geliştirilen NOARK sisteminde bu yöntem tercih edilmiştir. Belgelerin ait

---

38 **a.g.e.**, s. 264.

39 MacNeil, "Methods for Creating and Maintaning Reliable and Authentic Electronic Records", **a.g.e.**, s. 43.

40 E-ARK, **Common Specification for Information Packages**, **a.g.e.**

olduğu konu ya da vaka dosyası ve seriler üstverilerde yer almaktadır. Burada üstveriler üzerinden bir sorgu geliştirilerek belgeler üzerinde risk analizi ve format değişikliği gibi işlemler yapılabilmektedir. Bu yapı benimsenirken kurumlarda üretilen belgelerin hangi dosya ve seriyle ilişkilendirileceğinin daha onlar üretilmeden belirlendiği ifade edilmektedir[41].

Örneklerde görüldüğü üzere EBYS'lerde bir belge üretilmeden önce onun hangi kapsamda meydana geldiği, hangi dosya ve seriye ait olduğunun belirlenmesi gerektiği anlaşılmaktadır. Ancak, binlerce vaka yüzlerce konu dosyasının oluştuğu kurumlarda belgelerin ait olduğu dosyalar nasıl belirlenecek, dosya kodları nasıl atanacak sorusu tartışılmaktadır. Örgütlerde belgeyi hazırlayan büro personelinin kullanacağı dosyalar ve o dosyanın ait olduğu seriler fonksiyon analizi neticesinde belirlenebilmektedir. Başka bir deyişle, başarılı bir fonksiyon analizi yapıldıysa belgelerin ait oldukları dosya ve alacakları dosya kodu belirlenmiş olur. Bürolarda belgenin konusu seçildiğinde dosya kodu da atanır. Böylece ikinci kez dosya kodu seçilmesine gerek kalmaz.

Her ne kadar bu ilk dosya kodu belgenin özniteliklerini koruması bakımından değişmez form özelliklerinden olsa da belge kullanıldığı yere göre ikinci kez dosya kodu alabilir. Hâliyle belgenin ilk üretildiği yerde almış olduğu dosya kodu, belge farklı bir birime ya da kuruma gittiğinde kullanılmayabilir. Orada belgenin dâhil olacağı yeni fonksiyona göre dosya planından ikinci bir koda sahip olabilir. Böylece bir belgede aynı anda iki kod bulunabilir. Her ikisi de belge için gerekli ve geçerlidir. Fakat kullanıldıkları yerler farklılık gösterir. Belgenin ilk aldığı dosya kodu öznitelikleri için önemliyken, ikincisi gireceği dosyayı belirlediğinden güvenilirlik ve delil değeri analizinde kullanılır. Arşivsel bağ kurmak için belirlenecek belge hiyerarşisinde ikinci kod esas alınır.

3.2.1.2. Belge Hiyerarşisi Dışındaki Görüşler

Dosya kodları aracılığıyla belge hiyerarşisi oluşturmanın amaçlarından biri de belge ile ait olduğu fonksiyon arasındaki ilişkiyi kurmaktır. Çeşitli çalışmalarda bu

---

41 Olav Hagen Sataaslaatten, "The Norweigan Noark Model Requirements for EDRMS in the Context of Open Government and Access to Governmantal Information", **Records Management Journal**, C. 34, No: 3, 2014, s. 200-203.

ilişkinin söz konusu yapı kurulmadan, provenans bilgilerinin muhafaza edilmesiyle de tesis edilebileceğini ileri süren yaklaşımlarla karşılaşılmaktadır. Rupasinghe, Weerasena ve Murray'ın yaptığı çalışmada belgeden ayrı olarak saklanan ve belgeyle ilişkisi kurulan bir provenans kaydından bu amaçla yararlanılabileceği ileri sürülmektedir[42]. Ancak, burada belgenin tek bir nesne (item) olarak değerlendirildiği düşünülmektedir. Hâlbuki, belgeyi anlamlı kılan onun tek başına varlığı değil, ait olduğu fonksiyon kapsamında oluşan diğer belgelerle olan ilişkisidir. Durum böyle olunca, fiziki olarak ya da üstveriler aracılığıyla belge hiyerarşisi benimsenmediğinde yapılacak arşivcilik işlemlerinin zahmetli olacağı ifade edilebilir. Mesela, belirli bir dosya içerisindekileri başka bir dosyaya taşımak için belgelerin bulunduğu mevcut dosya üzerinden işlem yapmak mümkünken, aksi durumda sistem üzerinden tüm belgeleri de kapsayan bir sorgunun geliştirilmesi söz konusu olacaktır. Ancak, bu sorunla karşılaşmamak için provenans kaydında belgelerin ait olduğu dosya ve seriler üstveri olarak yer alabilir.

Belge hiyerarşisinin benimsenmesine ihtiyaç duyulmadığını ifade eden görüşlerde ise belgelerin dosya ve serilerle ilişkilendirilmesinin kullanıcıların keşfetme yetisini engelleyebileceği ileri sürülmektedir. Mesela, Geoffrey Yeo, belge hiyerarşisinin bilgisayar biliminin getirdiği yaklaşımlardan biri olduğunu belirterek bunun güncelliğini yitirdiğini ifade etmektedir[43]. Bu kanaati paylaşan başka bir çalışmada kullanıcıların aradıklarına erişebilmek için bu hiyerarşiden ziyade anahtar kelime kullanma gibi çeşitli sorgulardan yararlanabilecekleri belirtilmektedir[44].

Yeo, belge hiyerarşisinin güncelliğini yitirdiğini dile getirse de belgelerin ait oldukları fonksiyonla olan münasebetinin kurulması için onların serilerle ilişkilendirilmesi gerektiğini kabul etmektedir. Ancak, serilerin arşivciler tarafından geliştirilen sanal bir kavram olduğuna dikkat çekerek bunların belgenin form özellikleri ve üstveriler gibi fiziki bir karşılığının bulunmadığını ifade etmektedir.

---

42 S. L. Rupasinghe, H. H. Weerasena ve I. Murray, "Trustworthy Provenance Framework for Document Workflow Provenance", **International Conference on Computational Techniques in Information and Communication Technologies**, 11-13 Mart 2016, New York[ABD], Curran Associates, s. 168-175.

43 Geoffrey Yeo, "Bringing Things Together: Aggregate Records in a Digital Age", **Archivaria**, No: 74, 2012, s. 88.

44 Margo Seltzer ve Nicholas Murphy, "Hierarchical File Systems Are Dead", **Proceedings of the 12. Conference on Hot Topics in Operating Systems**, ABD, USENIX Association, 2009.

Bundan dolayı, birden fazla tasnif sisteminin mümkün olabileceğini ileri sürerek kullanıcıların üstveriler aracılığıyla kendi serilerini oluşturabileceğini dile getirmektedir[45]. Yeo, belgelerin tekil birer nesne olarak ele alınıp, belge hiyerarşisindeki gibi fiziksel bir ilişki kurmaktan ziyade, ilişkili olduğu diğer belgelerle arasında yapay zekâ ve derin öğrenme gibi yöntemler aracılığıyla mantıksal bir ilişki kurulabileceğini açıklamaktadır[46].

Benzer görüşleri savunan Zhang, bazı kullanıcıların belgelerin hangi fonksiyon ve iş kapsamında üretildiğini incelemek için değil, ulaşmak istediği bir bilginin koleksiyonda yer alıp almadığını sorgulamak için araştırma yapabildiğine dikkat çekmektedir. Durum böyle olunca, üstverilerin sağladığı filtreleme, arama ve sorgulama imkânıyla aradığı malzemeye erişilebileceğini ifade etmektedir. Bundan dolayı, kâğıt ortamdaki belgeler için geliştirilen belge hiyerarşisi gibi uygulamaların bu tür kullanıcılar için elverişli olmayabileceğini dile getirmektedir[47].

Zhang, bu görüşlerinin yanı sıra teknolojik göç gibi işlemlerin dosya düzeyinde değil, belge düzeyinde yapılması nedeniyle belgelerin hiyerarşik bir yapıda kurgulanmayabileceğini ifade etmektedir. Buna rağmen, belgelerin ait olduğu fonksiyonla ilişkisinin dosya kodu gibi üstveriler aracılığıyla kurulabileceğini ayrıca belirtmektedir. Ancak, belge düzeyinde yeteri kadar tanımlama yapılmazsa bu ilişkinin kurulması pek mümkün olmayabilir[48].

Bu görüşlere karşılık, İngiliz Milli Arşivinde gerçekleştirilen Alpha Projesi'nin yürütücülerinden Tom Crane, belirli bir konu ya da vaka kapsamında oluşan belgelerin birbirinden ayrı tutulmaması gerektiğini ifade etmektedir. Belgelerin organik bağı kurulmadan, onlara üstveriler aracılığıyla erişmenin belgelerin entelektüel mahiyetinin açığa çıkarılamamasına neden olabileceğini söylemektedir[49]. INTERPARES kapsamında yapılan başka bir çalışmada ise belgelerin işlem, faaliyet, iş ve fonksiyon ilişkisi

---

45 Yeo, "Bringing Things Together: Aggregate Records in a Digital Age", **a.g.e.**, s. 46-51, 58.

46 **a.g.e.**, s. 82, 88.

47 Jane Zhang, "Original Order in Digital Archives", **Archivaria**, No: 74, 2012, s. 185-186, 188.

48 **a.g.e.**, s. 188-192.

49 Tom Crane, **Baffled by Archives: Part One**, (Çevrimiçi) https :// blog. nationalarchives. gov. uk/baffled-by-archives-part-one/, 24 Mart 2020. ; The National Archives, **Technical Discovery: Project Alpha**, (Çevrimiçi) https :// blog. nationalarchives. gov. uk/ technical-discovery-project-alpha/, 24 Mart 2020.

içerisinde üretildiğinden hiyerarşik yapılarından koparılamayacağı dile getirilmektedir. Aksi takdirde, bir kargaşa (digital chaos) ile karşılaşılabileceği ileri sürülmektedir[50].

3.2.2. Diplomatik Analiz

3.2.2.1. Analizin Gerekliliği

Tarih boyunca kurumların yaptıkları iş ve işlemler sonucunda belge üretilmiştir. Ancak, zaman içerisinde bu belgelerin bazıları tahrif edilmiş, sahteleriyle karşılaşılmıştır. Bunun neticesinde doğrulukları sorgulanmaya başlanmıştır. Bu sorgulama, asıl belgeleri sahtelerinden ayırma çabalarını bir metodolojiye dönüştürerek diplomatiğin gelişmesine kaynaklık etmiştir[51].

Belge bilimi anlamına gelen diplomatik, belgelerin form özelliklerini, üretilme usulünü düzenleyen prosedürleri, üreten kaynağı ve üretildiği fonksiyonun incelenmesine rehberlik edecek metodolojiyi açıklar[52]. Söz konusu inceleme yapılırken belgelerin yapısı, karakteristiği, bileşenleri ve ilişkileri kritik edilir[53]. Bu hususlar, yasal ve idari prosedürlerle şekillenir. Prosedürlerde belgelerin üretim, iletim ve muhafaza süreçlerinde uygulanacak adımlar açıklanır. Diplomatik, bu süreçleri inceleyerek güvenilirliğin nasıl analiz edilebileceğine ilişkin yol haritası sunar[54].

Güvenilirliğin başarıyla korunması için belgelerin tanımlanıp bütünlüğünün muhafaza edilmesi gerekir. Bu süreç, doğrusal bir çizgi değildir; döngüsel olarak devam eder, belge imha edilince döngü tamamlanır. Bu süreçte güvenilirliğin başarıyla korunduğunu gösterecek unsurlara ihtiyaç duyulmaktadır. Bunların diplomatik analiz unsurları olan belgede yasal ve idari prosedürlerin tayin ettiği taşıyıcı ortam,

---

50 Giovanni Michetti vd., "Intellectual Control", **Trusting Records in the Cloud**, ed.: Luciana Duranti ve Corinne Rogers, Londra[Birleşik Krallık], Facet Publishing, 2019, s. 157-159.

51 Çiçek, **Modern Belgelerin Diplomatiği**, **a.g.e.**, s. 13.

52 **a.e.**

53 Duranti, "Structural and Formal Analysis: The Contribution of Diplomatics to Archival Appraisal in the Digital Environment", **a.g.e.**, s. 71.

54 Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice", **a.g.e.**, s. 20-21. ; INTERPARES'in koordinatörü Luciana Duranti, belgelerin güvenilirliğini diplomatik analizde üretim, iletim ve muhafaza süreçleriyle ilişkilendirmektedir. Üretim sürecinde, belgelerin sahip olduğu form özelliklerinden delil değeri analizinde kritik rollere sahip olanlar belirlenir. İletim sürecinde belirlenen bu özelliklerin üstveriler ve arşivsel bağ gibi bileşenlerde doğru verilip verilmediği değerlendirilir. Muhafaza sürecinde kurumun sayısal koruma kapasitesi çerçevesinde belgelerin güvenilirliğinin nasıl muhafaza edilebileceği kararlaştırılır (Duranti, "Structural and Formal Analysis: The Contribution of Diplomatics to Archival Appraisal in the Digital Environment", **a.g.e.**, s. 81).

düzenleyen, belgeden sorumlu ve işlem gibi iç ve dış kaynaklı form elemanlarının olabileceği belirtilmektedir[55]. Diplomatik, belgelerin öznitelikleri olarak ifade edilen bu hususların tanımlanmasına yardımcı olur[56].

Ancak, kâğıt belgeler için geliştirilen diplomatik teoride üretim, muhafaza ve koruma süreçlerindeki sıkı denetimin belgelerin özgün olduklarına dair bir karine sunması nedeniyle güvenilirliğin özgünlükle eş değer tutulduğu belirtilmektedir. E-belgeler söz konusu olduğunda ise özgünlüğün basamakları olan tanımlanabilirlik ve bütünlük arasındaki birliktelik ortadan kalkmıştır. Çünkü zaman damgası ve e-imza algoritmalarının güncellenmesi, teknolojik göç ettirme gibi süreçler belgelerin bütünlük analizlerinde daha kapsamlı bir süreç yönetimini gündeme getirmiştir[57]. Burada belgenin hangi faaliyet ve fonksiyon kapsamında üretildiği, format yenilemesi gibi değişimler ve diplomatik özelliklerinin kayıt altına alınması gerekir[58]. Böylece, güvenilirliğin korunduğuna ilişkin bir karine sunulabilir.

Durum böyle olunca, INTERPARES gibi çeşitli projelerde güvenilirliğin e-belgelerin diplomatik özelliklerinin kritik edilmesiyle değerlendirilebileceği fikri öne çıkmıştır. Burada belgelerin türüne göre sahip olması gereken özellikleri barındırıp barındırmadıklarını inceleyebilmek için belge analiz şablonu (template analysis)[59] hazırlanmıştır. Bu şablonda, bir e-belgenin diplomatik özellikleri incelenerek her eleman tanımlanır, amaçları açıklanır ve güvenilirliği değerlendirmek noktasında ne ölçüde yararlı olduğu belirtilir.

---

55 Rogers, "Diplomatics of Born-digital Documents: Considering Documentary Form in a Digital Environment", **a.g.e.**. s. 14.

56 Çiçek, **Modern Belgelerin Diplomatiği**, **a.g.e.**, s. 37.

57 Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice", **a.g.e.**, s. 21-23.

58 Duranti, "The Concept of Electronic Record", **a.g.e.**, s. 10.

59 MacNeil vd., "Requirements for Assessing and Maintaining the Authenticity of Electronic Records", **a.g.e.**, s. 1-2. INTERPARES çalışmaları kapsamında bir şablon (*Template Analysis*) geliştirilmiştir. Bir e-belgede bulunan form özellikleri bu tezde müstakil olarak incelenmemektedir. Fakat saha araştırmasında bu özelliklerin belge profilinde bulunup bulunmadığı sorgulanmıştır.

3.2.2.2. E-Belgelerin Diplomatik Özellikleri

3.2.2.2.1. Dokümanter Form

E-belgelerin güvenilirliği aynı zamanda standartlar ışığında geliştirilen uygulama yazılımları koşullarının da incelenmesini gerektirir. Diplomatik analiz, dokümanter form ve prosedürlerin tasarlanmasına kaynaklık ederek güvenilir sistemlerin geliştirilmesine katkı sağlar[60]. Başka bir deyişle güvenilir sistemler geliştirilirken belgelerin diplomatik özellikleri dikkate alınır. Kâğıt belgelerde iç ve dış kaynaklı form elemanları olarak ifade edilen ve delil değeri kritik unsuru olarak değerlendirilebilecek bu özelliklerin e-belgeler söz konusu olduğunda daha geniş ele alındığı görülmektedir. E-belgelerin diplomatik özellikleri dokümanter form, açıklama notları, kontekst ve taşıyıcı ortam olmak üzere dörde ayrılmıştır. Dokümanter form, belgenin idari ve dokümanter konteksti ile içeriğin temsilinde gerekli olan kurallar olarak tanımlanabilir. İç ve dış kaynaklı elemanları bulunur. İç kaynaklı elemanlar, doğrudan kontekstle ilişkili olup belgedeki işleme tanıklık eden unsurlardır. Üç gruba ayrılır. Birincisi, belgenin hukuki ve idari kontekstini gösteren antet, muhatap ve tarih gibi elemanlardır. İkincisi, olayın ya da durumun açıklandığı kısım olup işlemin nasıl gerçekleştirildiğini gösteren unsur olan metindir. Üçüncüsü ise belgenin dokümanter kontekstini ve onay mekanizmasını gösteren hazırlayan, tasdikleyen ve onaylayan gibi elemanlardır[61].

Modern belgelerin diplomatiği konusunu işleyen çalışmalarda belgenin dokümanter yapısında sırasıyla ilk protokol, metin ve son protokol alanlarının bulunduğu ifade edilmektedir[62]. Bu bilgi, bilişim teknolojilerinin bir neticesi olmayıp tarihte ilk diplomatik analizlerde de açıklanan bir yapıdır. Fakat kâğıt belgelerde olduğu gibi elektronik olanlarda da bu durum ilk bakışta anlaşılmayabilir. Çünkü belge türüne göre bu alanlar oldukça değişkendir. Bundan dolayı, ilk ve son protokolü anlayabilmek için EBYS'lerde belge türüne göre profil alanı oluşturulur. Bu profilde öncelikle belgenin varlığı için gerekli olan temel form elemanları yer alır. Aynı zamanda bu belge profili, belgeyi ait olduğu dosya ve seriyle ilişkilendirmek için gerekli olan form elemanlarını barındırır. Bu profil, en başta belge düzenlendiğinde

60 Rogers, "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice", **a.g.e.**, s. 21.
61 Rogers, "Diplomatics of Born-digital Documents: Considering Documentary Form in a Digital Environment", **a.g.e.**, s. 13.
62 Çiçek, **Modern Belgelerin Diplomatiği**, **a.g.e.**, s. 162.

oluşurken belgenin iletim tarihi ve alındığı tarih, dosyasına kaldırılma tarihi, konu ya da vakayı, eklerini, tekbiçim tanımlayıcıları, güvenlik önlemleri, havale işlemleri ve düzeltme notlarını ihtiva edebilir[63].

Belge profilinde yer alan dokümanter formun bu iç kaynaklı elemanları aynı zamanda entelektüel form özellikleri şeklinde tanımlanmaktadır. Bunun nedeni, iç kaynaklı elemanların görsellikten daha çok bilgi yönü ağır basan ve okunup analiz edilerek değerlendirilebilen unsurlar olmasıyla ilişkilendirilmektedir. Belgenin iç kaynaklı form elemanları, sorumlu, düzenleyen, oluşturan, alıcı, muhatap, onaylayan, tasdik eden gibi belgedeki kişiler, tarih, belgenin üretildiği yer, konu ve protokol olarak belirtilmektedir[64].

Belge formunun iç kaynaklı elemanlarından olan belgedeki kişiler, bir dokümanın belge vasfı taşıması için gerekli olan unsurlardandır. Kişiler, belgede sorumlu, düzenleyen ve muhatap şeklinde bulunur. Sorumlu, kanunların belli görev ve fonksiyonlar tanımlayarak yetkilendirdiği belediye, üniversite, bakanlık, ticaret odası veya eğitim vakfı gibi tüzel kişiliktir. Düzenleyen, sorumlu adına yetkilendirilmiş kişi olarak belgedeki işlemi yürütme görevi bulunan imza sahibidir[65]. Belgenin gönderildiği kişi ise muhatap olarak adlandırılır. Bu kişilerin her belgenin ilişkili olduğu diğer belgelerle kurduğu ağ içerisinde görünmesinin yanı sıra, belgenin sorumlusu olarak üreticinin de bu ağda yer alması gerekir. Çünkü üretici, belgenin ait olduğu fonun hukuki olarak sahibi ve sorumlusudur. Ancak, idari teşkilatta yaşanan değişiklikler, üreticilerin kolayca belirlenememesine neden olabilir. Mesela, belgelerin başka bir birime ya da kuruma devredildiği durumlarda üretici ile fonun sorumlusu[66] ve emanetçisi[67] farklı kişiler olabilir. Bu durumda, belge ile üreticisi arasındaki ilişkinin tanımlanabilmesi için belge profilinden yararlanılabilir[68].

---

63 Duranti, "The Concept of Electronic Record", **a.g.e.**, s. 14-15.

64 Çiçek, "Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme", **a.g.e.**, s. 93, 96; Heather MacNeil vd., "Template for Analysis", **The Long-term Preservation of Authentic Electronic Records: Findings of the INTERPARES Project**, s. 1-3, (Çevrimiçi) http :// www. interpares. org/ book/ interpares_book_j_app01.pdf, 28 Aralık 2020.

65 Çiçek, **Modern Belgelerin Diplomatiği**, **a.g.e.**, s. 94-95.

66 Sorumlu, fonksiyonu yürütme yetkisi bulunan, bu kapsamda belge düzenleme yetkisine sahip olan kişi/tüzel kişidir.

67 Emanetçi, artık fonksiyonu yürütme yetkisi bulunmayan, o belgeleri emanetinde tutan kişi/tüzel kişidir.

68 Rogers, "Diplomatics of Born-digital Documents: Considering Documentary Form in a Digital Environment", **a.g.e.**, s. 16-17. ; Çiçek, **Modern Belgelerin Diplomatiği**, **a.g.e.**, s. 94-97.

Belgenin iç kaynaklı elemanlarının yanı sıra bir diğer dokümanter form elemanları metin, görüntü, bağlantılar gibi dış kaynaklıdır. Bunlar, belgenin üretilme amaçlarını gerçekleştirmek ve sunumunda kullanılacak algılanabilir özelliklerini ifade eder. E-belgeler için bu özellikler, metin, grafik, görüntü gibi genel sunum özellikleri, özel sayfa düzenleri (mizanpaj), metin içerisinde farklı sayfalara bağlantı kurulup kullanıcıyı yönlendiren bağlantılar, renkler ve ses dosyalarının örnek oranları gibi belirli sunum özellikleri, e-imza ve e-mühür, zaman damgası ve filigran gibi özel işaretlerdir. Özel bir sunum şekli varsa bu bilgiler sunum özellikleri kısmında belirtilir. Özel sunum özellikleri, özel biçimler, yazı karakteri tipi ve rengi, farklı sayfalara yönlendirme yapan bağlantılar, eklentilerin grafik belirtileri, ses dosyalarının örnek oranları, görüntü dosyalarının çözünürlüğü ve haritaların ölçeği olabilir[69]. Bu özelliklerin de belge profilinde yer alması gerekir.

3.2.2.2.2. Açıklama Notları, Kontekst ve Taşıyıcı Ortam

E-belgelerin ikinci diplomatik özelliği olan açıklama notları, belge üretildikten sonra yapılan eklemeleri ifade eder[70]. Bu unsur, kâğıt belgeler için ilaveler adıyla geçmekte olup, dokümanter formun özelliklerinden ve belgenin dış kaynaklı elemanlarından biridir. E-belgeler için ise belge üzerinde değil ayrı bir üstveride müstakil bir alanda gösterilir.

Açıklama notları, işlem, kullanım ve yönetim safhaları olmak üzere üç türdür[71]. İşlem safhasındaki açıklamalara paraf ve imzalar, evrak kayıt numarası ve e-mühür örnek verilebilir. Kullanım safhasında acil kodlu veya sevk edilen yazılar, belgenin alındığı tarih, havale notu, belgeyi kullanan birim, gerçekleştirilen işlem, yapılan muamele ve iletim zamanı belirtilir. Yönetim safhasında ise belgenin arşive devredildiği tarih, arşiv numarası, versiyon numarası, dosya kodu ve belge sayısı gibi bilgiler ifade edilmektedir[72].

---

69 Çiçek, "Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme", **a.g.e.**, s. 95; MacNeil vd., "Authenticity Task Force Report",**a.g.e.**, s. 5-6. ; MacNeil vd., "Template for Analysis", **a.g.e.**, s. 1.

70 MacNeil vd., "Authenticity Task Force Report",**a.g.e.**, s. 6.

71 Çiçek, **Modern Belgelerin Diplomatiği**, **a.g.e.**, s. 163. ; Çiçek, "Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme", **a.g.e.**, s. 96.

72 Duranti, "The Concept of Electronic Record, Preservation of the Integrity of Electronic Records", **a.g.e.**, s. 14.; Çiçek, "Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın

E-belgelerin diplomatik özelliklerinin üçüncüsü kontekstir. Beş tür kontekstin olduğu belirtilmektedir. Bunlar, idari-hukuki, kaynağa ait, prosedüre ait, dokümanter ve teknolojik kontekstlerdir. Konteksti açığa çıkarmak, e-belgelerin üretimi, muhafazası ve kullanımı sonucunda oluşan iş süreçlerini anlamak için oldukça kritiktir. Bunlardan teknolojik kontekst dışındakiler kâğıt belgeler için de geçerlidir. Teknolojik kontekstte, donanım, yazılım, veri, sistem modelleri ve sistem idaresi kritik edilmektedir[73].

E-belgelerin diplomatik özelliklerinin dördüncü ve sonuncusu taşıyıcı ortamdır. Belgenin fiziksel taşıyıcısı olan araç, bu kısımda tanımlanır. Kâğıt belgelerin de diplomatik özelliklerinden olan taşıyıcı ortam, dış kaynaklı bir eleman olup, belgenin dokümanter formunda bir alt unsurdur. Ancak, e-ortama geçildiğinde belgenin ana diplomatik unsurlarından biri olarak görülüp, müstakil bir alan olarak değerlendirilmiştir. Bunun nedeni, uygulama yazılımlarında taşıyıcı ortam formatının değişkenliğidir. Belge, başka bir formatla da aynı mesajı verebilir[74]. Mesela, aynı bilgi JPEG formatındaki bir belgede veya TIFF formatındaki bir belgede bulunabilir. Format farklılığı, bilginin ve düzenleyenin değiştiği anlamına gelmemektedir. Aynı zamanda belgede öngörülen işlem ve doğuracağı hukuki sonuçlar formata göre de değişmemektedir. Ancak, uygulama yazılımlarında oluşan bu farklı formattaki belgelerin diplomatik özelliklerinin korunması gerekir. Hâliyle, bu özelliklerin muhafaza edildiği bilgi teknolojilerinin diplomatik analizde önemli bir rolünün olduğu anlaşılmaktadır.

3.2.2.3. Güvenilirlikle İlişkisi

Bilgi teknolojileri, pek çok kolaylık getirmesinin yanı sıra bilerek veya bilmeyerek e-belgelerin değiştirilme riskini de beraberinde taşımaktadır. Elektronik ortamda muhafaza edilen belgelerin güvenilirliğinin başarıyla korunması için öznitelikleri değiştirilmemeli ve bozulmamalıdır. Bunun için belgelerin tanımlanarak bütünlüğünün gösterilmesi gerekir.

Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme", **a.g.e.**, s. 96. ; MacNeil vd., "Template for Analysis", **a.g.e.**, s. 4-5. ; Çiçek, **Modern Belgelerin Diplomatiği**, **a.g.e.**, s. 185-189.

73 Çiçek, "Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme", **a.g.e.**, s. 96. ; MacNeil vd., "Template for Analysis", **a.g.e.**, s. 5-8.

74 Çiçek, "Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme", **a.g.e.**, s. 96. ; MacNeil vd., "Authenticity Task Force Report", **a.g.e.**, s. 6.

Tanımlama, belgenin karakteristik özelliklerini belirterek onun diğerlerinden ayırt edilmesini sağlar. Diplomatik bakış açısıyla bu karakteristik özelliklere, belgedeki kişiler, üretim tarihi, iletim tarihi, konu, arşivsel bağ, dosya kodu ve belgenin ekleri örnek verilebilir. Belgenin kimliğini oluşturan bu unsurlar, belge profilinde ya da üstverilerde açık bir şekilde belirtilmiş olabilir veya yukarıda açıklanan beş kontekstte (dokümanter, kaynağa ait, prosedüre ait, idari-hukuki ve teknolojik) örtük bilgi şeklinde yer alabilir[75].

Ancak, INTERPARES kapsamında yapılan saha araştırmalarında kurumlarda üretilen çoğu e-belgenin sabit bir dokümanter form ve değişmeyen bir içeriğe sahip olmadığı görülmüştür. Kurumlarda, aynı faaliyet kapsamında oluşan belgeler arasında arşivsel bağın kurulamadığı gözlenmiştir[76]. Bunun nedeni, e-belgelerin oluştuğu sistemlerin arşivcilik bakış açısıyla geliştirilmemesi olabilir. Hâl bu iken belgelerin güvenilirliğinin korunmasında arşivcilik kaynaklı yöntemlerin daha çok öne çıkarılması gerektiği düşünülmektedir.

Diplomatik analizde belgenin içerik, kontekst ve yapı özellikleri kritik edilerek güvenilirlik karineleri belirlenir. Bunlar, güvenilirliğin doğrulanmasında kullanılır. Bu doğrulama, belgenin hem güncel kullanım safhasında hem de arşivdeki muhafaza aşamasında edindiği özellikleriyle onda bulunması gereken öznitelikler arasında bir ilişki kurma işlemidir. Bu işlemler her iki safhada da yapılmalıdır. Ancak, belgenin güvenilirliğinin bir kez doğrulanması yeterli olmaz. Zaman içerisinde elektronik ortamda oluşabilecek kayıplar, e-imza ve zaman damgası sertifikalarının güncellenmesi gibi durumlardan dolayı belgelerin güvenilirliği belirli aralıklara kontrol edilmelidir. Böylece, gelecekteki kullanıcılar güvenilirliğin nasıl başarıyla korunduğunu, bunun hangi kriterlere göre analiz edildiğini inceleyebilir[77]. Burada arşivcilik bakış açısıyla geliştirilen üstverilerden yararlanılabileceği görülmektedir.

---

75 MacNeil vd., "Requirements for Assessing and Maintaining the Authenticity of Electronic Records", **a.g.e.**

76 MacNeil vd., "Authenticity Task Force Report", **a.g.e.**, s. 12-13.

77 Duranti, "Structural and Formal Analysis: The Contribution of Diplomatics to Archival Appraisal in the Digital Environment", **a.g.e.**, s. 83.

3.2.3. Arşivsel Güvenilirlik Üstverisi

E-belgelerin özgünlük, gerçeklik ve tamlık gibi özniteliklerinin zaman içerisinde bozulup değişmeden korunması anlamına gelen arşivsel güvenilirliğin devam ettirilmesi için birtakım üstveri araçları kullanılabilir. Bu üstveriler en başta belgenin düzenleyeni, sorumlusu, arşivsel bağ, tek biçim kimliklendirme, belgelerin yapı, içerik ve kontekstinin tanımlanması ile üretimden imhaya kadar olan sürecin kayıt altına alınması gibi araçlardır[78]. Farklı ülkelerdeki çalışmalarda güvenilirlikle ilgili olarak bu üstverilerden yararlanılabileceği belirtilmektedir[79].

Bahsedilen bu üstverilerin Kanada merkezli INTERPARES çalışmaları kapsamında geliştirilen koruma zincirinde (preservation chain) değerlendirildiği görülmektedir. Bu zincirde üstveriler, belgelerin güncel, yarı güncel ve arşivdeki işlemleriyle alakalı olarak üç döneme ayrılarak ele alınmıştır[80]. 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[81]. 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[82].

Güvenilirliğin başarıyla korunmasında benimsenen yöntemlerden biri de yedeklemedir. Hâliyle, kurumlarda yedeklemeyle ilgili üstveriler de oluşmaktadır.

---

78 Rogers, "Diplomatics of Born-digital Documents: Considering Documentary Form in a Digital Environment", **a.g.e.**, s. 12. ; INTERPARES, **INTERPARES 2: Experiential, Interactive and Dynamic Records**, **a.g.e.**, s. 277.

79 Literatürde arşivsel güvenilirlik üstverisiyle alakalı olarak yürütülen çalışmalar ve yapılan yayınların Kanada, Norveç, Malezya, Almanya, Litvanya, İtalya, Hindistan ve Çin gibi ülkelerde daha fazla olduğu görülmüştür.

80 **a.g.e.**, s. 200-205.

81 **a.g.e.**, s. 209-211.

82 **a.g.e.**, s. 213.

Bunlar, yedeklemenin türü, kapsamı, zamanı, referans numarası ve kim tarafından ne zaman onaylandığı gibi üstverilerden teşekkül edebilir[83].

Kurumlarda yedekleme yapılsa da 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[84].

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 özgünlüğünü onaylamak için kullanılan teknikler, özgünlüğü onaylayan kişi, özgünlük değerlendirme raporu referans numarası, özgünlüğü onaylanan belgelerin arşive devir zamanı, güncel belge döneminde yapılan dokümantasyonlar ile devir sırasında benimsenen güvenlik ve kontrol prosedürleri gibi hususlara yönelik üstverilerin kullanılabileceği anlaşılmaktadır[85].

E-belgelerin kullanımının artmasıyla birlikte INTERPARES kapsamında geliştirilen bu üstverilere benzer üstverilerin çeşitli ülkelerde de kullanılmaya başlandığı görülmektedir. Belgelerin dosya ve serileriyle ilişkilendirilerek saklandığı Norveç'te müstakil olarak özgünlük üstverisinin geliştirilmesi dikkat çekmektedir. Burada belgelerin özgünlüğü, erişim kontrolü ve bütünlüğü ayrı bir üstveri alanı olarak kurgulanmıştır[86]. Bununla birlikte, Malezya, Almanya, Litvanya, İtalya ve Hindistan gibi ülkelerde OAIS yapısında arşivlenen belgelerin tanımlanmasında[87] kullanılan üstverilerin arşivsel

---

83 **a.g.e.**, s. 214-215.

84 **a.e.**

85 **a.g.e.**, s. 221, 226-228. ; Joseph Tennis, bu üstverilerin yanı sıra belgelerin yaşam döngüsündeki süreçleri açıklayan log kaydı gibi dokümantasyonların güvenilirliğin korunmasına yardımcı olabileceğini ifade etmektedir (Joseph T. Tennis, "Data, Documents and Memory: A Taxonomy of Sources in Relation to Digital Preservation and Authenticity Metadata", **The Memory of the World in the Digital Age: Digitization and Preservation**, 26-28 Eylül 2012, ed.: Luciana Duranti ve Elizabeth Shaffer, Vancouver[Kanada], UNESCO, 2013, s. 935, 939).

86 Long Term Records Management Project, **Recommended Practices**, (Çevrimiçi) http :// research.dnv.com/LongRec/ResearchResults/Pages/RecommendedPractices.html, 28 Ocak 2020.

87 Malezya'da tanımlama standardı olarak Encoded Archival Descrpiton (EAD - Kodlanmış Arşivsel Tanımlama) ve Preservation Metadata Implementation Strategies (PREMIS - Koruma Üstverisi Uygulama Stratejileri), Almanya ve Litvanya'da ise Metadata Encoding and Transmission Standard (METS - Üstveri Kodlama ve İletim Standardı) kullanılmaktadır. Almanya ve Litvanya'da METS kullanılarak tanımlanan üstveriler, arşiv bilgi paketi olarak XML formatında tutulmakta ve zaman damgası kullanılarak e-imza ile imzalanmaktadır (Ap-

güvenilirlik üstverisi olarak kullanılabileceği kanaati oluşmaktadır. Malezya'da kullanılan belgelerin referans numarası ve muhafaza sürecinde yapılan arşivcilik işlemleri gibi üstveriler bunlara örnek verilebilir[88].

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[89].

Hindistan Anayasa Mahkemesinde oluşan belgeler, arşiv bilgi paketi hâline getirilirken özet değeri, format, dizin ve belge sayısı gibi üstveriler kullanılmaktadır. Ancak, Abichandani ve Prakash bu üstverilerin kullanılmasına rağmen standartlaşma olmadığına dikkat çekmektedir. Bundan dolayı üstverilerin belirlenen standartlar çerçevesinde üretilmesine ve belgelerin özgünlüğünü tasdik edecek yöntemlerin tayin edilmesine duyulan ihtiyacı dile getirmektedirler[90].

Bu örneklerin yanı sıra, Çin'deki Beijing arşivlerinde gerçekleştirilen bir uygulama dikkat çekmektedir. Burada, belgeler özniteliklerinin korunup korunmadığı

azli Bunawan, Sharifalillah Nordin ve Haryani Haron, "Model for Preserving the Electronic Records Event History Metadata in Malaysia Government Agencies", **Seventh International Conference on Computational Intelligence, Modelling and Simulation (CIMSim)**, 27-29 Temmuz 2015, ed.: David Al-Dabass, Zuwairie Ibrahim ve Mohd Ibrahim Shapiai, yayım yeri yok, yayımcı yok, 2015. ; Hrvoje Stancic, Arian Rajh ve Hrvoje Brzica, "Archival Cloud Services: Portability, Continuity and Sustainability Aspects of Long-term Preservation of Electronically Signed Records", **The Canadian Journal of Information and Library Science**, C. 39, No: 2, 2015, s. 218, 220, 223).

88 Bunawan, Nordin ve Haron, **a.g.e.** s. 29-34.

89 Radyoloji sonuçlarına yapılan medikal tanılar üzerinden hareket edilen İtalya'daki hasta kayıtları örneğinde, e-imza ile imzalanan ve uzun dönemli saklanmasına karar verilen belgelerin öncelikle gönderim bilgi paketleri oluşturulmaktadır. Bu paket oluşturulduktan sonra paketin daha önce sisteme yüklenip yüklenmediği ve e-imzaya ait sertifika ile rapor imzalanırken oluşturulan özet değeri kontrol edilmektedir. Bu kontroller sonucunda bir hata ile karşılaşılmazsa belgeye zaman damgası eklenmektedir (Silvio Salza ve Maria Guercio, "Authenticity Management in Long Term Digital Preservation of Medical Records", **9. International Conference on the Preservation of Digital Objects**, 1-5 Ekim 2012, ed.: Reagan Moore, Kevin Ashley ve Seamus Ross, Toronto[Kanada], University of Toronto, 2012, s. 177-178).

90 Payal Abichandani ve Rishi Prakash, "Digital Preservation of Court's Disposed Case Records - A Case Study from Indian Judicial System's Perspective", **APA/C-DAC International Conference on Digital Preservation and Development Trusted Digital Repositories**, 5-6 Şubat 2014, ed.: Dinesh Katre ve David Giaretta, Yeni Delhi[Hindistan], yayımcı yok, 2014, s. 220-227.

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[91].

Belgelerin özgünlüklerinin doğrulanmasına yönelik bir başka öneride noter gibi bir otoriteden yararlanılabileceği ifade edilmektedir. Burada, özgünlüğünün doğrulanması amacıyla e-belgelerin imzaları ve üstverileriyle birlikte bir paket hâline getirilebileceği ve bu paketin noter gibi bir otorite tarafından onaylanabileceği 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[92].

Yukarıda çeşitli çalışmalar ve ülkelerden verilen örneklerden de yararlanılarak Türkiye'de kullanılacak arşivsel güvenilirlik üstverisi alanlarının oluşturulmasına ihtiyaç duyulduğu düşünülmektedir[93]. Bu tez kapsamında öneri olarak arşivsel güvenilirlik üstverisi hazırlanmaya çalışılmıştır. Bunun için TS 13298, belge yönetimi ve arşivcilikle ilgili ISO standartları ve INTERPARES çalışmalarından

---

91 Guigang Zhang vd., "A New Electronic Records Security Model for Long-term Preservation", **10th Web Information System and Application Conference**, 10-15 Kasım 2013, ed.: Bin Li, Ruixuan Li ve Derong Shen, Yangzhou[Çin], yayımcı yok, s. 191-194.

92 Dimitrios Lekkas ve Dimitris Gritzalis, "Long-term Verifiability of Electronic Healthcare Records' Authenticity", **International Journal of Medical Informatics**, No: 76, 2007, s. 442-448.

93 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 arşivsel güvenilirliğiyle ilişkilendirilebilecek belgedeki kişiler, üretim tarihi, format, dosyalama, sayısal koruma gibi hususlar zorunlu ve seçmeli üstveriler olarak yer almaktadır (Yalçınkaya, "E-devlet Üstveri Standardının Oluşturulması ve Türkiye için Modellenmesi", **a.g.e.**). Bununla birlikte, Gülten Alır, 2008'de gerçekleştirdiği doktora tezinde Adalet Bakanlığında oluşan e-belgeler için kullanılabilecek bir üstveri modeli önermiştir. Hâliyle, bu modelde müstakil bir güvenilirlik üstverisi yer almamaktadır. Ancak Bakanlık'ta oluşan belgeler için kullanılması önerilen belgedeki kişiler, belgenin türü, e-imza ve ekler gibi üstveriler, aynı zamanda arşivsel güvenilirlik üstverisi olarak değerlendirilebilmektedir (Gülten Alır, "E-Türkiye Uygulamaları: Elektronik Belge Yönetimi ve Üst Veri", Yayınlanmamış Doktora Tezi, Ankara, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı, 2008, s. 97-100).

yararlanılmıştır[94]. Ancak, söz konusu üstverilerin, belirli bir zamanda bitirilmesi gereken bu tezde kapsamlı bir şekilde ele alınması mümkün olmamıştır. Buna rağmen, üstverilerin incelenen güvenilirlik düzeyleriyle ilişkisinin kurulması konusunda gayret gösterilerek Tablo 7. Arşivsel Güvenilirlik Üstverisi oluşturulmuştur.

3.3. Teknolojik Yöntemler

3.3.1. Elektronik Delil Elde Etme Yöntemleri

3.3.1.1. Uygulama Aşamaları

İdari ve hukuki işlemlerde bilişim sistemlerinin giderek artan bir şekilde kullanımı elektronik delillerin tespiti, muhafazası ve yargı mercilerine sunulmasıyla alakalı yöntemler geliştirilmesine sebep olmuştur. Bunlardan biri adli bilişim uygulamalarıdır[95]. İngilizce yabancı dildeki "forensics" 'ten Türkçe'ye adli bilişim şeklinde geçen bu kavram, sayısal ortamda gerçekleşen ve hukuki bir sonuca yönelme ihtimali olan adli vaka niteliğindeki bir olayın analiz edilmesi anlamına gelmektedir[96]. Fakat bu teknik analiz özellikle e-belgeden delil elde etme anlamına gelmemekte olup daha genel manada kullanılmaktadır. Her ne kadar belge yönetimi alanında da bu kavramın tercih edildiği görülse de[97] Türkçe'ye aktarılırken adli bilişim olarak değil, e-delil elde etme şeklinde çevrilmesi tercih edilmiştir[98].

---

94 Bu üstverilerin aynı zamanda saha araştırmasında incelenen kurumlarda var olup olmadığı da sorgulanmış; kaynakları Tablo 2'de belirtilmiştir.

95 Çiçek ve Sağlık, "E-Belgelerin Arşivsel Bağının Elektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme", **a.g.e.**, s. 267.

96 Türkiye'deki çalışmalarda "computer forensics" ya da "digital forensics" şeklindeki kavramlar da adli bilişim olarak kullanılmaktadır (**a.e.**).

97 Metin Turan, "Adli Bilişim ve Dijitalleştirme: Roller, Etkileşim ve Sorunlar", **e-BEYAS 2015 Sempozyumu Kurumsal Belleklerin Geleceği: Dijitalleştirme-Elektronik Arşiv-Elektronik Belge Yönetimi**, ed.: Fahrettin Özdemirci vd., Ankara, Ankara Üniversitesi, 2016, s. 121-134. ; Türkay Henkoğlu, **Adli Bilişim: Dijital Delillerin Elde Edilmesi ve Analizi**, İstanbul, Pusula Yayınları, 2014.

98 Forensics, Türkçe'de adli bilişim şeklinde kullanılsa da çalışılan bu doktora tezi, sadece teknolojik ortamda gerçekleşmiş suç niteliği olan vakaları inceleyen bir araştırma değildir. Bundan dolayı mevcut kavram, tezin ana teması olan e-imzalı belgelerin delil değeri konusuyla doğrudan örtüşmediği için olduğu gibi kullanılmak yerine "e-delil elde etme" şekliyle tercih edilmiştir. Çünkü e-belgelerden delil elde etmekle ilgili iş ve işlemlerin mahiyeti göz önüne alındığında adli bilişim kavramının meselenin muhtevasını tam olarak karşılayamadığı düşünülmektedir. (Çiçek ve Sağlık, "E-Belgelerin Arşivsel Bağının Elektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme", **a.g.e.**, s. 267-268). Konu uzmanlarının da adli bilişim kavramının yeteri kadar açıklayıcı olmadığını ifade ettiği görülmektedir (Hakan Aydoğan, "Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri", Yayınlanmamış Yüksek Lisans Tezi, Ankara, Polis Akademisi, 2009. ; Gökhan Şengül, F. K. Atsan ve Atila Bostan, "Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve

Saha uzmanları e-ortamdaki taşıyıcılardan delil elde etmeyi genelden özele bir bakış açısıyla ele almışlardır. Öncelikle, delil unsuru olabilecek her türlü verinin değerlendirildiği yöntemler dikkat çekmektedir. E-belgelerin kullanılmaya başlamasıyla bunların e-belgeye daha çok odaklandıkları görülmektedir.

Elektronik ortamdaki bir malzemeden delil elde edilirken takip edilecek aşamalarda küçük farklılıklar olsa da genellikle ortak bir süreç üzerinde uzlaşıldığı görülmektedir. Uluslararası ortak bir platform olan DPC için hazırlanan raporda bu ortak süreçte tanımlama, yetkilendirme, hazırlık, güvenliği sağlama, koşulları kayıt altına alma, delil toplama, paketleme, taşıma ve saklama, ilk inceleme, imaj alma ve kopyalama, analiz ile sunum ve raporlama aşamalarının olduğu belirtilmektedir[99].

İlk aşama olan tanımlamada vaka incelenir, anlaşılmaya çalışılır, ardından ihtiyaç duyulan adımlar kararlaştırılır ve delil analizi için fikir yürütülür. Yetkilendirme aşamasında delil elde etme işlemlerini yürütmek için kimlere yetki verileceği belirlenir. Hazırlık aşamasında inceleme için gerekli olan hususlar tespit edilmeye çalışılır. Sonraki aşamada analiz yapılacak malzemelerin bilgi güvenliği sağlanarak delil toplamak için gerekli cihazlar hazırlanır. Sonrasında uygulama koşullarının kayıt altına alınması için kullanılacak dokümantasyon oluşturulur ve delillerin toplanması aşamasına geçilir. Paketleme, taşıma ve saklama aşamasında delilin aidiyet zincirinin korunması için gerekli tedbirler alınır. İlk inceleme aşamasında delil inceleme cihazları değerlendirilir. Bu cihazlardan delil elde etmek için hangi donanım ve yazılım araçlarının kullanılacağı tayin edilir. Bunun için aynı belgenin nüshasını çıkarmak şeklinde ifade edilen imaj alma[100] ve kopyalama aşamasında yazma koruma cihazları kullanılır. Böylece, delil elde edilecek disklerin birebir imajı alınır ve deliller analiz edilmeye hazır hâle gelir. Burada kriptografi kullanılarak delillerin özet değerleri hesaplanır ve dosya yapıları incelenir. Son aşama olan sunum ve raporlamada, elde

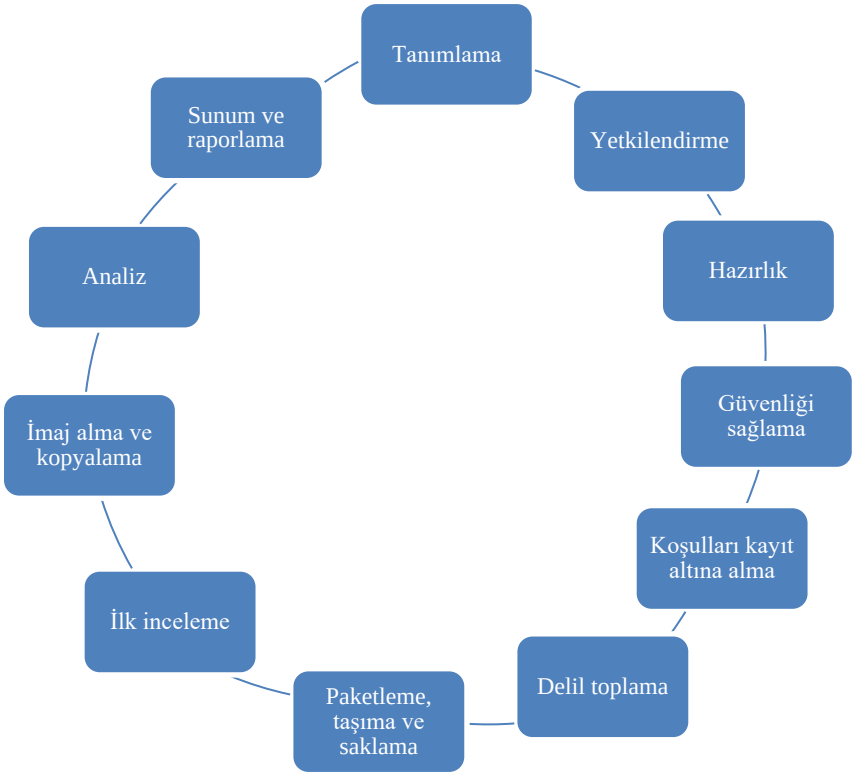
---

Gelecek Öngörüleri", **7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı**, 7-18 Ekim 2014, İstanbul, yayımcı yok, 2014, s. 96, (Çevrimiçi) https :// www. iscturkey. org/ assets/ files/2016/03/isc2014-32.pdf, 27 Kasım 2019. Bu çalışmada, digital forensics için sayısal sistem ve cihaz incelemesi kavramı önerilmiştir).

99 Jeremy Leighton John, **Digital Forensics and Preservation**, Birleşik Krallık, Digital Preservation Coalition [DPC], 2012.

100 Hedef diskteki tüm bitlerin kopyalanarak incelemeye esas teşkil edecek diske aktarılması imaj oluşturma olarak bilinmektedir. Bu işlemler yapılırken kullanılan donanım ve yazılım özellikleri kayıt altına alınarak aidiyet zinciri kurulmaya başlanır ve incelemeye esas teşkil edilen disk, güvenli bir analiz için ilgili birimlere aktarılır (Kirschenbaum vd., **a.g.e.**, s. 16).

edilen veriler log kayıtlarıyla birlikte sunuma hazır hâle getirilerek, incelenen delillerden bir sonuç elde edilir[101]. Bu aşamaların iş akış süreci şu şekille gösterilebilir:



Şekil 2. Elektronik Delil Etme Aşamaları

Delil incelemede, imaj oluşturmanın önemli bir yeri vardır[102]. İmajlar oluşturulurken donanımsal ya da yazılımsal yöntemler tercih edilmektedir. Donanımsal yöntemde, özel olarak geliştirilen cihazların bir tarafına delil elde edilecek disk, diğer tarafına da analizin yapılacağı disk bağlanır. Delil elde edilecek diskin bütünlüğü, bağlı olduğu girişin yazma korumalı olmasıyla sağlanmaktadır. Yazılımsal yöntemlerde ise bu iş için özel olarak geliştirilen uygulamalar tercih edilebilmektedir. Her iki yöntemde de delil elde edilecek diske yeni veri transferinin engellenmesi hedeflenmektedir[103].

101 John, **Digital Forensics and Preservation**, **a.g.e.**, s. 2, 15-16.
102 Kirschenbaum vd., **a.g.e.**, s. 16
103 Hayrettin Çatalkaya, Muhammer Karaman ve Erdal Koca, "Elektronik Kopyanın (Adli İmaj) Alınmasında Açık Kaynak Uygulamalarının Güvenirliği", **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi**, C. 1, No: 2, 2015, s. 16-17.

Bu işlemler yapılırken kullanılan donanım ve yazılım özellikleri kayıt altına alınarak aidiyet zinciri kurulmaya başlanır. Bu zincirin kurulması sağlıklı bir analizin de başlangıcı olarak kabul edilmektedir[104]. Bunun için özet değerlerinden faydalanılarak oluşturulan imaj dosyası, analizde kullanılacak disk ve ana diskteki verilerin birbirine eş olmasına dikkat edilir[105].

Bu işlemlerden sonra diskteki verilerin dosya sistemi açıklanır[106]. Bu sistem, aktif ve aktif olmayan dosyaları gösterdiğinden verilere erişmek için oldukça önemli kabul edilmektedir. Aktif dosyalar, işletim sisteminde hemen erişilebilir olanlardır. Aktif olmayanlar ise kullanıcının erişimine sunulmamış alanlarda bulunur. Örneğin silinmiş dosyalar bu alanda yer alır. Dosya sistemlerinin incelenmesi neticesinde aktif ve aktif olmayan alanlardan elde edilen tüm verilerin işlemler sonucunda oluşturulan dokümantasyona eklenmesi gerekir[107].

Söz konusu uygulama adımlarından da anlaşılacağı üzere e-delil elde etme yöntemleri ciddi emek isteyen bir süreçtir. Bu nedenle, kurumlarda ilgili yöntemler uygulanırken çeşitli sorunlar yaşanması muhtemeldir. Bunlara, EBYS'lerin e-delil elde etme yöntemlerini yeteri kadar destekleyememesi, mevcut e-delil elde etme yazılımlarının sınırlı sayıda dosya yapısıyla çalışabilmesi (FAT32, NTFS, Unix ve HFS vb.), kullanılmış disketler gibi eski donanımları analiz edecek malzeme eksikliği ve sürecin maliyetli olması örnek verilebilir[108].

Bu olumsuzluklara rağmen, e-delil elde etme yöntemlerinin incelenen malzemenin içerik listesinin net bir şekilde sunulması, veri bütünlüğü kontrolünde kazanımlar sağlaması, analiz edilen cihazdaki verileri üretmek için kullanılan yazılımları göstererek konteksti açığa çıkarması ile sistem loglarına kolaylıkla erişilmesi gibi faydaları vardır[109]. Bu faydalarından kaynaklanıyor olacak ki,

---

104 Kirschenbaum vd., **a.g.e.**, s. 16

105 Özet değerlerinin kontrolünün, Türkçe literatürde de checksum olarak ifade edildiği görülmektedir. Bu yöntemde her bayt, 16 ya da 32 bitlik bir polinoma tabi tutulmakta ve oluşan değer, sonraki kontrollerde referans olarak kullanılmaktadır (Mazlum Yalçınkaya, **a.g.e.**, s. 17). Durum böyle olunca, bu ifadenin Türkçe'de "bit sağlaması" olarak kullanılabileceği düşünülmektedir.

106 Bu dosya sistemleri, sabit diskler üzerindeki verileri düzenlemek için kullanılan temel yapılardır (Dosya Yerleşim Tablosu - File Allocation Table (FAT32), Yeni Teknoloji Dosya Sistemi - New Technology File System (NTFS), Hiyerarşik Dosya Sistemi - Hierarchical File System (HFS) gibi).

107 Kirschenbaum vd., **a.g.e.**, s. 16.

108 Christopher Lee vd., **From Bitstreams to Heritage: Putting Digital Forensics into Practice in Collecting Institutions**, yayım yeri yok, BitCurator, 2013, s. 23-24.

109 **a.g.e.**, s. 17.

ABD'deki Sayısal Savunuculuk Birliği (National Digital Stewardship Alliance - NDSA) 2014 yılındaki programında uzun dönemli korunacak elektronik malzemelerin sayısının gittikçe arttığını belirterek bunların korunmasında e-delil elde etme yöntemlerinin kullanılabileceğini ifade etmiştir. Bunun için gerekli teknik altyapı ve kurumsal politikaların oluşturulmasına vurgu yapmıştır[110].

3.3.1.2. Arşivlerde Kullanımı

E-delil elde etme yöntemleri, adli vakaların yanı sıra arşivlerde de kullanılmaktadır. İngiliz Milli Kütüphanesi, Stanford Üniversitesi ve Danimarka Milli Arşivinde bulunan e-arşiv malzemeleriyle alakalı olarak bu yöntemlerden faydalanıldığı bilinmektedir. Bunların yanı sıra, söz konusu yöntemlerin belgeler daha arşiv malzemesi olmadan güncel dönemdeyken hatta üretilme safhasında kullanımına yönelik çeşitli yaklaşımlar geliştirilmiştir.

E-delil elde etme yöntemlerinin arşivlerde kullanıldığı kurumlardan biri olan İngiliz Milli Kütüphanesine bağış yoluyla gelen şahıs arşivlerinin elektronik ortamdaki özgünlüklerini korumak için denetim günlükleri, yazma koruması ve imaj oluşturmadan faydalanıldığı belirtilmektedir. Burada belgelerin oluşumundan son aşamasına kadar geçen zamandaki süreçte yapılan işlemleri gösteren aidiyet zincirinin kurulmasının gerekliliğine vurgu yapılmaktadır. Bunun için log kayıtları ve denetim günlüklerinden yararlanılabileceği ifade edilmektedir[111].

İngiliz Milli Kütüphanesinde analiz edilen bu malzemeleri aranabilir hâle getirmek için belgelerin bileşenleri korunarak replikaları yani nüshaları oluşturulmuştur. Bunun için dosya formatları değiştirilerek e-delil elde etme yöntemleri aracılığıyla keşfedilen üstveriler, malzemelere eklenmiş ve dizinleme yapılmıştır. Bu üstverilere, dosya yapısı ve malzemenin formatı, imzalar, tarih, erişim izinleri, özet değerleri, boyut ve saklama konumu örnek verilebilir[112]. Burada dosya

---

110 National Digital Stewardship Alliance [NDSA], **2014 National Agenda for Digital Stewardship**, s. 4, 17, (Çevrimiçi) https :// www. digitalpreservation. gov/ documents/ 2014 NationalAgenda.pdf, 5 Mart 2020.

111 Jeremy Leighton John, "Adapting Existing Technologies for Digitally Archiving Personal Lives: Digital Forensics, Ancestral Computing, and Evolutionary Perspectives and Tools", **5. International Conference on Preservation of Digital Objects**, 29-30 Eylül 2008, Londra, The British Library, 2008, s. 48-55, (Çevrimiçi) https :// ipres-conference. org/ ipres08/ ipres2008-proceedings.pdf, 28 Mart 2020.

112 **a.g.e.**

formatlarının değiştirilip, üstverilerin eklenmesi değişen her türlü donanım ve yazılım ortamında çalışabilirliği sağlamak hedefiyle gerçekleştirilmiştir.

Arşivlerde e-delil elde etme yöntemlerinden faydalanıldığı bir başka örnekle Stanford Üniversitesinde karşılaşılmaktadır. Elektronik ortamda üretilen bir koleksiyonun arşive dâhil edilmesi sırasında bu yöntemlerden faydalanıldığı görülmektedir. İşlemler sırasında Forensic Recovery of Evidence Device (FRED - Delil Elde Etme Aracı) cihazı kullanılmıştır. E-delil elde etme işlemleri için geliştirilen bu cihazın disk imajları oluşturulurken yazma koruma uygulamalarını kendiliğinden etkinleştirdiği ifade edilmektedir. Arşive gelen koleksiyondaki disk ve disketlerin imajının alınması sırasında e-delil elde etme için geliştirilen ve bütünlüğü korumada etkili olduğu bilinen "Forensic Toolkit Imager" (FTK - Delil Elde Etme Araç Seti) adlı program kullanılmıştır. FTK, aynı zamanda belge hiyerarşisini de gösterdiğinden belgelerin tasnifinde kolaylık sağlamaktadır. FTK'dan tasnifi yapılmamış e-belgelerin düzenlenmesinde de yararlanılabileceği ileri sürülmektedir[113].

Arşivlerde e-delil elde etme yöntemlerinin kullanıldığı bir diğer alan teknolojik göç ettirme işlemleridir. Bunlar aracılığıyla Danimarka Milli Arşivinde 200 farklı formattaki 11.187 malzeme için yeni arşiv bilgi paketi oluşturulmuş ve teknolojik göçleri gerçekleştirilmiştir. Thirifays, Nielsen ve Dokkedal'ın bu işlemi açıkladığı çalışmada, standart bir yapıya sahip olmayan eski veriyi göç ettirmenin standart olanlara göre 70 kat daha uzun sürdüğü belirtilmektedir. Söz konusu çalışmada, pro-aktif bir yaklaşımın, yani sık aralıklarla, formatların güncel kullanımını yitirmeden yapılan incelemelerin verimliliği sağlayacağı ifade edilmektedir. Aynı zamanda uzun vadeli olmayan yaklaşımların ve zamanında verilmeyen kararların ciddi zararlara yol açabildiği dile getirilmektedir[114].

E-delil elde etme yöntemleriyle arşivciler, saklama planları bağlamında ya da durumu netleşmeyen birtakım malzemenin sehven silinmesi durumunda bunların arşivlik değere sahip olup olmadığını kontrol edebilmektedir. Bu amaçla açık kaynak

---

113 Laura Wilsey vd., "Capturing and Processing Born-Digital Files in the STOP AIDS Project Records: A Case Study", **Journal of Western Archives**, C. 4, No: 1, 2013.

114 Alex Thirifays, Anders Bo Nielsen ve Barbara Dokkedal, "Evaluation of a Large Migration Project", **8. International Conference on Preservation of Digital Objects**, 1-4 Kasım 2011, ed.: Jose Borbinha vd., Singapur, yayımcı yok, 2011, s. 24, (Çevrimiçi) https :// services. phaidra.univie.ac.at/api/object/o:294293/diss/Content/get, 28 Mart 2020.

kodlu BitCurator adında bir yazılım oluşturulmuştur. BitCurator hazır bir yazılım olarak kurulduğu örgütün belgeleri için uygulanabileceği gibi, farklı örgütlere ait bilgisayarlarda ya da işletim sistemlerinde oluşturulan belgeleri incelemek için de kullanılmaktadır. Bu yazılımın e-belgelerin saklama ünitelerindeki konumlarını, dosya ve bit yapılarını gösterdiği ifade edilmektedir[115].

Bu programın yanı sıra belge hiyerarşisine göre düzenlenen belgeler, Forensic ToolKit adlı uygulamayla açığa çıkarılmaktadır[116]. Bir diğer e-delil elde etme yöntemi programlarından olan Fiwalk ise incelenen dosyaların XML formatında üstverilerini ortaya koymaktadır. Burada, dosya adı, boyutu ve formatı, değiştirme, erişim ve oluşturma tarihi, dizin ve özet değeri gibi üstveriler bulunmaktadır[117].

Her ne kadar, arşivlenen e-belgelerin delil değeriyle alakalı teknolojik koşullar değerlendirilmiş olsa da -belge süreklilik modelinde olduğu gibi- bu belgelerin taşıyıcı ortam olarak teknik yapısı, form özellikleri ve formatı arşive devredilmeden güncel dönemde oluştuğundan delil değeri konusunun belge üretilirken ele alınması gerektiğini düşünenler bulunmaktadır. Majore, Yoo ve Shon'un yaptığı bir çalışmada teknolojik göç sırasında yapılan işlemlerin birer üstveri olarak kurgulanabileceği belirtilmektedir. Bunlara teknolojik göçün gerçekleştirilmesinin ardından belgelerin yeni format yapılarıyla sisteme tekrar yüklenmesiyle oluşan özet değeri, teknolojik göçün yapıldığı tarihi gösteren zaman damgası ve belgenin konumu örnek verilebilir[118]. Ancak bu yöntemlerin belgelerin üretim aşamasında devreye alınmadığı görülmektedir. E-delil elde etme yöntemleri konusunda çalışmaları bulunan Thorsten Ries, bu yaklaşımlarla güvenilirliğin yeteri kadar başarılı korunamayacağını, bu nedenle EBYS'lerde kullanılacak delil elde etme yöntemlerinin belgeler üretilmeden devreye alınması gerektiğini ifade etmektedir[119].

---

115 Kam Woods, Christopher Lee ve Sunitha Misra: "Automated Analysis and Visualization of Disk Images and File Systems for Preservation", **Archiving 2013**, Washington[ABD], Society for Imaging Science and Technology, 2013, s. 239-240.

116 Niu, "Original Order in the Digital World", **a.g.e.**, s. 63-65, 70.

117 Kam Woods, Christopher Lee ve Simon Garfinkel vd., "Extending Digital Repository Architectures to Support Disk Image Preservation and Access", **Proceedings of the 11th Annual International Association of Computing Machinery (ACM)/IEEE Joint Conference on Digital Libraries**, Ontario[Kanada], ACM, 2011, s. 63.

118 Sekie Amanuel Majore, Hyunguk Yoo ve Taeshik Shon, "Next Generation Electronic Record Management Systems Based on Digital Forensics", **International Journal of Security and its Applications**, C. 7, No: 1, 2013, s.192.

119 Antwerp Üniversitesi öğretim üyesi Dr. Thorsten Ries ile 13 Şubat 2020 tarihinde yapılan görüşme.

Majore, Yoo ve Shon'un yaptığı başka bir çalışmada bu yönde bir yaklaşımın izleri görülmektedir. Önerilen sistemde, disk imajı oluşturma, imaj yükleme, nesne analiz etme, üstveri oluşturma ve üstveri veri tabanları bulunmaktadır. Arşivcilerin belgeleri analiz etmek için öncelikle disk imajı oluşturması gerekir. Bu disk imajı, belirli bir dönemde üretilen verilerin kopyası mahiyetindedir. Böylece, belgelerin orijinaline zarar verilmeden analiz yapılabilecektir. Disk imajının yüklenmesi aşamasında oluşturulan bu imaj, işletim sistemlerinde okunabilir hâle getirilir. Bu aşamada disk imajının ne zaman oluşturulduğu, sürücünün seri numarası, imajı oluşturan kişi gibi üstveriler üretilir[120]. Hâliyle bu üstverilerin güvenilirlik analizinde kullanılabileceği düşünülmektedir.

Analiz aşamasında ise belgenin adı, formatı, oluşturulma tarihi, belgede yapılan değişikliklerin tarihi, şifreli olup olmadığı ve orijinal konumu gibi bilgiler elde edilebilmektedir. Böylece, oluşturulan bu sistemde belgenin adı ve referans numarası, özet değeri, sisteme dâhil edildiği zaman, konumu ve formatı ile oluşturan, düzenleyen ve sorumlu gibi üstveriler üretilir. Oluşturulan bu üstveriler, veri tabanlarında yetkisiz değişime izin verilmeyecek bir şekilde saklanarak güvenilirlik analizinde kullanılabilir[121].

E-delil elde etme yöntemlerinin temel araçlarından olan imaj oluşturmanın amaçlarından biri, belgelerin üretildiği dönemdeki kontekstini koruma altına alıp herhangi bir kaybın önüne geçmektir. Belgeyi kim düzenlemiş ve ona kim erişmiş gibi sorulara cevap bulmak hedeflenir. Bununla birlikte, belgelerin ilk üretildikleri dosya sistemi de koruma altına alınmaktadır. Böylece, bir işletim sisteminde üretilen bir belgenin başka bir işletim sistemine aktarıldığında özniteliklerinin kaybolmaması sağlanabilir[122].

Disk imajlarında bir disk, olduğu gibi kopyalandığı için tek tek dosyalar, seriler ya da belgelerin konumlarının belirtildiği dizinler değil, fonun kendisi tüm özellikleriyle birlikte kopyalanmaktadır. Böylece provenansın tesis edilip belgelerin aidiyet zincirinin kurulmaya çalışıldığı söylenebilir[123]. Bununla birlikte, e-delil elde etme yöntemleri aracılığıyla farklı disklerde yer alan fakat birbiriyle arasında organik bir bağ

---

120 Majore, Yoo ve Shon, "Secure and Reliable Electronic Record Management System Using Digital Forensic Techologies", **a.g.e.**, s. 155-158.

121 **a.g.e.**, s. 158-159.

122 Kam Woods ve Christopher Lee, "Acquisition and Processing of Disk Images to Further Archival Goals", **Archiving 2012**, Springfield[ABD], Society for Imaging Science and Technology, 2012, s. 147-152.

123 Christopher Lee, "Archival Application of Digital Forensics Methods for Authenticity, Description and Access Provision, **Comma**, No: 2, 2012, s. 137.

bulunan belgelerin de tespit edilebildiği görülmektedir. Burada, e-delil elde etme yöntemleriyle arşivsel bağı tesis edilmeyen belgelerin organik bağı kurulabilir mi sorusu akla gelmektedir[124]. Bunun için sahada ciddi çalışmaların yapılması gerekmektedir.

3.3.1.3. Güvenilirlik için Delil Elde Etme

Elektronik ortamda belgeler yönetilirken yapılan her işlem, log kaydı oluşması gibi bir iz bırakır. E-delil elde etme yöntemleri de bu izleri takip ederek vakaları analiz eder. Söz konusu yöntemlerin bu özelliği, kendisinin e-belgelerin aidiyet zincirini korumak için kullanılabileceğinin ileri sürülmesine neden olmuştur[125]. Bundan dolayı, "1994 yılında Elizabeth Diamond, arşivciyi bir sayısal delil elde etme uzmanına benzetmiştir"[126]. E-delil etme yöntemlerinin güvenilirlikle olan ilişkisine, bu yöntemlerin diplomatik analizle harmanlanması, belgelerin güvenilirliğinin korunmasıyla olan alakası ve e-delile ilişkin proje ve prosedürler ışık tutmaktadır.

Corinne Rogers, e-delilin korunması, derlenmesi, doğrulanması, tanımlanması, analiz edilmesi, yorumlanması, dokümantasyonu ve sunulması için ortaya konulan bilimsel yöntemler olarak değerlendirdiği bu sayısal delil elde etme yöntemini diplomatik analize benzetmektedir[127]. Çünkü, e-delil elde etme uzmanları ile belge yöneticileri ve arşivciler, elektronik ortamdaki delillerden olan e-belgelerin konteksti, ait olduğu kaynağı ve diğer delillerle arasındaki ilişkisini sorgular. Hâliyle, diplomatiğin e-belgeleri analiz için kullandığı tarih, belgedeki kişiler, arşivsel bağ, teknolojik kontekst ve açıklamalar gibi üstverilerin e-delil elde etme uzmanları tarafından da değerlendirilebileceği görülmektedir[128]. ABD ve Avustralya'daki farklı üniversitelerin oluşturduğu konsorsiyumun e-arşiv malzemelerinin e-delil elde etme yöntemleri marifetiyle yönetilmesi projesi olarak ortaya çıkan BitCurator ve daha çok Avrupa'daki bilgi merkezleri tarafından kullanılan açık kaynak kodlu delil elde etme yöntemleri yazılımı olan Archivematica gibi uygulamalar da diplomatik analiz ve e-

---

124 Lee vd., **a.g.e.**, s. 32.

125 Kirschenbaum vd., **a.g.e.**, s. 31. ; Lee vd., **a.g.e.**, s. 4, 9.

126 Çiçek ve Sağlık, "E-Belgelerin Arşivsel Bağının Elektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme", **a.g.e.**, s. 268.

127 Rogers, "Diplomatics of Born-digital Documents: Considering Documentary Form in a Digital Environment", **a.g.e.**, s. 9.

128 **a.g.e.**, s. 9-10, 15.

delil elde etme yöntemlerini kullanmaktadır[129]. Dolayısıyla belirtilen yöntemlerin birlikte kullanılmasıyla e-belgelerin güvenilirliğinin korunmasında yeni yaklaşımlar sağlanabilir.

E-delil elde ederken delilin bütünlüğü, özgünlüğü, gerçekliği, tamlığı ve kullanılabilirliğinin analiz edilmesi için değerlendirilen yöntemlerden belgelerin güvenilirliği incelenirken de yararlanılabileceği düşünülmektedir. Mesela erişim kontrolleri, belgenin özniteliklerinin korunması, kim tarafından düzenlendiğini belirtmek ve bileşenlerin tam olduğunu göstermek için e-delil elde etme yöntemlerinden faydalanılabilir. Bütünlüğün ve gerçekliğin kontrolünde log kayıtları ve özet değerlerinden yararlanılırken, kullanılabilirlik için disk imajı almak gibi yöntemler benimsenebilir[130].

E-delil elde etme uzmanları, elektronik ortamdaki bir delilin bütünlüğünü, özgünlüğünü, gerçekliğini ve tamlığını incelemektedir. Arşivciler de kendilerine gelen bir malzemenin bütünlüğünü sorgular, özgünlüğünü analiz eder; gerçekliği ve tamlığını kontrol eder. Hâliyle, bu iki alanın yöntemlerinin bir arada değerlendirilebileceği düşünülmüş ve Elektronik Belgelerden Delil Elde Etme Projesi (The Digital Records Forensics Project) gerçekleştirilmiştir. Proje sonuçlarının açıklandığı makalede "e-belgelerin güvenilirliğinin korunmasında e-delil elde etme yöntemlerinden yararlanılabileceği" ifade edilmektedir[131].

Bu projenin yanı sıra kurumların e-delil elde etmeye yönelik prosedürler hazırladığı da bilinmektedir. Mesela Kuzey Karolina Eyaletinde (ABD) Adli Delil Analiz Laboratuvarının (North Carolina State Crime Laboratory) Belge ve Veri Yönetimi Prosedürü'ne göre adli bir davaya konu olan olayla ilgili elektronik ortamda oluşan vaka dosyalarında tarih, delili ileten/getiren kişi, örneklerin tanımlanması ve

---

129 E-delil elde etme yöntemlerini belgelerin güvenilirliğinin korunmasında kullanan BitCurator ve Archivematica gibi çeşitli uygulamalar ortaya çıkmıştır. Bunlar, Türkiye'de henüz pek görülemese de diğer ülkelerde kullanılmaktadır (**BitCurator Web Sitesi**, (Çevrimiçi) https :// bitcurator.net, 1 Ağustos 2020. ; **Archivematica Web Sitesi**, (Çevrimiçi) https:// www. archivematica.org, 1 Ağustos 2020).

130 Alastair Irons, "Computer Forensics and Records Management: Compatible Disciplines", **Records Management Journal**, C. 16, No: 2, 2006, s. 107-109.

131 Luciana Duranti ve Corinne Rogers, "Memory Forensics: Integrating Digital Forensics with Archival Science for Trusting Records and Data", **eForensics Magazine**, C. 2, No: 15, 2013, (Çevrimiçi) https :// www. academia. edu/ 11328085/ Memory_ Forensics_ Integrating_ Digital_ Forensics_with_Archival_Science_for_Trusting_Records_and_Data, 29 Mart 2020.

gerekli analizin türü, başlangıç ve bitiş tarihi, sonucu, gerçekleştirilmesinden sorumlu birim ve kişiler, kullanılan teknikler, yöntemler ve uygulanan kalite kontrolü gibi bilgilerin bulunması gerekir[132]. Buradaki bilgilerin e-belgeler için de kullanılan üstverilere benzerlik gösterdiği düşünülmektedir. Belgedeki tarih, gönderen ve alıcı, faaliyetten sorumlu birim ve kişiler, güvenilirliğin onaylanmasında kullanılan teknik ve yöntemler ile güvenilirlik onayına dair kontroller bunlara örnek verilebilir. Öyle anlaşılıyor ki belgelerin kaynağının belirlenmesini sorgulayan arşivciler ile elektronik ortamdaki delilleri analiz eden e-delil elde etme yöntemi uzmanlarının ortaklaşa çalışması, güvenilirliğin başarıyla korunmasında önemli kazanımlar sağlayabilir.

3.3.1.4. Güvenilirliğin Korunması Faktörleri

3.3.1.4.1. Delil Formatları

E-delil elde etmede başvurulan yöntemlerden biri belgelerin saklandığı sürücülerin imajının alınmasıdır. Oluşan imaj dosyaları, sürücülerin birebir kopyası yani nüshasıdır. İmaj oluşturulduktan sonra delil elde etme uzmanı, orijinal dosya ile değil imaj dosyası ile çalışır. İmaj dosyası oluşturularak mevcutta var olan dosyaya herhangi bir veri ya da belge eklenmesi veya çıkarılması engellendiğinden, aynı zamanda olası değişikliklerin önüne geçilerek bütünlüğün korunması hedeflenir. Ancak, bütünlüğün korunması için imaj dosyasının ilk oluşturulan özet değeriyle sonradan yapılan kontrollerdeki özet değerinin örtüşmesi gerekir. Örtüşme sağlanmazsa belge tahrif mi edilmiş, yetkisiz değişimlere mi uğramış gibi şüpheler oluşabilecek ve güvenilirliği sorgulanabilecektir[133].

Bu sorunlardan dolayı belgelerin özniteliklerinden şüphe duyulmaması için çeşitli önerilerin dile getirildiği görülmektedir. Bunlar, bulanık özet değerinin kullanılması, belgelerin hata düzeltme kodlarıyla birlikte saklanması, özet değerleri kontrolünün otonom araçlarla yapılmasıyla İleri Seviye Delil Formatı (Advanced Forensics

---

132 North Carolina State Crime Laboratory, **Procedure for Record and Data Management**, North Carolina, ABD, 2013, s. 2, (Çevrimiçi) http :// www. ncids. com/ forensic/ labs/ Lab/ Policy/ Record-and-Data-Management-10-31-2013.pdf, 6 Aralık 2019.

133 Lee vd., **a.g.e.**, s. 1-2. ; Ancak, bu problemler yaşanmasa da sabit disklerin yapısının bozulması nedeniyle zaman içerisinde özet değerlerinin örtüşmemesi riskiyle karşılaşılmaktadır. Çünkü delillerin saklandığı sabit ve optik diskler, bitleri bölümlendirilmiş alanlarda (sektör) muhafaza ederler. Mesela sabit sürücüler, 512 bitlik sektörleri, optik sürücüler de 2048 olanları barındırır (Murat Özbek, **a.g.e.**, s. 260).

Format - AFF) ve Elektronik Delil Elde Etme Genişletilebilir İşaretleme Dili (Digital Forensics XML - DFXML) gibi yapılardan yararlanılması olarak öne çıkmaktadır.

E-delil elde etme yöntemlerinin arşivlerde kullanımı üzerine çalışmaları bulunan Spencer, özet değerlerinin uyuşmamasına bir çözüm olabilmesi amacıyla fuzzy hashing denilen bulanık özet değerinin kullanılabileceğini ifade etmektedir. Bu yöntemde, özet değerleri her bir bit satırı için oluşturulduğundan birbirinden farklı özet değerlerine sahip olan dosyaların benzerlikleri ortaya konulabilmektedir[134]. Böylece özet değerlerinin kontrolü daha sağlıklı bir sonuç verebilir.

Bursa Uludağ Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyesi Prof. Dr. Ahmet Emir Dirik, belge ve üstverilerin bir nesnedeki bit değişikliklerinin tespit edilmesini mümkün kılan "hata düzeltme kodlarıyla (error correcting code - ECC)" birlikte saklanması yönünde bir öneri getirmektedir. Hâliyle bir belgede değişiklik varsa onun nerede olduğu görülebilecektir[135]. Belge yönetimi konusunda saha çalışmaları bulunan Carol Kussmann ise belgelerin ilk alınan özet değerinin korunması için bu kontrolü otomatik olarak gerçekleştiren araçların kullanılmasını önermektedir[136].

Bu önerilerin yanı sıra, e-delil elde etme yöntemleri kullanılırken AFF ve DFXML'den de yararlanılabilir. İmaj verileri ve üstverilere ait e-imzaları içeren AFF, satır satır özet değeri oluşturup bunları ayrı bir dosyada saklamakta; birbirinin aynısı olan verileri göstermektedir[137]. AFF'nin yanı sıra analiz işlemlerinde incelenen diskteki veriler, DFXML formatındaki dosya yapılarıyla birlikte elde edilmektedir. Bu dosya yapısı, XML'e dönüştürülerek disk bölümlerinin yapıları, izinler, zaman damgaları, dosya özet değerleri ve silinen verilerle ilgili bilgiler incelenebilir[138].

---

134 Spencer, **a.g.e.**, s. 82-83.

135 Bursa Uludağ Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyesi Prof. Dr. Ahmet Emir Dirik ile 5 Aralık 2017 tarihinde yapılan görüşme.

136 Carol Kussmann, "Checksum Verification Tools", **Practical E-Records: Software and Tools for Archivists**, (Çevrimiçi) https://e-records.chrisprom.com/checksum-verification-tools, 16 Ekim 2019. ; Minnesota State Archives, **Center for Archival Resources on Legislatures**, (Çevrimiçi) http :// www. mnhs. org/ preserve/ records/ legislativerecords/ carol/ preservation. php, 16 Ekim 2019. Bu önerilere rağmen Frederick Cohen, farklı tarihlerde alınan özet değerlerinin örtüşmesinin her zaman belgenin bütünlüğünün korunduğunu göstermeyebileceğini ifade etmektedir. Çünkü elektronik ortamlarda bir bit yapısının aynısını yapmak mümkün olduğundan, bu yapının bozulmamasının belgenin değiştirilmediği anlamına gelmediğini ileri sürmektedir (Cohen, **a.g.e.**, s. 31-34).

137 Simon Garfinkel, "Providing Cryptographic Security and Evidentiary Chain-of-Custody with the Advanced Forensic Format, Library, and Tools", **International Journal of Digital Crime and Forensics**, C. 1, No: 1, 2009, s. 10-11.

138 Woods, Lee ve Misra, **a.g.e.**, s. 239-240.

AFF dosyası oluşturulduktan sonra döküm listesi mahiyetinde çıktı meydana getirilerek İleri Seviye Delil Formatı Listesi (Advanced Forensics Format Bill of Materials - AFFBOM) dosyası oluşturulur. XML veri yapısındaki bu dosya, belgelerin imzalandığı tarih, kullanılan e-imza sertifikası, notlar ve AFF dosyasındaki elemanları içermektedir. AFF ve AFFBOM'un aidiyet zincirine ilişkin önemli bilgiler sunduğu değerlendirilmektedir. Bununla birlikte, AFFBOM'da yer alacak bilgiler duruma göre zenginleştirilebilir. İmzalanan ama imaj dosyasında yer almayan, imzalanmayan ama imaj dosyasında yer alan, imzası doğrulanamayan ve düzeltilen bölümler de AFFBOM dosyasında yer alabilir[139].

AFFBOM, aynı zamanda şifrelemeyi de mümkün kılmaktadır. Buradaki şifreleme şemaları üç katmandan oluşur. Bunlar, içeriğin şifreleri, anahtar parola şifreleri ve açık anahtar şifreleridir. Ancak Garfinkel, bu katmanları AFF dosyalarının 32 bitlik içerikleri şifreleyememesi nedeniyle AFF'nin geliştirilmesi gereken yönleri olarak değerlendirmektedir. Bundan dolayı yapılan işlemlerin dokümantasyonunun oluşturulmasını önermektedir[140].

Bir döküm listesi mahiyetinde olan AFFBOM, hem belgenin kendisi hem de e-imza içerdiğinden EYP'ye benzetilebilir. Ancak, hem EYP'nin dosya kodu gibi güvenilirliğin kritik aracı olarak değerlendirilebilecek üstverileri zorunlu tutmaması hem de AFFBOM'un güçlendirilmeye ihtiyaç duyan şifreleme mekanizması nedeniyle ikisinin de geliştirilmeye açık yönleri bulunmaktadır. Buna rağmen zenginleştirilerek kullanılacak EYP, e-delil elde etme yöntemleri aracılığıyla şifrelemeyle ilgili zayıflıkları çözülen AFFBOM gibi kurgulanabilir. Böylece güvenilirliğin korunmasında daha güçlü bir karine elde edilebilir.

AFF'nin yanı sıra öne çıkan bir diğer format olan DFXML, disk bölümlerinin yapıları, izinler, zaman damgaları, dosya özet değerleri ve silinen verilerle ilgili bilgilerin analiz edilmesine imkân tanıdığından bunların belgelerin kontekstine nasıl katkı yaptığı incelenebilir[141]. DFXML tanımlanan dosyaların disk imajındaki fiziksel konumlarını ve kriptografik özet değerlerini içerir. DFXML'nin verilerin oluşturulduğu ve

---

139 Garfinkel, "Providing Cryptographic Security and Evidentiary Chain-of-Custody with the Advanced Forensic Format, Library, and Tools", **a.g.e.**, s. 10-11, 16.

140 **a.g.e.**, s. 17-22.

141 Woods, Lee ve Misra, **a.g.e.**, s. 239-240.

kullanıldığı uygulamaları da gösterdiğinden provenansı açığa çıkardığı söylenebilir. DFXML dosyaları, diskin fiziksel karakteri, imaj oluşturma süreci, silinen ve silinmeyen tüm dosyalardan elde edilen üstverileri içermektedir. Bununla birlikte, kullanılan e-delil elde etme aracının adı, versiyonu, delillerin nerede ve ne zaman bir araya getirildiği, delilin bünyesindeki yazılım kütüphaneleri gibi üstverileri barındırır[142]. DFXML'nin bu zengin üstverileri, onların EYP'de de benimsenebileceğini düşündürmektedir. Belgenin üretildiği yazılımın adı, versiyonu, hangi bilgisayarda ve ne zaman düzenlendiği, uygulama yazılımındaki yazılım kütüphaneleri gibi üstveriler EYP'de yer alabilir.

3.3.1.4.2. Yazılımın Korunması

E-delil elde etme yöntemi olarak yazılımlar korunurken öykünme ile kaynak kodlarını muhafaza etmenin öne çıktığı görülmektedir[143]. Kaynak kodlarında bu kodların arşivlenmesi tercih edilmekteyken, öykünmede elektronik ortamdaki bir malzemenin ilk üretildiği hâlinin korunması için kopyalama yapılmaktadır. Mesela uygulama yazılımlarının güncel olmayan fakat yazılımın üretildiği tarihte kullanılan bir işletim sisteminde açılmasında, bilgisayar oyunlarının çalıştırılmasında öykünme işlemleri yapılır[144].

Öykünme işlemlerinin bilgi taşıyıcıları için de benimsenebileceği görülmektedir. Örneğin bir belgenin üretildiği orijinal ortam, yazılım, kullanılan kütüphaneler ve uygulamalar gibi koşullar muhafaza edilerek belgenin ilk üretildiği hâli korunabilir[145]. O hâlde, öykünme aracılığıyla da belgelerin üretildiği sistemlerin bütünlüğü kontrol edilebilir[146]. Bu nedenle güvenilirlik, e-belgelerin üretildiği yazılımın kopyalanmasıyla sağlanabilir.

---

142 Buradaki diğer üstveriler şöyle belirtilebilir: Kullanılan e-delil elde etme aracının adı, versiyonu, nerede bir araya getirildiği ve bünyesindeki kütüphaneleri, delil elde etme işlemlerinin yapıldığı bilgisayarın adı, programın çalıştığı zaman ve kullanılan kütüphaneler, dışarı aktarılan bilgilerin nasıl aktarıldığı ve fiziksel olarak nerede saklandığı, bit dizilerinin kriptografik özet değerleri ve delil elde etme işlemi için faydalı olabilecek işletim sistemi bilgileri (Simon Garfinkel, "Digital Forensics XML and the DFXML Toolset", **Digital Investigation**, No: 8, 2012, s. 161, 162, 166, 172).

143 Software Preservation Network, **Emulation-as-a Service Infrastructure**, (Çevrimiçi) https :// www.softwarepreservationnetwork.org/eaasi/, 29 Mart 2020.

144 Harvey ve Weatherburn, **a.g.e.**, s. 123-124.

145 Klaus Rechert, Isgandar Valizada ve Dirk von Suchodoletz, "Future-Proof Preservation of Complex Software Environments", **9. International Conference on the Preservation of Digital Objects**, 1-5 Ekim 2012, ed.: Reagan Moore, Kevin Ashley ve Seamus Ross, Toronto[Kanada], University of Toronto, 2012, s. 180.

146 Zahra Tarkhani, Geoffrey Brown ve Steven Myers, "Trustworthy and Portable Emulation Platform for Digital Preservation", **14. International Conference on Digital Preservation**, 25-

Her ne kadar Duranti bu işlemlerin yeteri kadar güvenilir olmadığını ifade etse de Yale Üniversitesinin sayısal koruma uzmanlarından Euan Cochrane öykünmenin güvenilirliğin korunmasında oldukça sağlıklı sonuçlar verebileceğini ileri sürmektedir[147]. Cochrane'in geliştiricileri arasında yer aldığı Stabilize programıyla teknolojik göç ettirmeye ihtiyaç duyulmadığı ifade edilmektedir[148]. Hâl böyle olunca, öykünmenin gerçek senaryolar üzerinde denenerek e-belgelerin güvenilirliğine etkisinin anlaşılması hususu önemli bir araştırma konusu olabilir.

E-delil elde etmede öykünme kadar ölçülebilir sonuçlara ulaşmaya yarayan bir uygulama da yazılımlara ait kaynak kodlarının arşivlenmesidir. Yazılımlarda oluşan belgelere erişmenin en önemli koşullarından biri, belgelerin insanlar tarafından anlaşılabilir olmasıdır. Bunun için yazılımlar endüstriyel standartlara uygun kaynak kodlarıyla geliştirilmelidir. Bir uygulama yazılımının zaman içerisinde kullanımının devam edebilmesi ve geliştirilebilmesi için kaynak kodlarının muhafazası önemlidir. Bundan dolayı, bir yazılımın geliştirme geçmişini gösteren bu kodların arşivlenmesi gerekir[149].

Her ne kadar kaynak kodlarının saklanmasına yönelik GitHub[150] ve SourceForge[151] gibi platformlar mevcut olsa da bu platformlarda kaynak kodlarını uzun dönemli korumaya yönelik bir yaklaşımın yeteri kadar bulunmadığı gözlenmektedir. Bu amaçla geliştirilmesi hedeflenen Google Code[152] ve Gitorious[153] gibi projelerin de artık yaşamadığı bilinmektedir. Durum böyle olunca, kaynak kodlarını muhafaza etmenin yanı sıra onları uzun dönemli koruyan bir yaklaşımın da

---

29 Eylül 2017, Kyoto[Japonya], (Çevrimiçi) https :// ipres2017. jp/ wp-content/ uploads/ 30. pdf, 1 Ocak 2020.

147 Öykünme işleminin tartışmalı bir husus olduğu görülmektedir. Euan Cochrane, herhangi bir sayısal verinin delil değerinin korunması için bu işlemlerin yasal olarak zorunlu kılınmasını önermekteyken, Luciana Duranti, öykünüm işlemlerinin sağlıklı sonuçlar vermediğini ifade etmektedir (30 Ağustos 2018 tarihinde Yale Üniversitesi Kütüphanesi Sayısal Koruma Müdürü Euan Cochrane ile yapılan görüşme; 1 Eylül 2018 tarihinde INTERPARES Direktörü Luciana Duranti ile yapılan görüşme).

148 **Stabilize Web Sitesi**, (Çevrimiçi) https://www.stabilize.app/, 5 Haziran 2020.

149 Roberto Di Cosmo ve Stefano Zacchiroli, "Software Heritage: Why and How to Preserve Software Source Code", **14. International Conference on Digital Preservation**, 25-29 Eylül 2017, Kyoto[Japonya], yayımcı yok, 2017 (Çevrimiçi) https :// ipres2017. jp/ wp-content/ uploads/ 19Roberto-Di-Cosmo. pdf, 31 Aralık 2019.

150 **GitHub Web Sitesi**, (Çevrimiçi) https://github.com/, 5 Haziran 2020.

151 **SourceForge Web Sitesi**, (Çevrimiçi) https://sourceforge.net/, 5 Haziran 2020.

152 Google, **Google Code Web Sitesi**, (Çevrimiçi) https://code.google.com/archive/, 5 Haziran 2020.

153 UNESCO, **Software Heritage Web Sitesi**, (Çevrimiçi) https :// www. softwareheritage. org/ 2016/ 07/ 21/ gitorious-retrieved/, 5 Haziran 2020.

ortaya konmasına ihtiyaç duyulmuştur. Bu amaçla Software Heritage platformu geliştirilmiş ve açık kaynak kodlu bir arşivleme yazılımı oluşturulmuştur. Burada, kaynak kodlarının bütünlük kontrolü için tek biçim tanımlayıcılar ve SHA1 gibi algoritmalar kullanılmaktadır. Kaynak kodlarının provenans bilgisi için her koda bir tekbiçim kaynak tanımlayıcı (Unique Resource Locator - URL) verilmekte, özet değeri satır satır oluşturulmakta ve dizini tanımlanmaktadır. Aynı zamanda, geliştirilen yeni versiyonlar ve yapılan güncellemeler birer üstveri olarak kaydedilmekte ve yayınlanan son hâlleri, adı, versiyonu, yayınlama mesajı ve kriptografik imzalarıyla birlikte muhafaza edilmektedir[154]. Bununla birlikte, kaynak kodunun GitHub URL'si ve kodların konumu ile ait olduğu projeler gibi hususlar birer provenans bilgisi olarak tutulmaktadır[155].

Yeni yazılımlara ait kaynak kodlarının sisteme dâhil edilmesinde GitHub gibi kimi listeleme ve yükleme servislerinden faydalanılırken SHA1'in yanı sıra SHA256 algoritması da kullanılmaktadır. Aynı zamanda BLAKE2[156] sağlama toplamının kullanılması için de çalışmalar yapılmaktadır. Kaynak kodları, birbirinin aynası olacak şekilde disklerde en az 3 kopya saklanmakta ve otomatik olarak özet değeri kontrolü yapılmaktadır[157].

Kaynak kodları, bir yazılımın nasıl geliştirildiğini gösteren temel araçlardan biridir. Aynı zamanda yazılımın ne şekilde kullanılması gerektiğini açıklar. Bundan dolayı uygulama yazılımının doğru çalıştırılıp çalıştırılmadığı değerlendirilerek e-belgelerin güvenilirlik analizi yapılabilir. Ancak analiz sırasında kritik roller üstlendiği düşünülen bu kodların muhafazası ihmal edilen konulardan biridir. Türkiye'de bu kodların arşivlenmesine yönelik ulusal bir politika eksikliği bulunmaktadır.

Tüm bu açıklamalardan, e-delil elde etme yöntemlerinin belge yönetimi ve arşivcilikte uzun dönemli koruma uygulamasını değiştirebileceği söylenebilir. Çünkü halen birçok EBYS'de koruma için tercih edilen FRED gibi cihazları kurup işletmek örgütler için oldukça maliyetlidir. Bundan dolayı daha az maliyetli araç arayışlarının olduğu bilinmektedir. E-delil elde etme yöntemlerinin uygulanması şu an için ciddi yatırımlar gerektirse de ilerleyen yıllarda teknolojinin gelişmesiyle maliyetler düşebilir. Aynı zamanda belge yöneticisi ve arşivciler disk imajı, kriptografik özet

154 **a.g.e.**

155 **a.g.e.**

156 BLAKE, bir özet değeri algoritmasıdır. BLAKE2, BLAKE3, BLAKE-256, BLAKE-512 gibi türleri bulunmaktadır (**Blake Web Sitesi**, (Çevrimiçi) https://www.blake2.net/, 5 Haziran 2020).

157 **a.g.e.**

değeri, dosya yapıları, öykünme ve kaynak kodlarının korunması gibi konularda yetkinlik sahibi olmalıdır. Saha uzmanlarını yetiştiren eğitim müfredatları, bu yetkinlikleri kapsayacak şekilde güncellenmelidir[158].

3.3.2. Blokzincir Teknolojisi

3.3.2.1. Gelişimi

E-belgelerin güvenilirliğinin korunmasında kullanılan yöntemlerden biri de dağıtık defter teknolojisidir (DDT). Dağıtık defter, bir ağdaki katılımcılar tarafından bağımsız olarak tutulan ve güncelleştirilen bir veri tabanıdır. Buradaki kayıtlar, merkezi bir makam tarafından üretilmeyip, ağdaki katılımcıların oluşturdukları düğümler tarafından meydana getirilir ve saklanırlar[159]. DDT'de merkezi bir otoriteye ihtiyaç duyulmadan belgeler saklanabildiğinden bu teknoloji internetin keşfinden sonraki en önemli gelişmelerden biri olarak kabul edilmektedir[160].

DDT'de belge üretimi aşamaları şu örnekle açıklanabilir. Bakanlık, valilik ve kaymakamlığın yer aldığı bir süreçte oluşan belgeler defterlere kaydedilir ve bunlar her kurumun kendi ağında birebir kopyaları üretilerek saklanır. Görüldüğü üzere burada merkezi bir yapı mevcut değildir. Üretilen yeni bir belge, kararlaştırılan kurallar çerçevesinde her katılımcının veri tabanına kaydedilir[161].

Üretilen bu belgelerin güvenilirliğinin nasıl sağlanacağı sorusu üzerine ise belgelerin kriptoloji kullanılarak şifrelendiği blokzincir teknolojisi geliştirilmiştir[162]. Bu teknolojide işlem oluşturma aşamaları şöyle gösterilebilir[163]:

---

158 Lee, **a.g.e.**, s. 139.

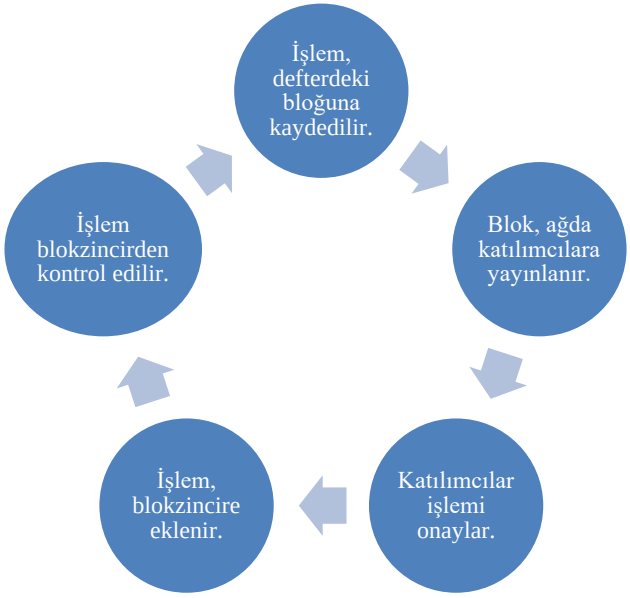
159 Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e**., s. 143.

160 Deloitte, **Blokzincir Potansiyelinin Keşfi: 2018 Yılı Türkiye Blokzincir Araştırması**, (Çevrimiçi) https:// www2. deloitte. com/ content/ dam/ Deloitte/ tr/ Documents/ consulting/blokzincir-potansiyelinin-kesfi.pdf, 15 Nisan 2020. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 143.

161 Nicholas Buchmann vd., "Enhancing Breeder Document Long-Term Security Using Blockchain Technology", **41. International Computer Software and Applications Conference**, yayım yeri yok, IEEE, 2017, s. 745.

162 Birleşmiş Milletler, **The Future is Decentralised**, s. 5-6, (Çevrimiçi) https:// www. unds. org/ content/undp/en/home/librarypage/corporate/the-future-is-decentralised.html, 30 Mart 2020.

163 Satoshi Nakamoto, **Bitcoin: A Peer-to-Peer Electronic Cash System**, 2008, (Çevrimiçi) https ://bitcoin.org/bitcoin.pdf, 16 Haziran 2019. ; Ahmet Sayarlıoğlu, **Herkes için Blok-zincir**, (Çevrimiçi) https:// medium. com/ @ahmet. sayarlioglu/ herkes-i%C3%A7in-blok-zincir-blokchain-1c85eb3a0bee, 30 Mart 2020. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 145.



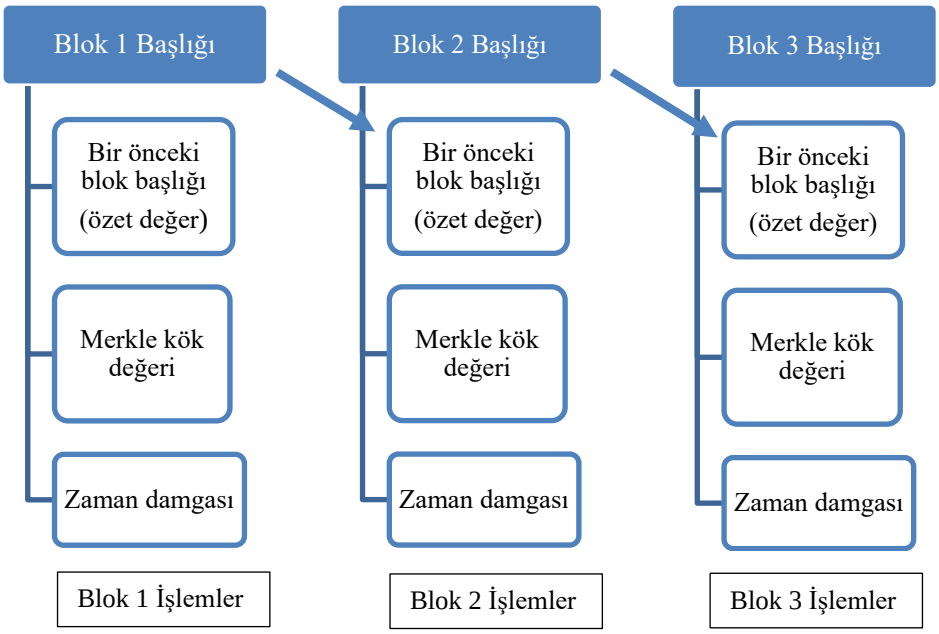
Şekil 3. Blokzincirde İşlem Oluşturma Süreci

Blokzincir teknolojisinde belgelerin saklandığı yapılar, blok olarak adlandırılmaktadır. Bloklar birbiri ardına bir zincir halkası gibi eklenir ve blokzincirler oluşur. Zincirin oluşmasında ilk adım, yapılan işlemlerin kayıt defterindeki bir blok içerisine kaydedilmesidir. İkinci adımda bu blok, ağdaki katılımcılara yayınlanır. Üçüncü adımda katılımcılar, zaman damgalı e-imza ile işlemin doğruluğunu onaylarlar. Dördüncü adımda onaylanan işlemler, blokzincire eklenir. Son adımda ise ağdaki katılımcılar işlemin aşamalarını ve son durumu blokzincirden kontrol ederler.

Her blok, zaman damgası alarak oluşturulduğu ana dair tarih ve saat bilgilerini içerir. Böylece, her biri kendi imzasına sahip, belirli bir zamanda kaydı bulunan, arka arkaya dizilmiş veri bloklarından meydana gelen bir zincir oluşturulur[164]. Blokzincirin bu özelliği şöyle gösterilebilir[165]:

164 **a.g.e.**, s. 146.; Darra Hofman vd., "The Margin Between the Edge of the World and Infinite Possibility: Blockchain, GDPR and Information Governance", **Records Management Journal**, C. 29, No: 1-2, 2019, s. 248.

165 Victoria L. Lemieux, **Blockchain Technology for Recordkeeping Help or Hype ? Blockchain Technology for Recordkeeping**, Montreal[Kanada], Social Sciences and Humanities Research Council of Canada, 2016. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 146.



Şekil 4. Blok Yapısı

Bloklardaki belgelerin korunması için kriptografik özetleme ve zaman bilgisi kullanılmaktadır. Bloklar, kendi içerisinde üretilmiş veriler ve başlıktan oluşur. Blok başlığı bir önceki bloğa ait özet değeri, blok içerisindeki verilere ait Merkle kök değeri[166] ve zaman bilgisini içermektedir. Bu durumda, herhangi bir yerde yaşanabilecek değişiklikler diğerlerini de etkileyecektir. Hâliyle, blok içerisindeki belgelerin değişmesi için hem hedeflenen hem de ondan sonra gelen tüm bloklar tahrif edilmelidir. Bu ihtimal, teorik olarak mümkün olsa da uygulamada pek gerçekçi bulunmamaktadır[167].

3.3.2.2. Arşivlerde Güvenilirlik İlişkisi

Blokzincir teknolojisinin e-belge yönetimi ve arşivcilikteki kullanımı üzerine çalışmaları bulunan Victoria Lemieux, blokzincir teknolojisinin kullanıldığı belge yönetim ve arşiv sistemlerini üç türde sınıflamaktadır. Bunlar, ayna (mirror), sayısal

166 Verilerin birçok parçaya bölünüp, daha sonra bu parçaların özet değerlerinin oluşturulmasıyla Merkle kök değeri elde edilmektedir.

167 Igor Zikratov vd., "Ensuring Data Integrity Using Blockchain Technology", **20. Conference of Open Innovation Association**, ed.: Sergey Palandin, Saint Petersburg[Rusya], IEEE, 2017, s. 538. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 146.

belge (digital record) ve aidiyet (tokenized) blokzincirleri şeklinde ifade edilebilir[168]. Ayna türü blokzincirlerde, belgeler sayısal ya da fiziki şekilde mevcut olmakla birlikte, bloklar bu belgelerin özet değerlerinden oluşmaktadır. Bu türde, belgeler blokzincirlerde üretilmemekte, asıl belgelerin kriptografik yansımalarından meydana gelmektedir. Dolayısıyla Lemieux, bu türü ayna olarak nitelendirmiştir. Burada belgelerin hesaplanan özet değerleriyle blokzincirlere yüklenen özet değerlerinin karşılaştırılarak bütünlüğün korunup korunmadığı incelenmektedir. Eğer özet değerleri örtüşmezse belgenin bir değişikliğe uğramış olabileceği düşünülecektir. Estonya'da üretilen sağlık kayıtları, İngiliz Milli Arşivi tarafından yürütülen ARCHANGEL Projesi ve Hırvatistan'da e-imzaların sertifika bilgilerinin blokzincirlerde saklanması, ayna tipi blokzincirlere örnek verilebilir[169].

Sayısal belge türünde ise belgeler akıllı sözleşmeler olarak zincirlerde üretilmektedir. Bu tür, geleneksel e-belge üretiminden farklılık arz etmektedir. Örneğin bir diploma üretilirken öğrencinin mezun olma şartlarını sağladıktan sonra geliştirilen algoritma, onun bir dilekçe vermesine gerek kalmadan diplomaları hazırlama sürecini başlatarak diplomayı oluşturmaktadır. Benzer bir örnek, İsveç'teki tapu müdürlüklerinde uygulanmaktadır[170]. İşte bu tür adımlar takip edildiğinden sayısal belge türünü akıllı sözleşmeler olarak adlandırmanın daha gerçekçi olacağı düşünülmektedir. Ancak, akıllı sözleşmelerin geçerliliği henüz delil hukuku tarafından

---

168 Victoria L. Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation", **2017 IEEE International Conference on Big Data**, ed.: Nie Jian-Yun vd., Boston[ABD], IEEE, 2017, s. 2273. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 154.

169 Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation, **a.g.e.** s. 2271-2278. ; Bralic, Stancic ve Stengard, **a.g.e.** ; John Collomosse vd., "ARCHANGEL: Trusted Archives of Digital Public Documents", **Proceedings of the ACM Symposium on Document Engineering**, yayım yeri yok, ACM, 2018, (Çevrimiçi) https://arxiv.org/pdf/1804.08342.pdf, 1 Nisan 2020. ; Tu Bui vd., "ARCHANGEL: Tamper-proofing Video Archives Using Temporal Content Hashes on the Blockchain", **CVPR Blockchain Workshop**, 17 Haziran 2019, Long Beach[ABD], yayımcı yok, 2019, (Çevrimiçi) https ://arxiv. org/ abs/ 1904. 12059, 1 Nisan 2020. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 155-156.

170 Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation", **a.g.e.**, s. 2274. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 156.

kabul edilmemiştir. Çünkü burada betiklerin (script)[171] mi yoksa algoritmaların[172] mı belge olarak kabul edileceği yönünde bir belirsizlik mevcuttur[173]. Aynı zamanda akıllı sözleşmelerde kritik güvenlik açıklarının olduğu görülmüştür[174].

Akıllı sözleşmelerin yanı sıra arşivlerde aidiyet türü blokzincir uygulamalarıyla da karşılaşılmaktadır. Lemieux, bu tür için "tokenized" ifadesini kullanmaktadır. Burada bir varlığın blokzincir ağındaki aidiyeti söz konusudur. Sistemde sadece belgeler değil, araziler, içecekler, sanat eserleri ve mücevherler gibi nesneler, kripto varlıklarla ilişkilendirilerek bloklarda saklanmaktadır[175]. Durum böyle olunca, İngilizce karşılığı tokenized şeklinde zikredilen uygulamanın "aidiyet türü blokzincirler" olarak adlandırılmasının daha açıklayıcı bir ifade olacağı değerlendirilmektedir.

Brezilya'da bir eyaletteki tapu kayıtlarının yönetiminde bu tür bir blokzincir uygulaması görülmektedir. Burada araziler bir varlık olarak değerlendirilmektedir. Bu varlıklar ve onlarla ilgili işlemler blokzincir ağına kaydedilmektedir. Araziler, bloklarda bir varlığa dönüştürülerek alım-satımı kripto varlıklarla gerçekleştirilmektedir[176]. Fakat yetkililer, sistemi pahalı bulduğundan bu uygulamayı mevcut belgelerin yarısını dikkate alarak gerçekleştirmiştir[177].

---

171 Betik, yazılımların tüm kodlarını içeren kısımlardır. Programlama dili olarak da bilinir. Ancak her programlama dilinin betiği birbirinden farklılık gösterir.

172 İranlı matematikçi Harezmi tarafından geliştirildiği bilinen algoritmalar, bir problemi çözmek için kullanılan sınırlı adımlar dizisidir ve bilgisayarlardan çok daha eski ve geniş bir kullanıma sahiptir (Brian Christian ve Tom Griffiths, **Hayatımızdaki Algoritmalar: Günlük Kararların Bilgisayar Bilimi**, çev.: Ali Atav, 3. bs., Ankara, Buzdağı Yayınevi, s. 14).

173 Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation", **a.g.e.**, s. 2275. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 157.

174 Loi Luu vd., "Making Smart Contracts Smarter", **23. ACM Conference on Computer and Communications Security Hofburg Palace**, 24-28 Ekim 2016, Viyana[Avusturya], ACM, 2016, (Çevrimiçi) https://eprint.iacr.org/2016/633.pdf, 1 Nisan 2020. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 157.

175 Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation", **a.g.e.**, s. 2275. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 157.

176 Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation", **a.g.e.**, s. 2275-2276.

177 Daniel Flores, Claudia Lacombe ve Victoria L. Lemieux, **Real Estate Transaction Recording in the Blockchain in Brazil**, s. 10, (Çevrimiçi) http:// blogs. ubc. ca/ recordsinthechain/ files/ 2018/ 01/RCPLM-01-Case-Study-1_v14_English_Final.pdf, 1 Nisan 2020. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 158.

Aidiyet türünün yanı sıra arşivlerde görülen başka bir uygulama, blokzincir teknolojisinin sayısal koruma amacıyla kullanılmasıdır. Tataristan Cumhuriyeti'nde arşive devredilen e-belgeler, özet değerleri ve zaman damgaları oluşturularak blokzincir ağında saklanmaktadır. Böylece, belgelerin kriptografik olarak korunduğu ve bütünlüklerinin muhafaza edildiği kabul edilmektedir[178]. Lemieux, belge yönetimindeki blokzincir uygulamalarını üç türde derlemişti; Tataristan Cumhuriyeti'nde görülen bu yaklaşım neticesinde "sayısal koruma projesi olarak blokzincir uygulamasının dördüncü bir tür olarak değerlendirilebileceği düşünülmektedir"[179].

Blokzincir teknolojisinin arşivlerdeki bu kullanım şekilleri incelendiğinde, ondan e-belgelerin güvenilirliğinin korunmasında da yararlanılabileceği akla gelmektedir. Güvenilirliğin özgünlük, tamlık ve gerçeklik niteliklerinin sağlanmasıyla korunduğu göz önüne alındığında, blokzincir teknolojisinin özgünlüğün gereklerinden olan bütünlüğün korunmasında oldukça faydalı olduğu görülmektedir. Blok yapısının değiştirilememesi, bu teknolojinin güvenilirliğin korunmasındaki en önemli vaatlerinden biri olarak öne çıkmaktadır[180].

Bu teknolojide özgünlüğün bir diğer gereği olan tanımlamaya yönelik yaklaşımlar da görülmektedir. Tanımlama, belgelerin özniteliklerini belirterek onların diğerlerinden ayırt edilmesini hedefler. Bunun yöntemlerinden biri de belgelerin konteksti ile arşivsel bağının açığa çıkarılmasıdır. Blokzincir uygulamalarında, her bir belgenin özet değerine tekil bir numara verilerek denetim günlükleri ya da log kayıtları aracılığıyla belgenin ait olduğu kaynak gösterilebilmektedir[181].

Bir diğer yöntem ise aynı işlem ya da faaliyet sonucu oluşan belgelerin özet değerini bir üst belgede toplayarak tekrardan özet değeri oluşturmaktır. Ancak, bu yöntemde oluşan üst belgenin özet değeri, yapılan işlemlerin yer aldığı belgelerin özet

---

178 Albert Galiev vd., "Archain: A Novel Blockchain Based Archival System", **Proceedings of the 2nd World Conference on Smart Trends in Systems, Security and Sustainability**, Londra[Birleşik Krallık], yayımcı yok, 2019, s. 87. ; Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation", **a.g.e.**, s. 2277.

179 Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 158.

180 Lemieux, "Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework", **a.g.e.**, s. 41-48.

181 **a.e.**

değerlerini elediği için daha önce yapılan işlemlerin kimliği kaybolmuş olacaktır. Bu durumda üst belgeyi oluşturan belgeler ve bunların özet değerleri de kaybolmaktadır[182].

Blokzincir teknolojisinde merak edilen bir diğer husus, vaka dosyalarının nasıl oluşturulup korunacağıdır. Vaka dosyasını oluşturan iş devam ettikçe bloklara belgelerin kaydedilmesi de süreceğinden blokların nasıl şekillendirileceği henüz net değildir. Bu sorunu çözmek için OP_Return betik kodundan[183] yararlanılabileceği ve işlemlere ait üstverilerde kullanılabileceği ileri sürülmektedir. Blokzincirde vaka dosyası oluşturmak için bu betik kodun yanı sıra ontolojilerden ve tanımlamadan yararlanılabileceği görülmektedir. Çünkü ontolojiler arşivsel bağın kurulmasında önemli bir araçtır. Örneğin bir vaka dosyasındaki belgelerin ait olduğu iş, dosya ve seri bilgileri semantik etiket olarak bloklara eklenebilir. Böylece bloğun oluşturulması için vaka dosyasını meydana getiren işin bitmesi beklenmez[184]. Arşivsel bağın blokzincirlerde kurulmasında belgelerin üretildiği gibi tanımlanmasının da bir yöntem olarak benimsenebileceği ifade edilmektedir. Bu durumda belgelerin oluşumuna kaynaklık eden her işlem, tek bir özet değeri ile ilişkilendirilmektedir[185].

Blokzincir teknolojisinde özgünlüğün korunmasına yönelik bu yaklaşımların yanı sıra Estonya'daki uygulamada görülen[186] Merkle ağaç yapısı da dikkat çekmektedir. Bu yapıda en alttaki verilerden yukarıya doğru bir özetleme değeri üretilerek tüm yapı için bu değer oluşturulabilmektedir[187]. İşlem-faaliyet-iş-fonksiyon hiyerarşisi içerisinde belge-dosya-seri ve birim yapısındaki her belge için bir özetleme değeri oluşturulup,

---

182 **a.e.** ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 159-160.

183 Bu kod, kripto varlıkların alım-satımında geçersiz işlemleri belirtmek için işletildiği gibi küçük boyuttaki verileri blokzincirlere yüklemek için de kullanılmaktadır (Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation", **a.g.e.**).

184 **a.e.** ; Thomas Sodring, Petter Reinholdtsen ve Svein Olnes, "Publishing and Using Record-keeping Structural Information in a Blockchain", **Records Management Journal**, C. 30, No: 3, 2020, s. 335.

185 Darra Hofman vd., "Building Trust Protecting Privacy Analyzing Evidentiary Quality in a Blockchain Proof-of-Concept for Health Research Data Consent Management", **IEEE 2018 International Congress on Cybermatics**, 30 Temmuz-3 Ağustos 2018, ed.: Juan E. Guerrero, Halifax[Kanada], s. 1654-1655.

186 Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation", **a.g.e.**

187 Ahmet Usta ve Serkan Doğantekin, **Blockchain 101**, 2. bs., İstanbul, Bankalararası Kart Merkezi, 2018, s. 114.

belgelerin ait olduğu dosya için de bir özetleme yapısı geliştirilebilir. Kaynaklarda Merkle yapısına ilişkin şu öneri dile getirilmektedir[188]:

"Dosyaların ait olduğu seriler için de tek bir özetleme yapısı tesis edilebilir ve bu seriler de birimler çatısı altında birleştirilip tek bir özetleme değerine sahip olur. Bu birimler yine birleşerek kurumu oluşturur ve kuruma bir özetleme değeri tevdi edilebilir. Aynı zamanda Merkle ağaç yapısına arşivsel bağla ilgili ontolojilerin semantik bir etiket olarak eklenmesi kontekstin korunmasını sağlayabilir".

Özgünlüğün korunmasına yönelik bu uygulamalarla birlikte, güvenilirliğin bir diğer unsuru olan gerçekliğe yönelik yaklaşımların da blokzincirlerde tatbik edildiği görülmektedir. Belgenin gerçekliğinden bahsedebilmek için belgedeki kişi ile imzanın uyumlu olması gerekir. Başka bir deyişle belgenin düzenleyeni, onu düzenleme yetkisine sahip olmalıdır. Blokzincirlerde bu gereklilik, erişim yetkileriyle sağlanmaktadır. Yetkisi olmayan kişiler, belgeyi imzalayamamaktadır. Aynı zamanda mevcut blokzincir uygulamalarında bu gereklilik, belgedeki imzanın inkâr edilememesiyle karşılanmaktadır[189].

Blokzincir uygulamalarında belgelerin bir diğer güvenilirlik unsuru olan tamlığa ilişkin yaklaşımlara da rastlanmaktadır. Tamlık, veri üzerindeki teknik ve prosedürel denetimlere bağlıdır. Sistem kontrolleri ve denetim günlükleri ya da log kayıtları aracılığıyla tamlığı artırmak mümkündür. Blokzincirde daha sağlıklı bir kalite kontrolünün gerçekleşebileceği öngörülmektedir. Mesela, Brezilya'daki bir uygulamada, kâğıt ortamda olup elektroniğe aktarılan tapu kayıtlarının özet değeri oluşturulmuş ve blokzincirdeki kaydın özet değeriyle karşılaştırılmıştır. Özet değerlerinin örtüşmesiyle de blokzincire eklenen kayıtların tamlığı denetlenmiştir. Aynı zamanda bu denetleme işleminin yapıldığına dair bir üstveri, blokzincire kaydedilen belgeye eklenmektedir[190].

---

188 Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 161.

189 Hofman vd., "Building Trust Protecting Privacy Analyzing Evidentiary Quality in a Blockchain Proof-of-Concept for Health Research Data Consent Management", **a.g.e.**, s. 1653.

190 Jamie Berryhill, Theo Bourgery ve Angela Hanson, **Blockchains Unchained: Blockchain Technology and its Use in the Public Sector**, s. 18-19, (Çevrimiçi) https :// www. oecd-ilibrary. org/governance/blockchains-unchained_3c32c429-en, 30 Mart 2020. ; Çiçek ve Sağlık,

3.3.2.3. Güvenilirliği Tehdit Edebilecek Riskler

3.3.2.3.1. Arşivcilikle İlgili Riskler

Mevcut blokzincir uygulamaları değerlendirildiğinde bu teknolojinin arşivcilik ve belge yönetimi disiplinlerinin bakış açısıyla yeteri kadar yorumlanmadığı görülmüştür. Bu nedenle, geliştirilmesi gereken yönleri olduğu düşünülmektedir. Bunlar, kripto varlık olarak alınıp satılabilen protokollerin kullanılması, Bizans Generalleri Yöntemi'nin açıkları, işlemlerin gerçekleştiği tarihlerinin belirlenememesi olarak öne çıkmaktadır.

Belge yönetimi için geliştirilecek protokollerde Avax, Ethereum, Ripple gibi bir kripto varlık olarak alınıp satılabilen protokollere bağımlı olunmamasının gerekli olduğu düşünülmektedir. Çünkü piyasada paranın alınıp satılmasıyla ilişkili olan bu kripto varlıklarda yaşanabilecek düşüş ve yükselişler sistemin sürekliliğini olumsuz etkileyebilir. Bu sorun, Lemieux ve arkadaşlarının 2020 tarihli çalışmasında da dile getirilmektedir[191]. Aynı zamanda, OECD'nin toplu taşımada blokzincir teknolojisinin kullanımına dair hazırladığı raporda devletlerin kendi protokollerini hazırlaması önerilmektedir[192].

Tüm bunlarla birlikte, belgelerin bütünlüğü için kullanılan Bizans Generalleri Yöntemi'nin tekrardan kurgulanması gerektiği öne sürülmektedir. Bu yöntemde blokzincirdeki bir düğümün ağa ilettiği mesaj, bu mesajı alan ana düğüm ya da diğer düğümler tarafından yayınlanmaktadır. Yeterli sayıda düğümlerin mesajları doğrulaması neticesinde de işlemler onaylanmaktadır. Düğüm sayısı ne kadar fazlaysa belgelerin tahriften uzak olma ihtimali de o kadar yüksektir. Ancak, mesajı doğrulayan düğüm sayısı azsa bir saldırganın ağdaki işlemlerin doğrulanması aşamasında kontrolü ele geçirmesi ve belgelerin orijinalliğini tahrif etmesi olasıdır[193]. Hâliyle bu ihtimali azaltacak yöntemlerin geliştirilmesine ihtiyaç duyulmaktadır.

"Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 159.

191 Victoria L. Lemieux vd. "Caught in the middle? Strategic Information Governance Disruptions in the Era of Blockchain and Distributed Trust", **Records Management Journal**, C. 30, No: 3, 2020, s. 317.

192 OECD, **Blockchain and Beyond: Encoding 21st Century Transport**, OECD, International Transport Forum, 2018, s. 9.

193 Hofman vd., "Building Trust Protecting Privacy Analyzing Evidentiary Quality in a Blockchain Proof-of-Concept for Health Research Data Consent Management", **a.g.e.**, s. 1655. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 163.

Yukarıdaki sorunların yanı sıra blokzincir teknolojisinin e-belgelerin tamlığına zarar verebilme ihtimali söz konusudur. Blokzincirlerde her blok, çeşitli işlemlere ait özet değeri ve diğer bilgilerle birlikte bloğun belirli bir tarihten önce oluştuğunu gösteren zaman damgası içerir. Bazı sistemlerde, bloklardaki zaman damgaları, işlemlerin kronolojik sırasının ispatı için kullanılan jetonların üretimini de düzenleyebilmektedir. Böylece düğümler, yapılan işlemlerdeki ortalama zamana göre zaman damgasında yer alan tarih ve saat bilgilerini hesaplayabilmektedir. Blokzincir teknolojisinin sağlıklı çalışabilmesi ve zaman damgası hatalarının önlenmesi için tüm düğümler, önceki işlemlerin zamanını muhafaza etmelidir. Aksi takdirde zaman damgası, doğru tarihi göstermeyebilir. Bununla birlikte, düğümlerin normal koşullarda çalıştığı durumlarda bile ağ zamanının yavaşlatılma veya hızlandırılma ihtimali bulunmaktadır. Bu durumda zaman damgası sağlıklı sonuçlar vermeyebilir. Aynı zamanda bazı blokzincir ağlarında kontrolü tek bir düğüm ele alabilir. Ancak, bloklardaki hatalı veya istenmeyen işlemlerin düzeltilmesi mümkün olsa da söz konusu hatalı işlem geçersiz olacağından onun hatasını düzelten işlem de geçerli olmayacaktır. Bu sorunun aynı faaliyet ya da işlem kapsamında oluşan belgelere arşivsel bağ ile ilgili bilgilerin eklenmesiyle çözülebileceği ifade edilse de mevcut blokzincir uygulamalarının bu konuda yetersiz kaldığı belirtilmektedir[194].

Tüm bu açıklamalardan blokzincir teknolojisinin e-belgelerin güvenilirliğinin korunmasında kullanılması için geliştirilmesi gereken yönlerinin bulunduğu anlaşılmaktadır. Bu konular üzerine çalışılırken sadece arşivcilik ve belge yönetimi bakış açısının değil, mühendislik ve hukuk gibi disiplinlerin yaklaşımlarından da faydalanılmalıdır. Böylece, bu teknoloji kullanılarak e-belgelerin güvenilirliğinin korunmasına yönelik daha başarılı sonuçlar elde edilebilir.

3.3.2.3.2. Blokzincirin Yapısından Kaynaklanan Riskler

Blokzincir teknolojisinin güvenilirliği tehdit edebilecek blokların aidiyetini belirleyememeye neden olan çatallaşma ve yetim blokların oluşumu gibi bu teknolojinin kendi yapısından kaynaklanan riskleri bulunmaktadır. Bunların yanı sıra,

194 Lemieux, "Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework", **a.g.e.**, s. 46-47. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 159.

şifreleme algoritmalarının güncelliğini yitirmesi ve blokzincir sisteminin aşırı enerji tüketimi de diğer yapısal riskler arasında kabul edilmektedir.

Dağıtık ve merkezi olmayan büyük ölçekli bir blokzincir mimarisinde ağdaki her bir makinenin blok yapısının her zaman tutarlı olmayabileceği değerlendirilmektedir. "Sistem içerisinde yakın zamanlı paralel blok üretimi, blokların ağ üzerindeki makinelere farklı zamanlarda iletilmesi gibi nedenlerden dolayı ağa bağlı makineler üzerinde farklı blok sıralamasına sahip düğümlerin bulunması karşılaşılan bir durumdur"[195]. Bunun neticesinde ana blokzincir üzerinde çatallaşma oluşabilmekte ve ikincil zincirler doğabilmektedir[196]. Bir ikincil zincir, zamanla ana blokzincire dönüşürken, o esnada geçerli olan bu ilk ana blokzincir ise artık bir ikincil zincir olarak muamele görebilmektedir[197].

Bu riskin yanı sıra, yeni eklenecek blokların bağlı olduğu üst bloğun bulunamaması durumunda yetim bloklar üretilebilmektedir. Bunlar, genelde birbirini takip eden hızlı blok üretimi ve blokların ağ yapısındaki gecikmeler gibi nedenlerden dolayı ters sıralama ile makinelere varmasından dolayı oluşabilmektedir. Bu bloklar, genellikle üst blokları ilgili makineye gelinceye kadar makine üzerinde ayrı bir havuz yapısında tutulurlar[198]. Ancak, saha araştırmalarının yeterli olmamasından dolayı belge yönetiminde kullanılacak blokzincirlerde ikincil zincirler olacak mı, yetim blokların üretilmesi nasıl engellenecek gibi şüpheler henüz giderilememiştir. Bunlar, belgelerin güvenilirliğine yönelik riskler olarak değerlendirilmektedir.

Blokzincirlerin yapısından kaynaklanan diğer sorunlar, herhangi bir kişi ya da kurumun blokzincirdeki kayıtları tahrif etmesi, sistemin devamlılığının kim tarafından nasıl sağlanacağı, düğümler arasındaki blok farklılıklarında hangisinin delil olarak kabul edileceği[199], özel anahtarların kaybı ve hangi sayısal koruma teknolojisinin

---

195 Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 162.

196 Usta ve Doğantekin, **a.g.e.**, s. 126.

197 Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 162.

198 Usta ve Doğantekin, **a.g.e.**, s. 127. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 163.

199 Lemieux, "Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework",**a.g.e.**, s. 41-48.

kullanılacağı[200] şeklinde ifade edilebilir. Diğer taraftan, işlem performansının düşüklüğü, yüksek yatırım gereksinimi, güncelleme sonrasında eski versiyona sahip kullanıcıların yeni blokzincir ağı oluşturma ihtimali, 0 ve 1'lerden oluşan şifreleme algoritmalarının kuantum teknolojisiyle çözülebilme durumu önemli sorunlar arasında kabul görmektedir[201].

Bu risklere karşılık, İngiliz Milli Arşivinde blokzincir kullanımı üzerine araştırmalar yapan ekibin lideri Alex Green, mevcut şifreleme algoritmalarının geliştirilmesi yönünde çalışmaların olduğunu ifade etmiştir[202]. Sayısal koruma konusunda önemli yayınları bulunan David Rosenthal ise SHA256 algoritmasına dayanması, önerilen sistemlerde kripto varlık teşvikinin kullanılması, bu varlıkların sarf ettiği enerji miktarı gibi meselelerden dolayı blokzincir teknolojisinin sürdürülebilirliğinin kısıtlı olduğuna ilişkin şüphelerini dile getirmektedir[203]. Bu sorunlarla birlikte Lemieux, siber saldırıları blokzincir teknolojisi için risk olarak değerlendirmektedir[204].

3.3.2.4. Geliştirilmesi Gereken Noktalar

E-belgelerin güvenilirliğinin korunmasında hangi teknoloji kullanılırsa kullanılsın, belgenin yaşam döngüsündeki arşivsel bağın muhafazası için arşivcilik ve belge yönetimi bakış açısının her dönem (güncel, yarı güncel, arşiv) korunması gerekir. Bu durum, blokzincir teknolojisi için de geçerlidir. Her ne kadar bu teknoloji, belgelerin gereksiz yere çoğaltılmasını engelleyerek hangi belge sahihtir sorusunu ortadan kaldırsa da arşivsel bağın kurulması, belgelerin prosedürlere uygun biçimde üretilmesi, erişim yetkilerinin belirlenmesi, sayısal koruma sistemlerinin kullanılması ve belgelerin devlet arşivlerinin emanetine alınması gibi işlemler açısından geliştirilmesi gereken yönlerinin bulunduğu düşünülmektedir.

---

200 Lemieux, "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation", **a.g.e.**, s. 2277.

201 Usta ve Doğantekin, **a.g.e.**, s. 100-101. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 163.

202 Alex Green, **Trustworthy Technology: The Future of Digital Archives?**, 2018, (Çevrimiçi) https://blog.nationalarchives.gov.uk/trustworthy-technology-future-digital-archives, 1 Nisan 2020.

203 David Rosenthal, **Do You Need a Blockchain,** 2018, (Çevrimiçi) https:// blog. dshr. org/ 2018/ 02/do-you-need-blockchain.htm, 1 Nisan 2020. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 163.

204 Lemieux, "Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework", **a.g.e.**, s. 41-48.

Bir belgenin kuruma ait bir işlem neticesinde oluştuğunu kanıtlamanın yolu, onun aynı iş kapsamında üretilen diğer belgelerle arasındaki ilişkinin kurulmasıdır. Aynı faaliyet sonucunda oluşan belgelerin birbirleri arasındaki ilişki olan arşivsel bağ anlaşılmadan fonksiyon ortaya çıkarılamaz[205]. Kâğıt ortamdaki belgelerin daha çok dosya, fonksiyon, seri ve birimle münasebeti olarak bilinen arşivsel bağın, elektronik ortamdaki uygulamalar göz önüne alındığında korunup korunamadığı henüz yeteri kadar bilinememektedir. Durum böyle olunca, elektronik ortamda arşivsel bağın kurulup korunması için belgelerin ait olduğu işlem, faaliyet, iş ve fonksiyonla olan ilişkisinin kopmamasına dikkat edilmelidir[206].

Arşivsel bağla ilgili bu hususun yanı sıra sistemde belge üretimini kontrol etmek amacıyla kullanılacak, belgelerin fiziksel ve entelektüel formlarının tanımlanması için gerekli olan özellikleri inceleyen prosedürler devreye alınmalıdır. Çünkü belgelerin prosedürlere uygun olarak üretilmesi güvenilirliğin bir unsurudur[207]. Örneğin aynı tür ve kaynağa ait belgelerin form elemanlarının birbirine benzerlik göstermesi güvenilirliğin gereklerindendir. Bundan dolayı, form özelliklerini kritik ederek güvenilirliği değerlendiren diplomatik analiz yöntemlerinden faydalanılabilir. Ancak, blokzincirlerde belgelerin prosedürlere uygunluğunun nasıl sağlanacağı, diplomatik analiz yöntemlerinin nasıl kullanılacağı henüz belirgin değildir. Çünkü yeterli standartlaşma sağlanamamıştır[208].

Blokzincir sistemlerinde arşivcilik bakış açısıyla geliştirilmesi gereken bir diğer alan erişim yetkileridir. Burada kimlerin ne tür belgelerle işlem yapabileceği önceden belirlenmeli, uygulama sıkı bir şekilde takip edilmeli ve bunun aksine izin verilmemelidir. Çünkü, işlemlerin e-imza gibi anahtar yapılarıyla gerçekleştirildiği blokzincirlerde anahtara sahip olan kişiler, sadece o anahtara tanımlanan yetkileri gerçekleştirebilmektedir. Hâliyle, anahtar yönetimi, anahtarların değişimi, saklanması,

---

205 Hofman vd., "Building Trust Protecting Privacy Analyzing Evidentiary Quality in a Blockchain Proof-of-Concept for Health Research Data Consent Management", **a.g.e.**, s. 1654. ; Victoria L. Lemieux, "Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective", **European Property Law Journal**, C.6, No: 3, 2017, s. 392-440. ; Lemieux, "Trusting Records: Is Blockchain Technology the Answer?", **Records Management Journal**, C. 26, No: 2, 2016.

206 Hofman vd., "Building Trust Protecting Privacy Analyzing Evidentiary Quality in a Blockchain Proof-of-Concept for Health Research Data Consent Management", **a.g.e.**, s. 1654-1655.

207 **a.g.e.**, s. 1656.

208 Flores, Lacombe ve Lemieux, **a.g.e.**, s. 22.

kullanımı ve yenilenmesini içermelidir. E-imzalı belgelerin güvenilirliğinde kullanılacak blokzincir sistemi, bu anahtarların çalınmasına veya erişilememe durumuna karşı güçlü önlemlere sahip olmalıdır[209]. Böylece, belgelerin gerçekliği daha güçlü korunabilir.

Blokzincir teknolojisinin ilerleyen yıllarda daha çok kullanılabileceği tahmin edilmektedir. Hâliyle bu uzun vadeli kullanım beklentisi, sayısal koruma anlayışında da blokzincirlerden yararlanılabileceği fikrini gündeme getirmiştir. Çünkü belgelerin kullanım ömrünü artıracak güvenilir bir kontekst ve ortam sunmak için tasarlanmış faaliyetler olarak tanımlanabilecek sayısal koruma, bit yapısı ve semantik bütünlük, format ve ortam sürdürülebilirliği ile bilgi güvenliğini konu edinmektedir. Arşivsel bağın kurulmasıyla gösterilebilecek semantik bütünlük, belge tahrif olursa ortadan kalkacak ve belgenin geçmişteki olayların delili olma niteliği son bulabilecektir. Bit bütünlüğünün bozulması ise özet değerlerinin karşılaştırıldığı durumlarda problemli sonuçlar oluşturabilmektedir[210].

Belgelerin üretiminden iletilmesine, dosyalanmasından tasfiyesine kadar olan süreçlerde kullanılabilen blokzincir teknolojisinin milli arşivler tarafından da benimsenebileceğine ilişkin raporlarla karşılaşılmaktadır. Örneğin ABD Milli Arşivinin blokzincir teknolojisi kullanılarak belgelerin arşive devrine yönelik araştırmalar yaptığı görülmektedir. Bu konuda bir rapor hazırlanmıştır. Raporda, e-belgelerin güvenilirliğinin nasıl korunacağına ilişkin bir yaklaşım görülemese de bazı önemli sorular gündeme getirilmiştir[211].

"NARA, blokzincir ağında sadece belgelerin tasfiyesiyle görevlendirilmiş müstakil bir düğüm olarak mı yer alacak yoksa belgelere erişebilmek için blokzincirin bir parçası mı olacaktır? Bir kuruma ait bloklar, NARA'nın bloklarına transfer edilebilecek midir? Bir blokzincir ağındaki belirli kısımları transfer etmek mümkün olacak mıdır?"

Bununla birlikte, milli arşivlerin kendilerine devredilen belgelere ilişkin bilgileri blokzincirlerde görüp kontrol ederek daha şeffaf ve güvenilir bir yapının söz

209 Hofman vd., "Building Trust Protecting Privacy Analyzing Evidentiary Quality in a Blockchain Proof-of-Concept for Health Research Data Consent Management", **a.g.e.**, s. 1654-1655.

210 **a.g.e.**, s. 1655-1656. ; Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 164.

211 NARA, **Blockchain White Paper**, Washington[ABD], NARA, 2019, s. 10-11.

konusu olabileceği belirtilmektedir[212]. Bu aşamada milli arşivlerin rolü ne olacak, tüm kurumlar arşivlerin oluşturacağı blokzincir ağında mı belgelerini üretecek gibi soruların tartışılması gerekli görülmektedir.

Bu teknolojinin merkezi bir otoritenin kontrolünü gerektirmemesi nedeniyle alım satımdan evlenmeye kadar farklı işlemler için tasdik makamı olan noter ya da belediye gibi kurumlara eskisi kadar ihtiyaç duyulmayabileceği ifade edilmektedir. Fakat bu yaklaşımın tersine bir sonuç oluşturması da muhtemeldir[213]. Örneğin milli arşiv gibi otorite kurumlar süreci en baştan düzenleyebileceğinden blokzincirde belirli bir standartta belgeler üretilebilir. Hâliyle, bu teknoloji kullanılsa da süreci sürdürülebilir yönetmek için yetkili organların gerektiğinde müdahil olması beklenir. Tüm bu tartışmalara rağmen bu teknoloji ülkelerde elektronik arşivlemenin başarısına katkı yapabilir.

Blokzincirin arşivcilik ve belge yönetimi bakış açısıyla geliştirilmesinin yanı sıra, kullanılan protokollerin de gözden geçirilmesi gereklidir. Çünkü blokzincirde kripto varlık olarak da işlem gören Ethereum, LinkChain, Avax gibi protokoller kullanılmaktadır. Bu protokollerin uzun vadede ne kadar sürdürülebilir olacağı merak edilmektedir. Ayrıca, protokoller arası geçişlerde bu geçişin sorunsuz gerçekleşip gerçekleşmediği dikkatle incelenmesi gereken bir meseledir[214]. Bu nedenle açık kaynak kodlu protokollerin kullanılmasının gerekli olduğu değerlendirilmektedir.

3.3.3. Yapay Zekâ, Yapay ve Derin Öğrenme

3.3.3.1. Yapay Zekâ

3.3.3.1.1. Gelişimi ve Arşivlerde Kullanımı

Yapay zekâ, insanların çeşitli işlemleri üzerinde hiç düşünmeden gerçekleştirmelerini sağlayan yöntemlerden biridir. İnsanlar, düşünme eylemlerini yapay zekâlı araç ya da uygulamalara öğreterek önceden kendilerinin gerçekleştirdiği bazı işleri onlara devretmektedir. Yüzyıllarca devam eden çalışmalar sonucunda bir birikim oluşmuş ve Alan Turing bu birikimi makineler öğrenebilir mi sorusuyla değerlendirerek yeterli eğitim sonucunda makinelerin programlanabilir her süreci

212 Sodring, Reinholdtsen ve Olnes, **a.g.e.**, s. 337.

213 Çiçek ve Sağlık, "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **a.g.e.**, s. 166.

214 **a.e.**

öğrenip gerçekleştirebileceğini ifade etmiştir[215]. Belge yönetiminde görülebilecek yapay zekâ çalışmaları da bu bağlamda ele alınabilir.

Arşivcilik ve belge yönetiminde yapay zekânın kullanımına ilişkin çeşitli araştırmalar yapıldığı görülmektedir. Bu araştırmalarda yapay zekâdan belgelerin metinlerine göre sınıflandırılmasından otomatik olarak tasnif edilmesine, tasfiyeden arşive devrine kadar pek çok alanda faydalanılabileceği belirtilmektedir[216]. Bununla birlikte, tanımlama, erişim ve bir belgede - T.C. kimlik numarasının bulunması gibi- kişisel veri olup olmadığının kontrol edildiği "hassasiyet değerlendirmesi" (sensitivity review) işlemlerinde yapay zekâdan yararlanılabileceği öngörülmektedir[217].

Örneğin kurumlarda daha önce kullanılan EBYS'den yeni sisteme aktarılan belgelerin tasfiyesinde yapay zekâdan faydalanılabileceği görülmüştür. Avustralya Milli Arşivinin kâğıt ortam için geliştirilmiş tasfiye uygulamalarını elektronik ortamın sağladığı kolaylıklarla yapabilmek için yapay zekâ kullandığı çalışmalar mevcuttur. Bunun için otomatik üstveri ekleme-çıkarmaları yapma, semantik analizler, taksonomi ve ontoloji geliştirme ile bağlı veri çalışmaları yapılmaktadır[218]. Fakat belge yönetiminde geniş bir örneklemle sahada gerçekleştirilmiş yapay zekâ projelerinin eksikliği dikkat çekmektedir.

Yapay zekâdan yararlanıldığı başka bir çalışmada e-delil elde etme yöntemlerinin de kullanıldığı BitCurator programı kapsamında doğal dil işleme ile arşiv koleksiyonlarındaki malzemelerin otomatik olarak sınıflandırılması ve tanımlanması konusunda incelemeler yapılmıştır. Burada başarılı sonuçlara ulaşmak için arşiv malzemesinin kaliteli olması gerektiği belirtilmektedir. Her ne kadar ilgili çalışmada kaliteli arşiv malzemesinin nitelendirildiği görülemese de bunun e-belgeler açısından üstverileri standart bir şekilde oluşturulmuş, arşivsel bağı kurulmuş belgeleri ifade ettiği düşünülmektedir. Hâl böyle olsa da kâğıt ortamda oluşturulup sayısallaştırılan belgeler için doğal dil işleme kullanarak gerçekleştirilen çalışmalar

---

215 Nils J. Nilsson, **Yapay Zekâ**, çev.: Mehmet Doğan, 2. bs., İstanbul, Boğaziçi Üniversitesi Yayınevi, 2019, s. 19, 69.

216 Rolan vd., **a.g.e.**, s. 185.

217 Tim Hutchinson, "Natural Language Processing and Machine Learning as Practical Toolsets for Archival Processing", **Records Management Journal**, C. 30, No: 2, 2020, s. 157-161.

218 Rolan vd., **a.g.e.**, s. 185, 191, 194.

mevcutken[219], elektronik ortamda oluşan malzemeler için bunun nasıl gerçekleştirileceği yeni araştırmaları beklemektedir[220].

Bu açıklamalardan arşivlerde yapay zekânın kullanımı neticesinde belge yöneticisi ve arşivcinin rollerinin zayıflayabileceği düşünülebilir. Ancak, durumun tersi olacağı yani rollerinin artacağı tahmin edilmektedir. Mesela, belge üretilirken oluşan otomatik üstverileri koruyup, bunları ilk üretildiği gibi arşivciye devretmekle görevli olan belge yöneticileriyle bu üstverileri kullanarak tanımlama yapacak olan arşivci arasındaki bağ, yapay zekâ ile daha da artacaktır. Emin Gedikli, yapay zekâ çalışmalarında kullanmak amacıyla belge yöneticilerinin doğru dosyasına kaldırıldığı düşünülen belgelere "doğru dosyaya eklendi" damgası verebileceğini ve arşivcilerin bu damgaya sahip belgeleri yapay zekâ çalışmalarında kullanabileceğini söylemektedir[221]. Böylece bu iki rol arasındaki bağ güçlenebilir.

3.3.3.1.2. Güvenilirlikle İlişkisi

Daha çok 1970'li yıllarda tıbbi bilimler alanında yaygınlaşmaya başlayan uzman sistemlerden 90'lı yıllarda bilişim teknolojisinin gelişmesiyle literatürde görülmeye başlayan yapay zekâ uygulamalarında yararlanıldığı görülmektedir. Uzman sistemlerde, kurallar belirlenmekte ve bunlar sistemlere öğretilmektedir. Eğer-ise önermeleri kurulmaktadır. Bu önermeler, hastanın boynu ağrırsa ona bal sürmeyi tavsiye etmek gibi daha çok tıp alanında kullanılmıştır. Bu tür yaklaşımların yapay zekâlı sistemlerde de programlandığı bilinmektedir[222].

Bu önermeler, aynı zamanda kural tabanlı sistemler olarak da adlandırılmaktadır. E-belgelerin güvenilirliği için benimsenecek yaklaşımlarda bu özellikten

---

219 Perseus Digital Library, **Web Sayfası**, (Çevrimiçi) https://www.perseus.tufts.edu/hopper/, 31 Aralık 2019. ; Northwestern Üniversitesi, **Wordhoard Projesi Web Sayfası**, (Çevrimiçi) http :// wordhoard. northwestern. edu/ userman/ index.html, 31 Aralık 2019. ; Illinous Üniversitesi, **Metadata Offer New Knowledge (MONK - Yeni Bilgi Sunan Üstveri) Projesi Web Sayfası**, (Çevrimiçi) http://monk.library.illinois.edu/, 31 Aralık 2019.

220 Christopher Lee ve Kam Woods, "Diverse Digital Collections Meet Diverse Uses: Applying Natural Language Processing to Born-Digital Primary Sources", **14. International Conference on Digital Preservation**, 25-27 Eylül 2017, Kyoto[Japonya], yayımcı yok, 2017, (Çevrimiçi) https://ipres2017.jp/wp-content/uploads/50.pdf, 31 Aralık 2019.

221 Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümü Araştırma Görevlisi Emin Gedikli ile 18 Nisan 2019 tarihinde yapılan görüşme.

222 Nilsson, **a.g.e.**, s. 297-298.

faydalanılabilir. Ancak bunun öncesinde bilgisayarlara güvenilirliğin başarıyla korunmasını sağlayacak unsurların neler olduğu öğretilmelidir.

Bu süreçte sadece güvenilir belgelerle alakalı kriterlerin öğretilmesi yeterli olmayabilir. Çünkü kurumlar açısından güvenilirlik testinden geçemeyen örnekler de önemlidir. Bilgisayarlara güvenilir görülmeyenler de tanıtılmalıdır.

Bir belgede güvenilirlik için gerekli olan unsurların tespit edilememesi her zaman güvenilirliğin korunamadığı anlamına gelmeyebilir. Mesela bir belgedeki e-imza doğrulanamasa da bir sorun olmayabilir. Bunun için güvenilirliği tehdit eden unsurlar da yapay zekâya öğretilmelidir. Bu yapılarak kural tabanlı sistemlerin öğrenemediği durumlar karşısında etkili çözümler geliştirilebilir[223]. Burada güvenilirliğin temel unsurları ve onu tehdit eden etkenler için bir taksonomi oluşturma durumu söz konusudur[224]. Böylece güvenilirliği tesis eden hususlar hiyerarşik bir yapıda ortaya konularak bunları tehdit eden unsurlar arasında bir ilişki kurulabilir.

Tüm bu açıklamalara göre yapay zekâ, e-belgelerin özgünlük, gerçeklik ve tamlık niteliklerini değerlendirerek güvenilirliği kritik etme imkânı verir. Hatta belgenin üretilme safhasında da bundan yararlanılabilir[225]. Özgünlüğün şartlarından biri, belgelerin karakteristik unsurlarının kimliklendirilmesi yani onların tanımlanmasıdır. Bu unsurlardan biri de arşivsel bağdır. Arşivsel bağın belgelerin organik bağının kurulup, dosyalanmasıyla tesis edildiği bilinmektedir. O hâlde, yapay zekâ belgelerin dosyalanmasında önemli bir araç olan organik bağın kurulmasında kullanılabilir. Bunun için kurumun faaliyet ve fonksiyonları neticesinde oluşan belgeler tasnif edilerek, hangi işe ait olup nasıl dosyalanacağının yapay zekâya öğretilmesi gerekir.

Özgünlüğün korunması, belgelerin diplomatik özelliklerinin tanımlanmasıyla son derece ilişkilidir. Bunun için bu özelliklerden olan kişiler, arşivsel bağ, kontekst ve taşıyıcı ortam ile belgeye işlem ve yönetim safhasında yapılan eklemeler ve açıklamalar sistemdeki üstveri alanlarına kaydedilir. Yapay zekâ, kaydedilen bu

---

223 Rolan vd., **a.g.e.**, s. 182.

224 Nilsson, **a.g.e.**, s. 451, 488.

225 Güvenilirliğin diğer unsurlarından gerçeklik, belgenin prosedürlere uygun üretilmesiyle; tamlık ise belgedeki form elemanlarının tam olmasıyla sağlanabilmektedir. Bunun için belgedeki kişi ile faaliyetin uyumu, belgedeki imza sahibinin o işlemi düzenlemekle yetkili olması, belgede yer alması gereken üstveriler ile form elemanlarının bulunması gibi hususların kontrolünde yapay zekâdan yararlanılabilir. Bu unsurlar tam değilse belgenin üretilmesine izin verilmemelidir. Böylece yapay zekâ, güvenilirliğin korunmasına yardımcı olabilir.

özellikleri, belirlenen kurallar çerçevesinde işleyerek arşivsel tanımlamayı gerçekleştirmelidir. Özgünlüğün bir diğer şartı ise her dönem bütünlüğün korunmasıdır. Bunun için belgelerin sahip olduğu özniteliklerin değişmeden muhafaza edilmesi gerekir. Hâliyle, bu öznitelikler belirli aralıklarla kontrol edilmelidir. Burada yapay zekâdan yararlanarak, bütünlüğü bozabilecek unsurlarla karşılaşıldığında sistemin uyarı vermesi sağlanabilir[226]. Aynı zamanda yapay zekâ, formatı güncellenecek belgelerle bu işlem neticesinde özniteliklerde meydana gelebilecek değişimlerin belirlenmesinde kullanılabilir.

3.3.3.2. Yapay Öğrenme

3.3.3.2.1. Arşivcilik ve Belge Yönetiminde Kullanımı

E-belgelerin güvenilirliğinin korunmasında yapay zekânın yanı sıra daha önceki verilere dayanılarak başarılı sonuçlar elde etmeyi mümkün kılan yapay öğrenmeden de faydalanılabilir. "Yapay öğrenme, bilgisayarların örnek veri ya da geçmiş deneyimi kullanarak başarımlarını artıracak biçimde programlanmasıdır"[227]. Burada bir süreçle ilgili nitelikli olduğu düşünülen veriler, bilgisayarlara öğretilerek süreçler iyileştirilebilmektedir. Örneğin bir tercüme programında başarılı bulunmuş çeviriler programa öğretilerek yeni çevirilerde daha başarılı sonuçlar elde edilmektedir[228].

Arşivcilik ve belge yönetiminde yapay öğrenmenin kullanımına ilişkin çeşitli araştırmalar yapılmaktadır. Bunlar, arşivlerde verilerin saklama ve tasfiye kararlarının verilmesi, e-postaların değerlendirilmesi ve arşivlenmesi ile güncel dönemde belgelere yeni dosya kodlarının atanması gibi konular üzerinedir. New South Wales Eyaleti Arşivi, verilerin saklama ve tasfiye kararlarının verilmesinde yapay öğrenmeden faydalanmaktadır. Avustralya'daki Victoria Eyaletinde e-postaların değerlendirilmesinde yapay öğrenme

---

226 Jakub Breir ve Jana Branisova, "A Dynamic Rule Creation Based Anomaly Detection Method for Identifying Security Breaches in Log Records", **Wireless Personal Communications**, No: 94, 2017. ; Kashif Sultan, Hazrat Ali ve Zhongshan Zhang, "Call Detail Records Driven Anomaly Detection and Traffic Prediction in Mobile Cellular Networks", **IEEE Access**, 2018.

227 Ethem Alpaydın, **Yapay Öğrenme**, 4. bs., İstanbul, Boğaziçi Üniversitesi Yayınevi, 2018, s. 1. Alpaydın, İngilizcesi machine learning olan ve Türkçe'de bazı çalışmalarda makine öğrenmesi olarak kullanılan bu kavramı, mekanik yönünün pek kalmaması nedeniyle yapay öğrenme şeklinde benimsemektedir. Tezde de yapay öğrenme kavramı kullanılmıştır.

228 Cade Metz, An Infusion of AI Makes Google Translate More Powerful Than Ever, **Wired**, (Çevrimiçi) https :// www. wired. com/ 2016/ 09/ google- claims- ai- breakthrough- machine-translation, 29 Eylül 2020.

destekli araçlar kullanılmıştır. Arşivlik öneme sahip e-postaların seçilmesinde yapay öğrenmenin faydalı sonuçlar verdiği dile getirilmektedir[229].

Bununla birlikte, e-postaların arşivlenmesinde Stanford Üniversitesi tarafından yapay öğrenme temel alınarak geliştirilen ePADD adlı açık kaynak kodlu bir yazılımın kullanıldığı görülmektedir. Burada belirli bir örneklem üzerinde kişisel bilgi içeren kelimeler seçilmiş, bu kelimeler üzerinden yapay öğrenme uygulamaları yapılarak diğer e-postalardaki hassas kelimeler belirlenmiştir. Fakat bu belirlemenin doğru olup olmadığının kontrolünde yine arşivcilerin gözetimine ihtiyaç duyulduğu anlaşılmıştır. EPADD'ın arşivcilik pratiklerinde büyük kolaylıklar sağladığı ifade edilmektedir. Bununla birlikte, AB'nin kişisel verileri koruma kanunu mahiyetindeki düzenlemesi olan General Data Protection Regulation (GDPR - Genel Veri Koruma Yönetmeliği)'e uyum sağlanması noktasında ePADD'dan da faydalanılabileceği görülmüştür[230].

Yapay öğrenmenin arşivlerde kullanımı üzerine geliştirilen bu yaklaşımların yanı sıra güncel belge yönetimi döneminde de kullanılmaya çalışıldığı dikkat çekmektedir. Yapay öğrenme yöntemiyle belgelerin otomatik olarak dosya kodu alıp sınıflandırılması üzerine Kasım Binici tarafından yapılan bir çalışma dikkat çekmektedir. Bu çalışmada belgelerin yapay öğrenme kullanılarak vaka ve konu dosyalarına yerleştirmelerinden ziyade, yeniden bir tasnif yapılarak işlem safhasında verilen dosya kodlarıyla, geliştirilen algoritmanın verdiği dosya kodunun ne kadar örtüştüğüne odaklanıldığı görülmektedir. Mesela bir kişi ile ilgili kurul kararlarını içeren belgeleri hem personel özlük dosyaları hem de kurul kararlarıyla ilişkilendirmek mümkünken, yeniden yapılan tasnifte belgelerin sadece kurul kararlarıyla ilişkilendirildiği anlaşılmaktadır[231].

Dosya kodları, belgelerin ait olduğu faaliyet ve fonksiyonla ilişkisini sağlayan yani güvenilirliğin kritik edilmesini mümkün kılan araçlardan biridir. Bunların sadece belgeye bir erişim ucu olarak değerlendirilmesi, arşivsel bağın yeteri kadar kurulamamasına neden olabilir. Fakat Binici'nin çalışmasında açıkladığı yapay öğrenme yaklaşımıyla bir konu

229 Rolan vd., **a.g.e.**, s. 183, 186-190.

230 Josh Schneider vd., "Appraising, Processing, and Providing Access to Email in Contemporary Literary Archives", **Archives and Manuscripts**, C. 47, No: 3, 2019, s. 314, 315, 321.

231 Kasım Binici, "Makine Öğrenmesi Yaklaşımıyla e-Belgelere Standart Dosya Plan Numaralarının Otomatik Olarak Atanması Üzerine Bir Çalışma", **Bilgi Yönetimi**, C. 2, No: 2, 2019, s. 120, 122.

dosyasına girecek belgelerin otomatik olarak sınıflandırılması, belge yönetiminde oldukça önemli bir gelişme olarak kabul edilebilir.

3.3.3.2.2. Güvenilirlikle İlişkisi

Yapay öğrenme uygulamalarıyla emniyet güçlerinin suçların yoğun olduğu bölgeleri tespit edip adli vakalara hızlı müdahale ettiği göz önüne alındığında[232], e-belgelerin güvenilirliğini tehdit eden sorunlara odaklanıp bunları çözümleyecek bir algoritmanın geliştirilmesi mümkün görünmektedir. Burada, ne kadar çok veriye sahip olunursa o kadar gelişkin algoritma üretilebilir. Alpaydın, yapay öğrenme ile başarılı sonuçlar elde etmek için gerekenin yeni algoritmalar değil, büyük miktarda örnek veri ve yeterli hesaplama gücü olduğunu ifade etmektedir[233]. Hâliyle, e-belgelerin güvenilirliğinin korunmasında kullanılacak yapay öğrenme uygulamaları için sağlıklı ve etiketlenmiş veriye ihtiyaç duyulmaktadır.

Bilişim teknolojilerinde yapay öğrenme çalışmaları yapılırken kullanılan öğrenim, geçerleme ve sınama kümeleri oluşturma yöntemlerinden yararlanılabileceği değerlendirilmektedir. Bu kümelerde veriler çeşitli işlemlere tabi tutulur. Öğrenim kümesinde veriler işlenerek yanlış öngörü yapanlar elenmektedir. Öğrenme kümesi büyüdükçe genelleme hatası azaldığından bu kümedeki verilerin oldukça geniş tutulması önerilmektedir. Ancak, öğrenme kümesi modeli tek başına çözüme ulaştırmak için yeterli olmadığından bir geçerleme kümesi oluşturulur. Burada modelin varsayımları test edilir. Oluşturulan modelin nasıl sonuçlar verdiği ise sınama kümesinde değerlendirilir[234].

Durum böyle olunca, e-belgelerin güvenilirliğinin nasıl korunduğunu yapay öğrenme ile ölçmek için bir öğrenim kümesi, geçerleme kümesi ve sınama kümesine ihtiyaç duyulduğu anlaşılmaktadır. Ancak, aynı öğrenme ve geçerleme kümesi, bir süre sonra geçerleme olanı öğrenme kümesinin bir parçası hâline geldiğinden her zaman kullanılamamaktadır[235]. Hâliyle bu kümelerin belirli aralıklarla yenilenmesi gerekir. Güvenilirlik analizlerinde belgeyi kritik etmek için bir veri kümesi

---

232 Pedro Domingos, **Master Algoritma: Yapay Öğrenme Hayatımızı Nasıl Değiştirecek?**, çev.: Tufan Göbekçin, 3. bs., İstanbul, Paloma Yayınları, 2019, s. 15, 17.

233 Alpaydın, **a.g.e.**, s. 29.

234 **a.g.e.**, s. 28-31.

235 **a.g.e.**, s. 31.

kullanıldığında önce bir kısmı deneme kümesi olarak ayrılmalı, sonra kalanı öğrenme ve geçerleme için değerlendirilmelidir.

Yapay öğrenme uygulamaları öğrenme kümeleri üzerinden şekillendiğinden bu kümedeki belgelerin sağlıklı olması gerekir. Hâliyle bu tür belgeler, organik bağı kurulup doğru dosyalanmış, öznitelikleri korunmuş olanlardır. Bunun için öncelikle üretilen belgeler sahip olduğu koşullara göre gruplandırılmalıdır. Mesela, doğru dosyalanan belgelere doğru dosyalandı etiketi verilebilir. Bu uygulama, bütünlüğü koruduğu düşünülenler için de benimsenebilir. Böylece, sağlıklı olduğu düşünülen belgeler yapay öğrenme uygulamaları için kullanılmaya hazır hâle gelir. Bu belgelerle de geçerleme kümesi elde edilerek sınama kümesi oluşturulmalıdır.

3.3.3.3. Derin Öğrenme

Derin öğrenme, verilerin insan beyni gibi çalışan yapay sinir ağları üzerinden eğitildiği bir yaklaşımdır[236]. Bu yaklaşımın daha çok algoritmaların geliştirilmesinde kullanıldığı görülmektedir. O hâlde e-belgelerin güvenilirlik algoritmaları için de derin öğrenmeden yararlanılabileceği düşünülmektedir.

Derin öğrenme uygulamalarında bir veriyi sürekli çalıştırmak anlamına gelen pekiştirme yöntemlerinin oldukça başarılı sonuçlar verebileceği ileri sürülmektedir. Örneğin 5 bin etiketli bir örnek, kabul edilebilir bir performansa sahipken, 10 milyon etiketli bir örnekle insan performansına eşit hatta daha yukarı düzeyde bir model eğitiminin sağlanabileceği kabul edilmektedir[237]. Durum böyle olunca, belge yönetimindeki derin öğrenme uygulamaları için 10 milyon malzemeli bir örneklemin başarılı sonuçlar verebileceği ifade edilebilir.

Bir algoritma geliştirirken bazı parametrelere bağlı olarak tanımlanmış bir model, veri ya da geçmiş deneyim üzerinde modelin başarımını ölçmek için bir ölçüt tanımlanır. Burada amaç, modelin parametrelerini bu başarım ölçütüne göre en iyi sağlayan değerleri bulmaktır. Bunun için uygulamanın yapılacağı vakayla alakalı veriler kullanılarak sonuçlar elde edilir. Kullanılan veriler girdi, üzerinde çalışılan husus ise

---

236 John D. Kelleher, **Deep Learning**, yayım yeri yok, MIT Press, 2019, s. 1.

237 Ian Goodfellow vd., **Derin Öğrenme**, çev. Fatoş Yarman Vural vd., Ankara, Buzdağı Yayınevi, 2018, s. 20-21.

sınıf olarak tanımlanmaktadır[238]. E-belgelerin güvenilirliğinin korunmasında girdi belgelerin güvenilirlik kriterleri, sınıf ise güvenilirliğin ne kadar korunduğu şeklinde ifade edilebilir.

Algoritmaların başarılı sonuçlar verebilmesi için girdilerin kalitesi oldukça önemlidir. Mesela bir belgenin güvenilirliğinin hangi oranda korunduğunu tespit edebilmek için derin öğrenme dünyasında öznitelik olarak bilinen güvenilirlik unsurlarının öğretilmesi gerekir[239]. Bu öznitelikler bir algoritmaya dönüştüğü ölçüde güvenilirliğin korunmasında başarılı sonuçlar elde edilebilir.

Ancak, sadece güvenilirliği tesis eden unsurların algoritmaya dönüştürülmesi yeterli olmaz. Güvenilirliği olumsuz etkileyebilecek durumların da algoritmaya öğretilmesi gerekir. Fakat gerçekleşme olasılığı düşük bir olayı öğrenmek, gerçekleşme olasılığı yüksek olanı öğrenmekten daha çok bilgi ve işlenmesi gereken malzeme içerdiğinden bunun için matematiksel formüller kullanılmaktadır[240].

Kimi araştırmacılar, algoritma geliştirmenin kökenini 19. yüzyılın sonlarına kadar götürmektedir. International Business Machines (IBM - Uluslararası İş Makineleri)'in kurucusu olarak kabul edilen Herman Hollerith, tren biletlerinin delinmesi işleminden esinlenerek bilgi depolamak için delikli makine kâğıtlarından oluşan bir sistem ve bunları sayıp ayıracak Hollerith Makinesi'ni geliştirmiştir. 1890'da ABD'de nüfus sayımında bu makine kullanılmıştır. Hollerith'in kurduğu Computing Tabulating Recording Company daha sonra adını IBM'ye dönüştürmüştür[241].

Hollerith Makinesi'nin geliştirilmesindeki düşünce, saklanan malzemelerden gelecekte bilgi edinebilmek olabilir. Psikoloji ve bilişim alanındaki araştırmalarıyla bilinen Christian ve Griffiths, gelecekte ihtiyaç duyulmayacağı düşünülen bilgi taşıyıcıları için tasnif ve düzenleme yapmayı zamanın verimli kullanılmaması olarak değerlendirmektedir. Hiç tasnif yapılmayan yığın içerisinde arama yapmak ise etkin kabul edilmemektedir. Burada, hangi bilgi taşıyıcılarının saklanıp hangilerinin saklanmayacağına ve bunların nasıl tasnif edileceği ile ne zaman imha edileceğine karar verilmesi gerekir[242]. İşte bu sürecin arşivleme algoritmasının temelini oluşturduğu düşünülmektedir. Clifford Lynch,

238 Alpaydın, **a.g.e.**, s. 1-4.
239 Goodfellow vd., **a.g.e.**, s. 3.
240 **a.g.e.**, s. 70-71.
241 Christian ve Griffiths, **a.g.e.**, s. 18, 95.
242 **a.g.e.**, s. 112, 131, 151.

gerçekleştirilen işlemlerin şeffaflığı ve hesap verebilirliği ile gelecek kuşaklara aktarılması için bu algoritmaların korunmasını önermektedir[243].

Christian ve Griffiths'e göre ABD'deki kurumlarda üretilen çoğu veri, 1970'li yıllardan beri bir tasnif yapılmadan saklanmaktadır. Bunun 1975'te işlemcilerdeki transistor sayısının her yıl yüzde elli artacağını öngören Moore Yasası'ndan kaynaklandığı söylenebilir. Böylece, aranan verilere daha hızlı erişileceği düşünülmüştür. Ancak, 1990'lı yıllara gelindiğinde öngörülen transistör üretim sayısına ulaşılamadığından, yoğun veri üretiminden kaynaklı sıkıntılar yaşanmış ve daha özenli bir hafıza hiyerarşisinin benimsenmesi ihtiyacı doğmuştur. Bunun için bilgisayarlarda önbellekler kullanılmıştır. Ancak, önbellekler ana hafızanın sadece bir kısmını oluşturduğundan veriler orada sonsuza kadar saklanamamaktadır. Nasıl kullanılacaklarını belirleyen bir algoritmaya ihtiyaç duyulmaktadır. Bunun için tasfiye ve imha algoritmaları geliştirilmektedir[244].

Görüldüğü üzere algoritma tasarlamak tek bir disiplinin altında kalkabileceği bir iş değildir. Arşivcilik ve belge yönetimi için geliştirilecek algoritmalarda matematik, mühendislik, bilgisayar bilimi, istatistik ve yöneylem sahalarından destek almak gerekir. Bu yapılırken arşivcilik paradigmalarından uzaklaşılmamalıdır. Aksi takdirde hedeflenen sonuçlara ulaşmak güçleşecektir. Arşivci ve belge yöneticilerinin bu konularda gerekli yetkinlikleri elde ederek yapılan araştırmalara katkı verebileceği düşünülmektedir.

243 Clifford Lynch, "Stewardship in the Age of Algorithms", **First Monday**, C. 22, No: 14, 2017, s. 2.
244 Christian ve Griffiths, **a.g.e.**, s. 136-137.

DÖRDÜNCÜ BÖLÜM
SAHA ARAŞTIRMASI

4.1. Yöntem

4.1.1. Araştırmada Yöntem Yaklaşımı

Keşfetmeye odaklanmış çoğu araştırmada olduğu gibi e-imzalı belgelerin delil değerini açığa çıkarmaya çalışan bu tezde yorumlayıcı çatı benimsenmiştir. Çünkü Türkiye koşullarında bu delil değeri meselesi, daha önce akademik bir çalışmada problematiği ortaya konulup yeteri kadar tartışılmadığından, sorunun öncelikle keşfedilerek yorumlanmasına ihtiyaç duyulduğu değerlendirilmiştir. Tez kapsamındaki saha araştırmasının felsefesi, problem ve araştırma sorularının nasıl formüle edilebileceğini ve sorulara cevap bulabilmek için nasıl bir yol izleneceğini belirlemektedir[1].

Metodoloji kitaplarında araştırmalardaki yorumlayıcı çatı felsefesini postpozitivizm, sosyal yapılandırmacılık, postmodernizm ve pragmatizm gibi yaklaşımlar oluşturmaktadır. Pragmatizmde, eylemler, durumlar ve araştırmanın sonuçları gibi çalışmanın ürününe odaklanılır. Uygulamalar ne işe yarar sorusu sorularak problemlerin çözümünü bulmak hedeflenir[2]. E-imzalı belgelerin uzun dönemde özniteliklerinin nasıl korunabileceğinin incelenmesini hedefleyen bu tezde pragmatizm felsefesinden yararlanılmıştır. EBYS uygulamalarının bir neticesi olan e-imzalı belgelerin delil değerinin arşivsel güvenilirlik yaklaşımıyla korunup korunamayacağı tartışılmıştır.

Pragmatizmde metodolojik bir varsayım benimsenebilir. Tümevarımsal bir şekilde veri toplama ve analiz etme daha baskın görülür. Nitel ve nicel yaklaşımların bir arada kullanılmasına müsaittir[3]. Bu nedenle pragmatizm, tezde de benimsenen karma yöntem araştırmaları için uygun bir yapı olarak kabul edilmektedir.

Karma yöntem, araştırma problemlerini anlamak için hem nitel hem de nicel verilerin toplandığı, iki veri setinin birbiriyle bütünleştirilerek sonuçlar çıkarıldığı bir

---

1 John W. Creswell, **Araştırma Deseni: Nitel, Nicel ve Karma Yöntem Yaklaşımları**, çev.: Selçuk Beşir Demir vd., 3. bs., Ankara, Eğiten Kitap, 2017, s. 6.

2 John W. Creswell, **Nitel Araştırma Yöntemleri: Beş Yaklaşıma göre Nitel Araştırma ve Araştırma Deseni**, çev.: Mesut Bütün vd., 3. bs., Ankara, Siyasal Kitabevi, 2016, s. 28, 37. ; Creswell, **Araştırma Deseni: Nitel, Nicel ve Karma Yöntem Yaklaşımları**, **a.g.e.**, s. 10-11.

3 Creswell, **Nitel Araştırma Yöntemleri: Beş Yaklaşıma göre Nitel Araştırma ve Araştırma Deseni**, **a.g.e.**, s. 28, 37.

araştırma yaklaşımı olarak tanımlanmaktadır[4]. Nicel desenler kapalı uçlu cevaplardan, nitel veriler ise açık uçlu yapılardan meydana gelmektedir. 1960'lardan itibaren, sadece nicel ölçümlere dayanarak analiz yapılamayacağı, nitel verilerin de kullanılabileceği ileri sürülmüştür[5]. Bu iki yaklaşımın da kullanıldığı karma yöntem araştırmalarında bu yönteme özel bir araştırma sorusu belirlenir. Tezde benimsenen karma yöntem araştırma sorusu ise şöyle belirtilebilir: **Kurumlarda oluşan e-imzalı belgelerin delil değeri, mevcut e-belge yönetimi uygulamalarında hangi oranda korunmaktadır ve bu değer arşivsel güvenilirlik yaklaşımıyla nasıl incelenebilir?** Böylece, arşivlenen e-imzalı belgelerin güvenilirliğinin muhafazasında geliştirilecek stratejilere teknik ve teknolojik modellerin yanı sıra farklı bir yöntem önerisi getirilmeye çalışılmıştır.

E-imzalı belgelerin delil değeri konusuna incelendiği sahaya göre çeşitli yaklaşımlar geliştirilebilir. Hukukçuların e-imzanın geçerliliği üzerinden değerlendirdiği bu konuyu belge yöneticileri ve arşivciler e-imzayla birlikte fonksiyon ve belge arasındaki ilişki bağlamında tartışmaktadır. Tezde arşivsel güvenilirlik kuramıyla hareket edilmiştir. Önceleri görüş niteliğinde belirginleşen bu kuram, daha çok 20 yıldan fazla bir süredir devam eden INTERPARES proje çıktıları ışığında tartışılmış, diplomatik analiz ve arşivsel bağ gibi farklı argümanlar üzerinde akıl yürütmeleri yapılmıştır.

Her ne kadar adı geçen proje, e-belgelerin güvenilirliği konusunda birtakım sonuçlar ortaya koysa da bunların mevzuattaki karşılığının ülkelere göre değerlendirilmesi gerekir. Dolayısıyla arşivsel güvenilirlik yaklaşımının ülkelerin hukuk düzeni içerisinde yasal dayanağı tartışılmalıdır. Ancak sahayla alakalı doğrudan bağlayıcı mevzuat olmadığı ya da yetersiz kaldığı yerlerde ise uluslararası prosedürlerden yararlanıldığını da belirtmek gerekir. Bu sebeple e-imzalı belgelerin delil değerinin analiz edilmesi için saha araştırmasında kullanılacak sorular hazırlanırken ISO'nun çıkardığı uluslararası standartlardan faydalanılmıştır. Bundan dolayı tezde benimsenen soru ve hipotezler, INTERPARES çıktıları yanı sıra ISO standartları ışığında

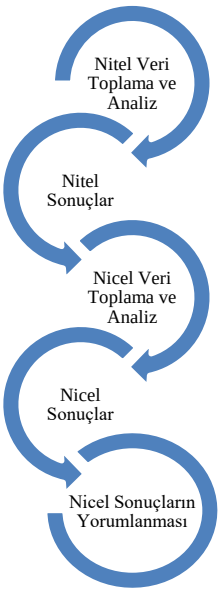
---

4 John W. Creswell, **Karma Yöntem Araştırmalarına Giriş**, çev. Mustafa Sözbilir vd., Ankara, Pegem Akademi Yayınları, 2017, s. 2.

5 Creswell, **Araştırma Deseni: Nitel, Nicel ve Karma Yöntem Yaklaşımları**, **a.g.e.**, s. 14-16.

şekillendirilmiştir. Bunun yanı sıra, ulusal standartlar ve birlikte çalışabilirlik esasları gibi ülke genelini kapsayan umumi düzenlemeler de yol gösterici olmuştur.

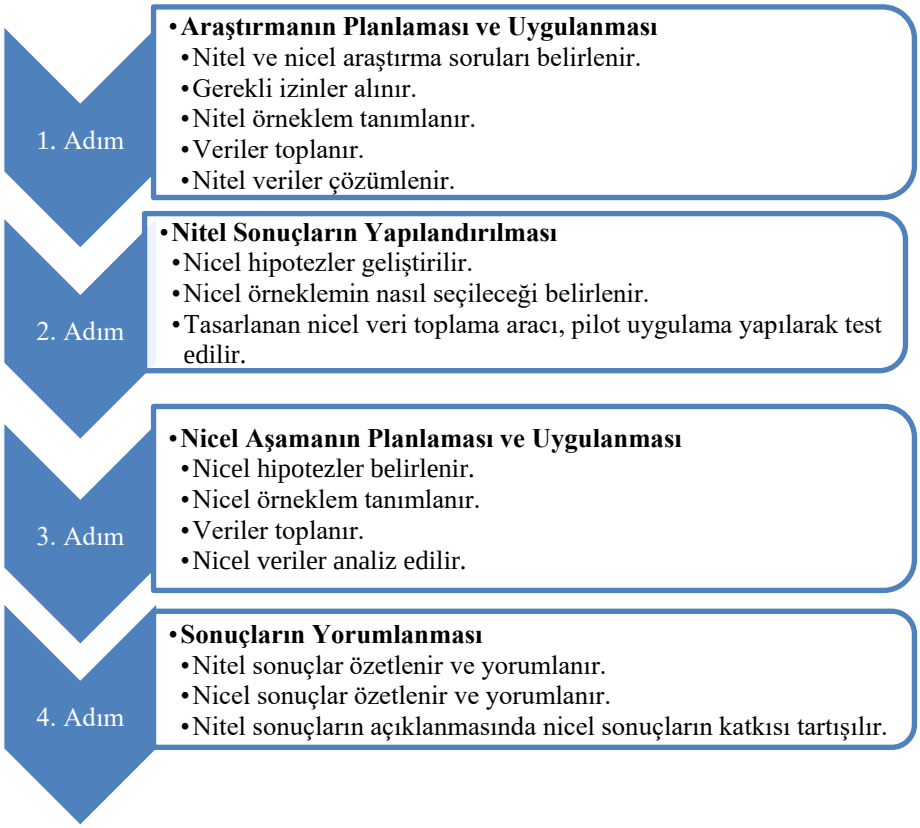
Sahada yapılan gözlemlerde e-imzalı belgelerin arşivlenmesi sürecinde risk ve tehditlere bağlı sorunlarla henüz yeteri kadar yüzleşilmediğinden, Türkiye'de arşivlenen e-imzalı belgelerin güvenilirliği meselesine idarecilerin çok da öncelik vermediği kanaati oluşmuştur. Bu sebeple uzun vadede doğabilecek riskler sorun olarak değerlendirilmediğinden öncelikle problemin keşfedilmesine ihtiyaç duyulmuştur. Bu keşif için gerek sahada yapılan gözlem gerekse literatür okumaları sırasında dikkat çeken sorular, birtakım kanaatlerin oluşmasına kaynaklık etmiştir. Mesela "arşivlenen e-imzalı belgelerin akıbeti uzun dönemde ne olacak" sorusu en temel meselelerden biridir. Birtakım okumalarla yeterli olgunluğa ulaştığı düşünülen bu mesele için saha uzmanlarıyla görüşmeler yapılmıştır. Sonrasında e-imzalı belgelerin güvenilirliğinin kurumlarda nasıl sağlandığı gözlenmeye çalışılmıştır. Bu gözlem ve görüşmeler neticesinde problemin keşfedilerek, buna ilişkin değişkenlerin saptanıp sayısal olarak değerlendirildiği "keşfedici sıralı karma yöntem" benimsenmiştir. Bu yöntemin işlem basamakları şu şekilde gösterilmektedir[6]:



Şekil 5. Keşfedici Sıralı Desen İşlem Basamakları

6 Creswell, **Karma Yöntem Araştırmalarına Giriş**, **a.g.e.**, s. 58.

Keşfedici sıralı desende öncelikle nitel veriler derlenip analiz edilmektedir. Bu aşama sonrasında nicel veriler toplanılarak değerlendirilir ve sonuçlar ortaya çıkarılır. Son aşamada nicel sonuçlar yorumlanmaktadır. Keşfedici desende uygulanan temel prosedür ise şöyle belirtilebilir:

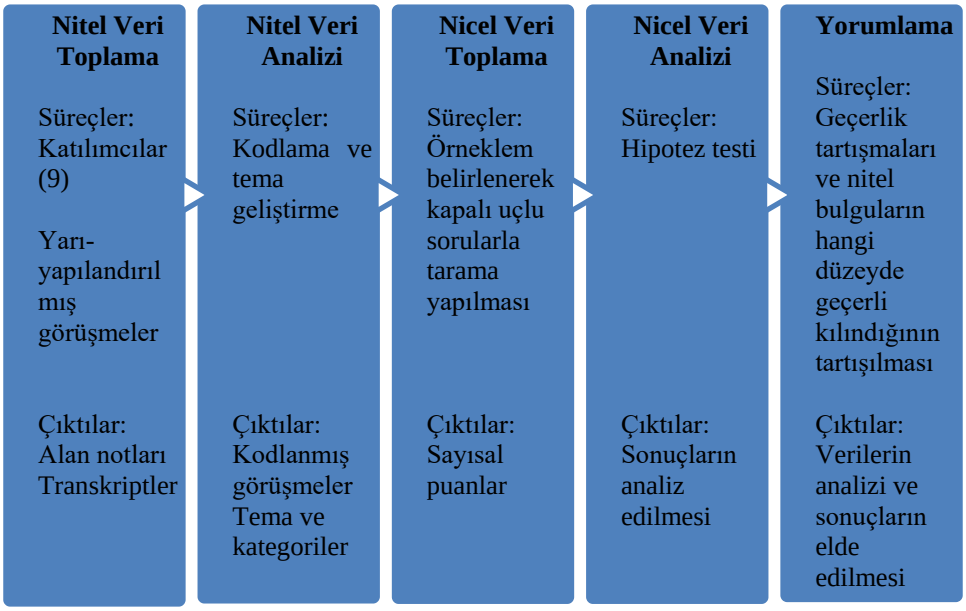


Şekil 6. Keşfedici Desende Uygulama Adımları

Bu yöntemin dört adımdan oluştuğu görülmektedir. Birinci adım, araştırmanın planlanması ve uygulanması sürecidir. Burada nitel ve nicel araştırma soruları kararlaştırılarak etik kurul izni alınır. Sonrasında nitel örneklem belirlenerek veriler toplanıp değerlendirilir.

İkinci adımda nitel sonuçlar yorumlanıp nicel hipotezler ve örneklemin nasıl geliştirileceği kararlaştırılmaktadır. Belirlenen nicel veri toplama aracıyla pilot uygulamalar yapılmaktadır. Tezde kullanılan nicel veri toplama aracıyla Ankara Üniversitesi, Bursa Teknik Üniversitesi ve daha çok belediyelere hizmet veren TS 13298 sertifikalı bir yazılım firmasında pilot çalışma uygulanmıştır.

Üçüncü adımda nicel hipotezler ve örneklem nihai olarak belirlenmekte; saha çalışması yapılıp elde edilen veriler analiz edilmektedir. Son adımda ise nitel ve nicel sonuçlar aralarında ilişki kurularak yorumlanır[7]. Tezde nicel araştırma için belirlenen örneklem, bakanlıklardan oluşmuştur. 6 kurum araştırmaya katılmıştır. Nitel ve nicel araştırma neticesinde elde edilen sonuçlar, bu bölümün tartışma kısmında değerlendirilmektedir. Araştırma sürecinin safhaları ise şu diyagramla gösterilebilir:



Şekil 7. Keşfedici Sıralı Desen Diyagramı

Şekil 7'de araştırma sürecinin safhaları gösterilmiştir. Nitel veri toplama kısmında katılımcılarla görüşmeler yapılmış, elde edilen veriler kayıt altına alınmıştır. Nitel veri analizi kısmında bu verilerin tezde incelenen güvenilirlik düzeyleriyle ilişkisi kurularak kodlaması yapılmış ve temalar oluşturulmuştur. Bu işlemler yapılırken MAXQDA programından yararlanılmıştır. Nicel veri toplama aşamasında ise belirlenen örneklemdeki kurumlara sorular sorulmuş, alınan cevaplar üzerinden değerlendirmeler yapılarak elde edilen veriler ışığında hipotez test edilmeye çalışılmıştır. Yorumlama safhasında nitel ve nicel verilerin geçerliliği tartışılmıştır[8].

---

7 John W. Creswell ve Vicki L. Piano Clark, **Karma Yöntemler Araştırmaları: Tasarımı ve Yürütülmesi**, çev.: Yüksel Dede vd., 3. bs., Ankara, Anı Yayıncılık, 2018, s. 94-97.

8 Creswell, **Karma Yöntem Araştırmalarına Giriş**, **a.g.e.**, s. 64.

Bahsedilen bu yaklaşımların tümü araştırma tasarımını oluşturmaktadır. Bu tasarımın genel bir şekli şöyle belirtilebilir:

Şekil 8. Araştırma Tasarımı

Tezde sahadaki problemin yorumlanmasına yönelik bir yaklaşım benimsendiğinden yorumlayıcı çatı tercih edilmiştir. Problemin yorumlanması aşamasında nitel ve nicel yaklaşımlar kullanılarak metodolojik varsayım benimsenmiştir. Problemin keşfedilmesi tercih edildiğinden nitel araştırmada durum çalışması yapılmıştır. Nicel araştırmada ise seçilen örneklem üzerinden evrenin geneline yorumlama yapabilmeyi mümkün kılacak tarama deseni seçilmiştir[9].

4.1.2. Nitel Araştırma

Nitel araştırma, bir probleme bireylerin veya grupların atfettiği anlamları keşfetme ve anlamaya yönelik bir yaklaşımdır. Soruların geliştirilmesi, katılımcılardan veri toplanması, özelden genel temalara ulaşan tümevarımsal veri analizi ve yorumlanması aşamalarını içerir[10]. Kolaylıkla ölçülemeyen değişkenleri belirleme, bir

---

9 Creswell, **Nitel Araştırma Yöntemleri: Beş Yaklaşıma göre Nitel Araştırma ve Araştırma Deseni**, **a.g.e.**, s. 28, 37. ; Creswell, **Araştırma Deseni: Nitel, Nicel ve Karma Yöntem Yaklaşımları**, **a.g.e.**, s. 155.

10 Creswell, **Araştırma Deseni: Nitel, Nicel ve Karma Yöntem Yaklaşımları**, **a.g.e.**, s. 4.

grup ya da evreni çalışma gibi nedenlerle nitel araştırma yürütülebilir. Kompleks bir konuya ayrıntılı bir anlayış getirmek için de yapılabilir. Bunun için insanlarla doğrudan görüşmeler gerçekleştirilir[11]. Nitel araştırma çalışmalarında araştırmanın sorusu, deseni, örneklemi, veri toplama teknikleri, verilerin analizi, araştırmacının rolü ile geçerlik ve güvenirliğe ilişkin hususlara yer verilmesi beklenmektedir. Bunlar şöyle açıklanabilir:

Soru: Kurumlarda oluşan e-imzalı belgelerin delil değeri, arşivsel güvenilirlik yaklaşımıyla nasıl incelenebilir?

Desen: Tezde nitel araştırma deseni olarak durum çalışması benimsenmiştir. Bu türde bir durum ya da olay derinlemesine analiz edilir[12]. Burada, araştırmacı bir durum hakkında bilgi toplar ve betimleme yaparak tema ortaya koyar. E-imzalı belgelerin güvenilirliği konusunda betimleme yapabilme imkânı vermesi nedeniyle tezde nitel araştırma deseni olarak durum çalışması tercih edilmiştir.

Durum çalışması, psikoloji, tıp, hukuk, siyaset bilimi gibi alanlarda sıklıkla kullanılan bir yaklaşımdır. Kökeni 1920'lere kadar götürülmektedir. Burada konuyla ilgili kategori ve temaların belirlenmesi beklenir[13]. Nasıl ve neden sorusu sorularak bir durumun açıklanması hedeflenir, onun seyrettiği çizgi incelenir[14]. Araştırma probleminin çözümlenmesi amaçlanır.

Durum çalışmaları, tek durum ve çoklu durum olmak üzere ikiye ayrılmıştır. Yine bu türler kendi içlerinde de bütüncül ve iç içe geçmiş durum desenleri olarak gruplandırılır. Bütüncülde tek bir birim analiz edilirken, iç içe geçmiş olanda birden fazla analiz birimi söz konusudur[15]. Tezin nitel araştırma kısmında sadece mülakat yapılan saha uzmanlarının görüşleri değerlendirildiğinden bütüncül tek durum deseni benimsenmiştir.

---

11 Creswell, **Nitel Araştırma Yöntemleri: Beş Yaklaşıma göre Nitel Araştırma ve Araştırma Deseni**, **a.g.e.**, s. 48.

12 Creswell, **Araştırma Deseni: Nitel, Nicel ve Karma Yöntem Yaklaşımları**, **a.g.e.**, s. 13-14.

13 Creswell, **Nitel Araştırma Yöntemleri: Beş Yaklaşıma göre Nitel Araştırma ve Araştırma Deseni**, **a.g.e.**, s. 97-98.

14 Robert K. Yin, **Case Study Research: Design and Methods**, 4. bs., California[ABD], SAGE Publications, 2009, s. 8.

15 **a.g.e.**, s. 46. ; Ali Yıldırım ve Hasan Şimşek, **Sosyal Bilimlerde Nitel Araştırma Yöntemleri**, 10. bs., Ankara, Seçkin Yayınları, 2018, s. 301.

Örneklem: Tezde nitel araştırma örneklemi olarak Türkiye'de farklı kurumlardaki e-belge yönetimi uygulamalarını değerlendirmiş kişiler seçilmiştir. Bunun nedeni katılımcılardan elde edilen görüşlerin genel durumu yansıtmak noktasında azami bir yaklaşım geliştirmek istenmesidir. 9 kişi ile görüşme yapılmıştır. Katılımcılar, rastgele numaralandırılmış ve görüşleri bu numaralarla aktarılmıştır.

Veri Toplama Teknikleri: Katılımcılara sorulacak soruları da kapsayan etik kurul onayı alınmış ve yarı-yapılandırılmış 17 soru sorulmuştur. Yedi görüşme yüz yüze, bir görüşme e-posta üzerinden, bir görüşme ise video-konferans yoluyla gerçekleştirilmiştir. Yüz yüze görüşme sağladığı etkileşim nedeniyle en iyi bilgi kaynağı olarak kabul edilse de araştırmacının baskın olması ihtimali sorunları arasında kabul edilmektedir[16]. Ancak, tüm katılımcılarla yüz yüze görüşme yapılması hedeflense de COVID-19 salgını nedeniyle e-posta ve video-konferans yöntemleri de tercih edilmiştir. Bu yöntemlerin, katılımcılara zaman ve yer esnekliği sağlayarak sorgulanan bilginin düşünülmesi ve cevap için daha fazla sunma imkânı sağladığı ileri sürülmektedir. Buna rağmen, katılımcının gizliliğinin sağlanamaması ve verinin korunamaması kaygıları nedeniyle dikkatle yaklaşılması önerilmektedir[17].

Verilerin Analizi: Elde edilen veriler, kod, kategori ve temalar altında bir araya getirilmiştir. Kodlama, verilerin etiketlenerek küçük bilgi kategorileri içinde toplanmasını ifade etmektedir. Tüm veriler değil, araştırma konusuyla ilgili olduğu düşünülenler bir etiket hâline getirilip, kodlanmıştır. Bu kodlar, daha geniş bir kapsamda kategorilere, kategoriler de temalara dönüştürülmüştür[18].

Nitel araştırmada elde edilen kodlar ve kategoriler, belge, teknolojik koşullar ve kurum düzeyi temaları altında değerlendirilse de sorulara verilen cevaplar bu düzeylerin her biriyle ilişkili olabilir. Mesela teknolojik göçle ilgili soruya verilen bir cevap, belge düzeyiyle, kurumsal politikalarla ilgili soruya verilen başka bir cevap ise teknolojik koşullar düzeyiyle ilgili görülebilir. Buna rağmen elde edilen cevapların

16 Creswell, **Nitel Araştırma Yöntemleri: Beş Yaklaşıma göre Nitel Araştırma ve Araştırma Deseni**, **a.g.e.**, s. 160-161.
17 **a.g.e.**, s. 164.
18 **a.g.e.**, s. 184-186.

belirlenen temalarla ilişkisinin kurulabileceği düşünülmüş ve bu ilişkiyi kurmada sık kullanılan yazılımlardan biri olan MAXQDA tercih edilmiştir. Bu tercihin nedeni, nitel verileri kodlama aracılığıyla değişkenlerle ilişkilendirme, kullanılan kod sayılarını gösterme ve kod dağılımlarının görsel sunumlarını oluşturmada sağladığı yetkinlikler olarak belirtilebilir[19]. Oluşan kod, kategori ve temalar EK 4, EK 5 ve EK 6'da verilmiştir. Katılımcıların görüşlerinde e-imzalı belgelerin güvenilirliğinin korunmasıyla ilgili olarak kritik bulunan ifadeler kalın punto ile yazılmıştır.

Araştırmacının Rolü: Araştırmacı, lisans ve yüksek lisans 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 çalışmaktadır.

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. Bu gözlemler, saha araştırmasının yapılmasını gündeme getirmiştir. Fakat araştırmacı kendi gözlemlerinin bir sınırlılık arz ettiğini ve hipotez geliştirmek için yeterli nitelikte olmadığını düşünmektedir. Bu nedenle nitel araştırma örneklemi, kamudaki farklı belge yönetimi uygulamalarını incelemiş veya tatbik etmiş kişilerden seçilmiştir.

Yapılan mülakatlar sadece sorular çerçevesinde gerçekleştirilmiş, katılımcıların belirli bir tarafa yönlendirilmemesine çalışılmıştır. Nitel araştırmalarda kişilerin bakış açılarının yansıtılması filtreli bilginin sunulması olarak kabul edilir ve bilgi tasarlanmış olarak değerlendirilir. Her katılımcının aynı düzeyde algılama ve ifade etme becerisine sahip olmadığı ileri sürülmektedir. Bu durum, araştırmacının yönlendirme yapmadan katılımcıyı bilgilendirmesini gerektirir[20].

---

19 Creswell ve Clark, **a.g.e.**, s. 258.

20 Creswell, **Araştırma Deseni: Nitel, Nicel ve Karma Yöntem Yaklaşımları**, **a.g.e.**, s. 191, 201.

Geçerlik ve Güvenirlik: Nitel araştırmalarda geçerlik için bulguların doğru olup olmadığı incelenir. Elde edilen bulgular tez metnine aktarılırken literatürdeki yeri belirtilmiştir. Literatürde karşılığı bulunan görüşler dipnotta "Görüş A", bulunmayanlar ise "Görüş B" şeklinde kısaltılarak yazılmıştır. Ayrıca probleme ilişkin kanaatlerin sınanmasında karşılaşılan katılımcıların aksi yöndeki -negatif veya uyuşmaz- görüşleri de tartışılmıştır.

Kullanılan bir diğer geçerlik yöntemi ise akran değerlendirmesidir[21]. Araştırmacı dışında başka bir kişi, tez hakkında soru sormuş ve inceleme yapmıştır. Bu noktada, tez süresince altı ayda bir toplanan tez izleme kurulunun görüşleri alınmıştır.

Güvenirlikte ise farklı araştırmacılar tarafından geliştirilen kodların çapraz kontrolünün yapılması önerilmektedir[22]. Güvenirliği sağlamak için Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümünde araştırmanın temas ettiği konular hakkında çalışmaları bulunan doktora öğrencilerinin görüşlerinden faydalanılmıştır. Emin Gedikli, Varol Saydam ve Oytun Cibaroğlu'na nitel veriler gönderilmiştir. Yaptıkları kodlamalarla araştırmacınınki kontrol edilmiştir.

4.1.3. Nicel Araştırma

Nicel araştırmada değişkenler arasındaki ilişki incelenerek nesnel kuramlar denenir. Değişkenler, ölçme araçlarıyla ölçümlenmekte; sayısal veriler istatistiksel işlemler kullanılarak analiz edilmektedir[23]. Nicel araştırma çalışmalarında araştırmanın sorusu, hipotezler ve değişkenler, desen, örneklem, veri toplama teknikleri, verilerin analizi, araştırmacının rolü ile geçerlik ve güvenirliğe ilişkin hususlara yer verilmesi beklenmektedir. Bunlar şöyle açıklanabilir:

Soru: Kamu kurumlarında oluşan e-imzalı belgelerin delil değeri mevcut e-belge yönetimi uygulamalarında hangi oranda korunmaktadır?

---

21 **a.g.e.**, s. 191, 201-203.
22 **a.g.e.**, s. 191, 203.
23 **a.g.e.**, s. 4.

Ana Hipotez: E-imza, zaman damgası ve e-mühür gibi yapıların kırılganlıkları ve kurumların gerekli denetimleri uygulamamasından dolayı arşivlenen e-imzalı belgelerin uzun süre saklanmaları sürecinde delil değerinde kayıplar yaşanabilir.

H1: E-imzalı belgelerin güvenilirliğinin korunması için arşivsel bağın kurulmasına ihtiyaç duyulmaktadır. Bu bağın başarılı bir şekilde kurulamadığı örgütlerde belgelerin delil değerinin zayıflayacağı düşünülmektedir.

H2: E-imzalı belgelerin güvenilirliğinin korunması için doğru teknolojik koşullara ihtiyaç duyulmaktadır. Bu koşulların yeteri kadar mevcut olmadığı kurumlarda belgelerin delil değerinin zayıflayacağı düşünülmektedir.

H3: E-imzalı belgelerin güvenilirliğinin korunması için belge yönetimi konusunda politika ve prosedürlere ihtiyaç duyulmaktadır. Bunların yeteri kadar bulunmadığı kurumlarda belgelerin delil değerinin zayıflayacağı düşünülmektedir.

Değişkenler: Tezde bağımlı değişken, e-imzalı belgelerin delil değeri; bağımsız değişkenler ise arşivsel bağ, teknolojik koşullar ve kurumsal politikalar ile prosedürlerdir. Değişkenler ile anket maddelerinin ilişkisi EK 7'de (Tablo 2) verilmiştir.

Desen: Nicel araştırma deseni olarak tarama deseni benimsenmiştir. Burada bir evrende seçilen örneklemdeki eğilim, tutum ya da görüşler sayısal olarak tanımlanmaya çalışılır ve evren hakkında çıkarımlarda bulunulur[24]. Tezde kamu kurumlarında oluşan e-imzalı belgelerin delil değerinin nasıl korunduğuna dair tutumlar incelenmektedir. Evrenin tamamını incelemek belirli bir zaman diliminde bitirilmesi gereken bu tez için pek mümkün olmadığından bir örneklem seçilerek inceleme yapılmıştır. Tarama yönteminin tezin amacıyla bu noktada uyumlu olduğu düşünülmüştür.

Tarama desenindeki verilerin[25] bir kez toplandığı kesitsel ve verilerin çeşitli zamanlarda toplandığı boylamsal olmak üzere iki türü bulunur. Kesitsel türün mevcut

---

24 **a.g.e.**, s. 155-156.

25 Tarama deseninin kökleri 1817'ye kadar götürülmektedir. İlk olarak ulusal eğitim politikasıyla ilgili çalışmalarda kullanıldığı ifade edilmektedir. 20. yüzyılda kullanımı giderek artmıştır.

pratikleri ölçmek bakımından faydalı olduğu belirtilmektedir[26]. Bu nedenle tezde kesitsel tür kullanılmıştır. Belirlenen örneklem üzerinde veriler bir kez toplanmıştır.

Örneklem: Tezin evrenini kamu kurumları oluşturmaktadır. Bu evrenden bir örneklem seçilerek evren hakkında çıkarımlar yapılmak istenmiştir. Bunun için küme örnekleme yoluna gidilmesi düşünülmüş ve örneklemi Türkiye'de en çok kamu personeli çalıştıran kurumların kümesi olan bakanlıklar oluşturmuştur. Saha araştırmasının yapıldığı sırada 2018'de kurulan Cumhurbaşkanlığı Hükümet Sistemi içerisinde 16 bakanlık bulunmaktaydı[27]. Örnekleme, Cumhurbaşkanlığı ile birlikte bütün bakanlıklar dâhil edilmiştir. Adlarının belirtilmemesi şartıyla 17 kurumdan 6'sı araştırmaya katılmıştır. Kurumların verdiği cevaplar takma ad kullanılarak aktarılmıştır[28]. Alınan cevaplar rastgele numaralandırılarak ifade edilmiştir.

Tezde sorulan sorular daha çok ISO standartları ve INTERPARES çalışmaları kapsamında geliştirilmiştir. Soruların kaynağı EK 7 (Tablo 2)'de belirtilmiştir. Belirlenen sorular kurumlara iletilmeden önce Bursa Teknik Üniversitesi, Ankara Üniversitesi ve daha çok belediyelere uygulama yazılımı sunan TS 13298 lisanslı bir firmanın EBYS yetkilileriyle pilot çalışmalar yapılmıştır. Bunun neticesinde ankette kullanılan bazı kavramların tanımlanmasının ve anketin cevaplanması sırasında araştırmacının da katılımcılarla birlikte bulunmasının gerekli olduğu anlaşılmıştır.

1950'lerden sonra pek çok alanda yapılan çalışmalarda kullanılan bir yöntem olmuştur (John W. Creswell, **Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research**, 4. bs., Boston[ABD], Pearson, 2012, s. 376).

26 Creswell, **Araştırma Deseni: Nitel, Nicel ve Karma Yöntem Yaklaşımları**, **a.g.e.**, s. 156. ; Creswell, **Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research**, **a.g.e.**, s. 377.

27 "Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi", Kararname Numarası: 1, **R.G.**, S 30474, tar. 10.07.2018 (Çevrimiçi), https:// www. resmigazete. gov. tr/ eskiler/ 2018/ 07/20180710-1.pdf, 6 Kasım 2020. ; "Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi", Kararname Numarası: 15, **R.G.**, S 30499, tar. 04.08.2018 (Çevrimiçi), https:// www.resmigazete.gov.tr/eskiler/2018/08/20180804-1.pdf, 6 Kasım 2020.

28 Kurumlar, adlarının belirtilmemesi şartıyla araştırmaya dâhil olabileceklerini beyan etmiştir. Durum böyle olunca, bakanlıklar düzeyindeki bu kurumların adları belirtilmemiş; Kurum1, Kurum2, Kurum3 … şeklinde tanımlanmışlardır. Bu durum, takma ad kullanma şeklinde ifade edilmektedir (TÜBİTAK Ulusal Akademik Ağ ve Bilgi Merkezi, **Araştırma Verileri Yönetimi Eğitim Portalı**, (Çevrimiçi) https:// acikveri. ulakbim. gov. tr/ acik-veri-acik-bilim/ bolum-3-veri-isleme/ 3-4-verinin-anonimlestirilmesi/ , 24 Haziran 2020).

Veri Toplama Teknikleri: Katılımcılara sorulacak soruları da kapsayan etik kurul onayı alınmış ve kapalı uçlu anket aracılığıyla sorular sorulmuştur. Görüşmeler, video-konferans ve telefon aracılığıyla gerçekleştirilmiştir. Yapılan ön testlerde katılımcıların soruları tek başlarına yanıtladıklarında mevcut durumdan farklı cevaplar verdikleri görülmüştür. Bunun nedeninin soruları anlama biçimleri olduğu düşünülmüştür. Çünkü bazı sorular, katılımcıların daha önce uygulamadıkları yöntemlere ilişkindir. Bu sorunu gidermek için araştırmacı, gerekli durumlarda kurumda kullanılan EBYS üzerinden sorulan soruyu test etme yöntemini seçmiştir.

Verilerin Analizi: Anket soruları, tezde incelenen güvenilirlik düzeylerinden belge, teknolojik koşullar ve kurum düzeyleriyle ilişkilendirilmiştir. Kurumun dosyalama uygulamaları, kullanılan üstveriler, teknolojik koşullar ve yazılı prosedürlerin varlığına ilişkin sorular sorulmuştur. Verilen cevaplara göre bir puanlama yapılmıştır.

Katılımcılara evet/hayır cevabı verilecek kategorik ölçekli 154 soru sorulmuştur. Bu sorular kendi içerisinde zorunlu ve seçmeli olarak ayrılmıştır. Zorunlu sorular, belgelerin delil değerini korumak için yapılması gerekenleri ifade etmektedir. Seçmeliler ise delil değerini korumayı destekleyen fakat mevcut olmaması çok ciddi bir eksiklik olarak görülmeyenleri ölçmeye çalışmaktadır. Bu nedenle zorunlu ve seçmeli soruların puan karşılığı farklı belirlenmiştir.

Nicel araştırma soruları, tezde incelenen güvenilirlik düzeyleriyle ilişkilendirilmiştir. Kurum düzeyinde 28 (19 zorunlu, 9 seçmeli), teknolojik koşullar düzeyinde 49 (35 zorunlu, 14 seçmeli), belge düzeyinde ise 77 (59 zorunlu, 18 seçmeli) soru sorulmuştur. Burada her düzeyin güvenilirliğe eşit katkı yaptığı düşünülmektedir. Puanların eşit oranda olması için her bir düzey 25 puan üzerinden hesaplanmıştır. Sorular üç düzeyde gruplandırılıp toplamı da 75 puan ettiğinden azami puanın 100'e tamamlanabilmesi için her bir kuruma ayrıca 25 puan tanımlanmıştır. Böylece hesaplamanın daha anlaşılır olması amaçlanmıştır.

Düzeylerdeki zorunlu soruların karşılıkları toplam 20 puan, seçmelilerin karşılıkları ise toplam 5 puan olarak belirlenmiştir. Bunun nedeni zorunlu soruların toplamda %80'lik bir paya sahip olarak daha önemli bir konumda bulunmasının istenmesidir. Aksi takdirde, zorunlu pratikleri uygulamayıp seçmelileri uygulayan

kurumların daha başarılı gözükmesi durumu söz konusu olacaktır. Kurum düzeyinde zorunlu bir pratiği ölçen sorunun katsayısı 1.052 (20/19) iken, seçmelinin 0.555 (5/9)'dir. Aynı şekilde teknolojik koşullar düzeyinde zorunlu bir pratiği ölçen sorunun katsayısı 0.571 (20/35), seçmelinin ise 0.357 (5/14) olarak hesaplanmıştır. Hesaplama algoritmasının kolay bir şekilde elde edilebilmesi nedeniyle Microsoft Office Excel yazılımı kullanılmıştır.

Bu kriterlerin yanı sıra, bazı zorunlu pratikler başarılı bir belge yönetimi sürecinin başlangıcı olarak kabul edildiğinden kritik bir öneme sahiptir. Belge ve arşiv yönetimi politikasının hazırlanması, dosya planının oluşturulması, EBYS'de kullanılan algoritmaların saklanması gibi pratikler zorunluluk şeklinde değerlendirildiğinden bunları ölçmeye çalışan soruların katsayılarının diğerlerine göre farklı olması gerekir. Eğitim, meteoroloji ve maliye gibi farklı alanlardaki çeşitli çalışmalarda kritik olduğu düşünülen hususların başarıya etkisinin %60 olarak değerlendirildiği bilinmektedir[29]. Hâliyle, belirtilen sahalara yönelik akademik çalışmalarda yaygın olarak kullanılan oranlamanın bu tezde de benimsenebileceği düşünülmüştür. Durum böyle olunca, kurumların bir düzeyde başarılı olabilmesi için o düzeyde %60 başarıya ulaşması yani en az 15 puan alması gerekmektedir.

Her soruda kritik olarak değerlendirilen zorunlu kriterler mevcut olmadığından kritik zorunlu, zorunlu ve seçmeli şeklinde bir ayrım yapmak puan dağılımını az olan kritik zorunlu kriterler lehine, diğerlerinin ise aleyhine değiştirecekti. Bu nedenle kritik zorunlu soruların katsayıları, bunların bulunduğu ana sorular içerisinde şu formülle hesaplanmıştır:

Zorunlu kritik soruların katsayısı= [İlgili soruda alınabilecek azami puan-(Zorunlu ve seçmeli soruların katsayıları toplamı) * 0.4]/Kritik zorunlu sayısı

---

29 Neşe Öztürk Gübeş, "An Investigation into Weighting Problem in Norm-Referenced Grading System", **Eurasian Journal of Educational Research**, No: 93, 2021. ; Larry Phillips ve Adrian Stock, **Use of Multi-Criteria Analysis in Air Quality Policy**, Department for Environment, Food and Rural Affairs, 2003, (Çevrimiçi) https :// uk-air. defra. gov. uk/ assets/ documents/ reports/cat09/0711231556_MCDA_Final.pdf, 24 Haziran 2020. ; Queensland Government Contract Services Department of Public Works, **Guidance on Evaluating Tenders Using Price Quality Method**, (Çevrimiçi) https:// www. hpw. qld. gov. au/ __data/ assets/ pdf_ file/ 0013/ 3334/ pricequalitymethod.pdf, 24 Haziran 2020. ; Jiahe Qian, Yanming Jiang ve Alina A. von Davier, **Weighting Test Samples in IRT Linking and Equating: Toward an Improved Sampling Design for Complex Equating**, Educational Testing Service, Princeton[ABD], 2013, (Çevrimiçi) https :// origin-www. ets. org/ Media/ Research/ pdf/ RR-13-39.pdf, 24 Haziran 2020.

Saha araştırmasında 29 soru kritik zorunlu olarak değerlendirilmiştir. Bunların 14'ü belge, 9'u teknolojik koşullar, 6'sı kurum düzeyindedir. Soruların dağılımı EK 9, EK 10 ve EK 11'de gösterilmiştir. Kurumlar, verdikleri cevaplara göre bir başarı düzeyine sahip olmuş ve toplam puanları 0-25 aralığındaysa değerlendirme dışı, 26-40 arasındaysa başarısız, 41-55 arasındaysa zayıf, 56-69 arasındaysa orta, 70-84 arasındaysa başarılı ve 85-100 arasındaysa çok başarılı kabul edilmiştir.

Sorulara verilen cevaplar, tablolarda belirtilerek tezde incelenen güvenilirlik düzeyleriyle ilişkilendirilmiştir. Belge düzeyindeki sorular, **e-imzalı belgelerin güvenilirliğinin korunması için arşivsel bağın kurulmasına ihtiyaç duyulmaktadır. Bu bağın başarılı bir şekilde kurulamadığı örgütlerde belgelerin delil değerinin zayıflayacağı düşünülmektedir** hipoteziyle; teknolojik koşullar düzeyindeki sorular, **e-imzalı belgelerin güvenilirliğinin korunması için doğru teknolojik koşullara ihtiyaç duyulmaktadır. Bu koşulların yeteri kadar mevcut olmadığı kurumlarda belgelerin delil değerinin zayıflayacağı düşünülmektedir** hipoteziyle; kurum düzeyindeki sorular ise **e-imzalı belgelerin güvenilirliğinin korunması için belge yönetimi konusunda politika ve prosedürlere ihtiyaç duyulmaktadır. Bunların yeteri kadar bulunmadığı kurumlarda belgelerin delil değerinin zayıflayacağı düşünülmektedir** hipoteziyle ilintilendirilmiştir.

Araştırmacının Rolü: Pilot uygulamalar neticesinde araştırmacının katılımcılarla birlikte çalışması gerektiği görülmüştür. Çünkü ön testlerde katılımcıların soruları farklı yönde algılayabildikleri gözlenmiş, aynı zamanda bazı soruların açıklanmasına ihtiyaç duyulduğu fark edilmiştir. Kurumlardaki EBYS sorumlularının daha çok bilgi işlem kökenli olması göz önüne alındığında, arşivcilik yöntem ve kavramları esas alınarak hazırlanan soruları ilk başta anlamamaları tabii karşılanabilir. Bu nedenle araştırmacı, anketin cevaplanmasında katılımcılarla birlikte onların çalışma ortamında yer almıştır. Mesela, bir katılımcı kurumundaki pratikleri açıklamış ve sorunun bunu karşılayıp karşılamadığını sormuştur. Sorular kategorik ölçekli olduğundan yönlendirmeye açık bir tarafının bulunmadığını belirtmek gerekir.

Geçerlik ve Güvenirlik: Nicel araştırmaların geçerliğinde soruların konuyu ölçüp ölçmediği, güvenirliğinde ise ölçme aracının kaç kişi tarafından incelendiği

analiz edilen hususlardan biridir[30]. Güvenirlikte elde edilen sonuçların tekrarlanabilir olması aranır. Sonuçlar güvenilir değilse geçerli de kabul edilmemektedir[31]. Geçerlik ve güvenirlik için nitel araştırma katılımcılarının görüşlerine başvurulmuş ve tez izleme komitesinin kanaatleri sorulmuştur.

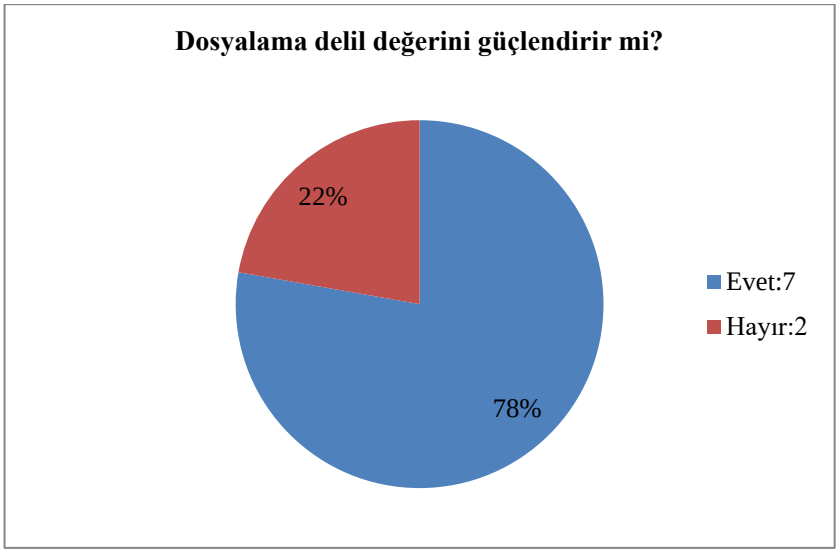
4.2. Bulgular

4.2.1. Nitel Bulgular

4.2.1.1. Belge Düzeyi

Nitel araştırmada sahadaki uzmanların önermeleri ne derece benimsediği analiz edilmiştir. Sorular, incelenen güvenilirlik düzeyleriyle ilişkilendirilmiştir. İlk olarak belge düzeyindekiler değerlendirilmiştir. Bunlar, dosyalama, arşivsel bağ, üstveriler, değerlendirme, EYP, erişim profiliyle ilgilidir. Bunların dışında, katılımcıların önerdiği güvenilirlik mekanizmaları da dikkate alınmıştır.

Belge düzeyinde ilk soru, dosyalamanın delil değerini güçlendirip güçlendirmediğiyle ilgilidir. Bu soruya 7 kişi evet, 2 kişi hayır cevabını vermiştir. Buna ilişkin şöyle bir grafik oluşturulabilir:



Şekil 9. Dosyalama ve Delil Değeri İlişkisine Verilen Cevaplar

30 Creswell, **Araştırma Deseni: Nitel, Nicel ve Karma Yöntem Yaklaşımları**, **a.g.e.**, s. 160.
31 Creswell, **Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research**, **a.g.e.**, s. 159, 161.

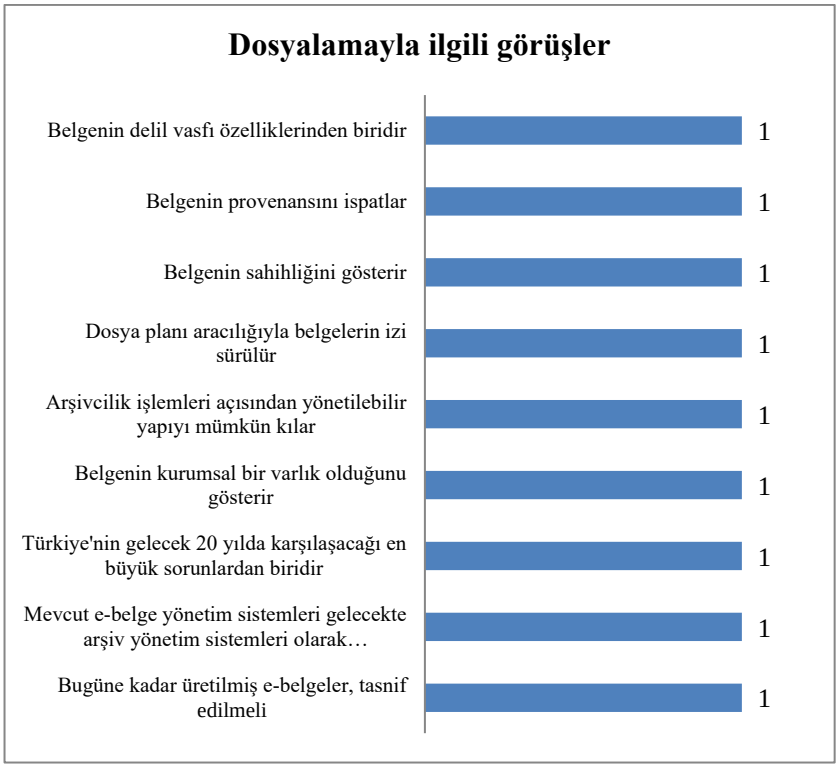
Evet cevabı verenlerin görüşleri şöyle dile getirilebilir. NİT01, dosyalamanın *"belgenin delil değerini kuvvetli bir şekilde güçlendireceğini*" ileri sürmüş, NİT02 ise dosyalamayı "*mütemmim cüz*" olarak değerlendirmiştir. NİT03, "*tek başına delil vasfı taşıyamayabileceğine*" vurgu yapsa da "*dosyalamanın vaka dosyaları için oldukça önemli olduğunu*" aktarmıştır. NİT04, "*dosya bütünlüğü olmazsa hak ihlalilin söz konusu olabileceğini*" beyan etmiştir. NİT06, "*doğru sınıflandırılmamış bir belgeye erişimin zor olacağını ve belgenin gözden kaçırılabileceğini*" ifade etmiştir. NİT07, "*dosyalamanın belgenin kurumsal ilişkisini ortaya koyduğunu ve buradan hareketle belgenin kurumsal bir varlık olup olmadığının anlaşılmasında yardımcı bir unsur olduğunu*" dile getirmiştir.

NİT09, bu konuda önemli görüşler ifade etmektedir. "***Dosyalama pratiklerini, belgenin delil vasfı özelliklerinden biri***" olarak kabul etmektedir. "***Dosyalama pratiğinin belgenin provenansını ispatladığını***" dile getirmekte, "*dosya planı aracılığıyla belgenin hangi fonksiyon ve faaliyet kapsamında üretildiğinin anlaşıldığını*" belirtmektedir. Böylece, "*belgelerin izinin sürüldüğünü, fonksiyonla serinin, faaliyetle klasörün eşleşmesi*" gerektiğini ileri sürmektedir. Dosyalamanın önemini şöyle açıklamaktadır: "*Dosyalama, belgenin hangi faaliyet ve fonksiyon kapsamında üretildiğini belirttiğinden sahihliğini de göstermektedir. Aynı zamanda, dosyalama arşivcilik işlemleri açısından yönetilebilir bir yapıyı mümkün kılar. Sürecin en başında, bir dosya planı oluşturup dosyalama yapısı kurgulamak hem arşivcilik açısından işlemlerin yönetilebilir olmasını sağlayacak hem de belgenin sahihliği konusunda fonksiyon ve faaliyet bağlamında bir delil göstergesi oluşturacaktır. Belgeleri imha edecek veya Devlet Arşivleri Başkanlığına gönderecek ya da kendi arşiv sistemine aktaracaksa da bunun bir dosya yapısı içerisinde yapılması gerekecektir. Devlet Arşivleri Başkanlığı, belgeleri dosya yapısı içerisinde gönderilmesini isteyecektir. Aksi takdirde, ayıklama ve imha diye bir kavrama ihtiyaç duyulmaz".*

Bu açıklamalarla birlikte NİT09, "***elektronik ortamda dosyalamayı Türkiye'nin gelecek 20 yılda yüzleşeceği en büyük sorunlardan biri***" olarak değerlendirmektedir. "*EBYS dönüşüm süreci kadar sancılı olacağını*" ileri sürmektedir. "***Şu anda kullanılan e-belge yönetim sistemlerinin gelecekte arşiv yönetim sistemleri olarak kullanılamayacağını***" belirtmektedir. "*Belgelerin organik yapısını göstermek için geçmişe dönük bir çalışma yapmanın hiç de kolay olmadığını*" ifade etmektedir. "***Gelecekte, bugüne kadar EBYS'lerde üretilmiş belgeleri sınıflandırmak gibi yeni bir bilgi ve belge yönetimi***

alt iş kolunun ortaya çıkacağını" dile getirmekte; "*geçmişte üretilmiş e-belgelerin tasnifi için uzmanlıklara ihtiyaç duyulacağına*" dikkat çekmektedir. "***Aksi takdirde veri yığınları oluşacağını ve belgelerin anlamını kaybedeceğini***" iddia etmektedir[32].

Dosyalamanın belgelerin delil değerini güçlendirdiğine ilişkin bu görüşlerin yanı sıra, NİT05 ve NİT08 "*dosyalamanın belgenin delil değeriyle bir ilişkisi olmadığını*" ifade etmiştir. Burada dile getirilen olumlu ve olumsuz görüşlerin literatürle uyumlu olduğu söylenebilir. Literatürde belgelerin bir dosyayla ilişkilendirilmesi gerektiğini belirten ve aksini iddia eden yaklaşımlar mevcuttur[33]. Elde edilen görüşler neticesinde dosyalamanın delil değerini kuvvetlendirdiği dile getirilebilir. Burada dile getirilen görüşler şöyle belirtilebilir:

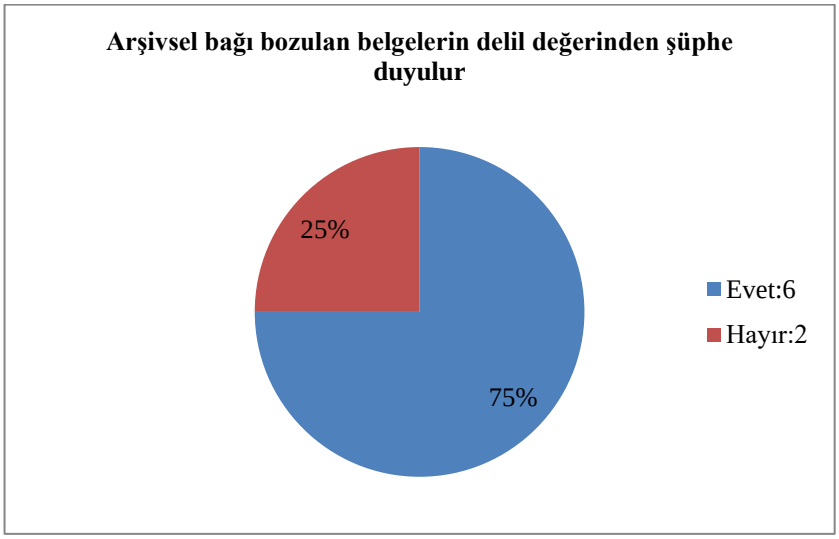


Şekil 10. Dosyalamayla İlgili Görüşler

32 NİT09'un ifade ettiği hususlar, Niyazi Çiçek'in bu konuda yaptığı çalışmalarda da görülmektedir (Çiçek, "Elektronik Belge Yönetimi Uygulamalarında Bir Alt Sistem Olarak Dosya Yönetimi", **a.g.e.**). Literatürde karşılığı bulunan görüşler dipnotta "Görüş A", bulunmayanlar ise "Görüş B" şeklinde kısaltılarak yazılmıştır.

33 Görüş A (Sataaslaatten, **a.g.e.**, s. 200-203. ; Yeo, "Bringing Things Together: Aggregate Records in a Digital Age", **a.g.e.**).

Dosyalamadan sonraki soru, arşivsel bağı bozulan belgelerin delil değerinden şüphe duyulup duyulmayacağıyla ilgilidir. Bir kişi hariç herkesten cevap alınmış, 6 kişi evet, 2 kişi ise hayır cevabını vermiştir. NİT04 bu soruya cevap vermemiştir. Alınan cevaplara ilişkin şöyle bir grafik oluşturulabilir:

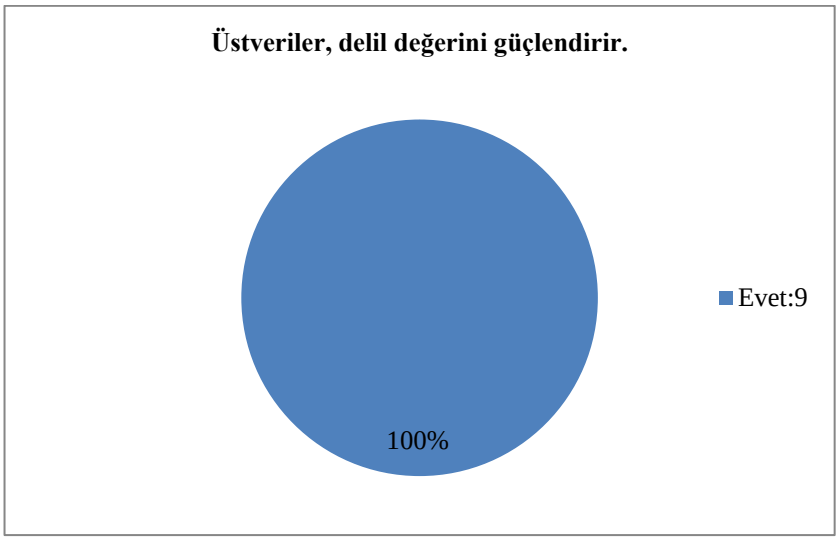


Şekil 11. Arşivsel Bağ ve Delil Değeri İlişkisine Verilen Cevaplar

Dosyalamayla delil değerinin bir ilişkisi olmadığını ifade eden NİT05 ve NİT08 bu soruya da benzer yönde cevap vermiş ve arşivsel bağı bozulan belgelerin delil değerinden şüphe duyulamayacağını ifade etmiştir. Bunun nedeni sorulduğunda, "*belgelerin ait oldukları faaliyetle ilişkisinin üstverilerle sağlandığı*" açıklamasını yapmışlardır. NİT01, "***seri-dosya ve belge hiyerarşisinin bozulması durumunda belgelerin konu bütünlüğünün bozulacağını ve delil değerinin sıkıntıya uğrayacağını***" dile getirmiştir. NİT02, "*belgelerin organik bağını kuramıyorsak belgeye müdahale edilip edilmediğinin sorgulanacağını*" belirtmiştir. NİT03, "***belgenin bir dosyaya ait olmasının onun bütüncül sürecini gösterdiğini ve seri-dosya-belge hiyerarşisinin zorunlu bir sistem kriteri olarak benimsenmesi gerektiğini***" aktarmıştır. NİT07 ise "*belgelerin kurumsal ilişkileri belirlenemediğinde belgeden şüphe duyulabileceğine*" dikkat çekmiştir. NİT09, "*seri-dosya-belge hiyerarşisi bozulan belgelerin öksüz olarak değerlendirildiğini, vaka ve konu dosyası ayrımı yapılmayan belgelerin ise bir süre sonra neyi ifade ettikleri ve ilişkilerinin kavranması noktasında ciddi problemlerin yaşanacağını*" ileri sürmektedir. Dile getirilen görüşlerin

literatürle uyumlu olduğu söylenebilir[34]. Elde edilen cevaplar neticesinde arşivsel bağı bozulan belgelerin delil değerinden şüphe edilebileceği anlaşılmaktadır.

Güvenilirliğin belge düzeyiyle ilişkilendirilen bir diğer önerme sorusu üstverilerin delil değerini güçlendirip güçlendirmediğidir. Tüm katılımcılar bu soruya evet cevabını vermiştir. Verilen cevaplara ilişkin grafik şöyle gösterilebilir:



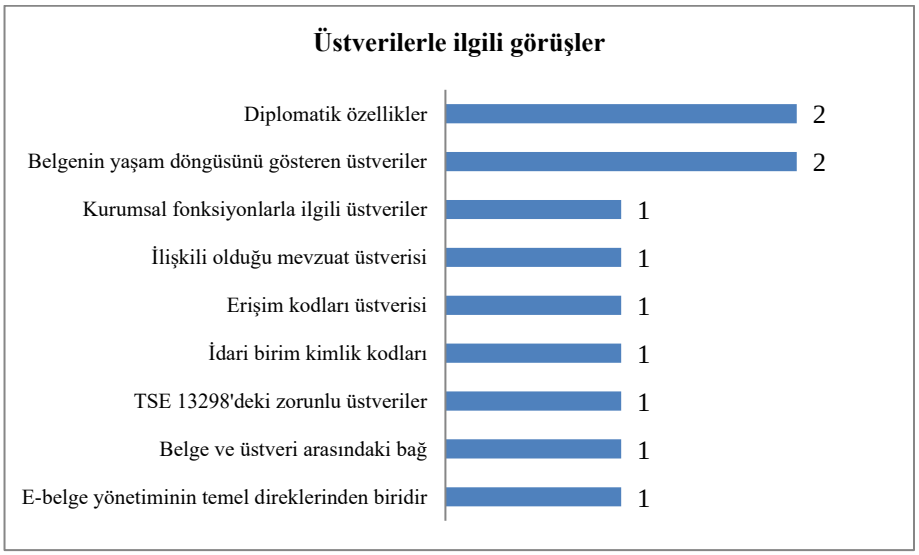
Şekil 12. Üstveri ve Delil Değeri İlişkisi

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*"

[34] Görüş A (Duranti, "The Concept of Electronic Record, Preservation of the Integrity of Electronic Records", **a.g.e.**, s. 11).

dile getirmiştir. Aynı zamanda "*idari birim kimlik kodlarını ihtiva eden üstverilerin iyi bir şekilde saklanması gerektiğini*" ifade etmektedir.

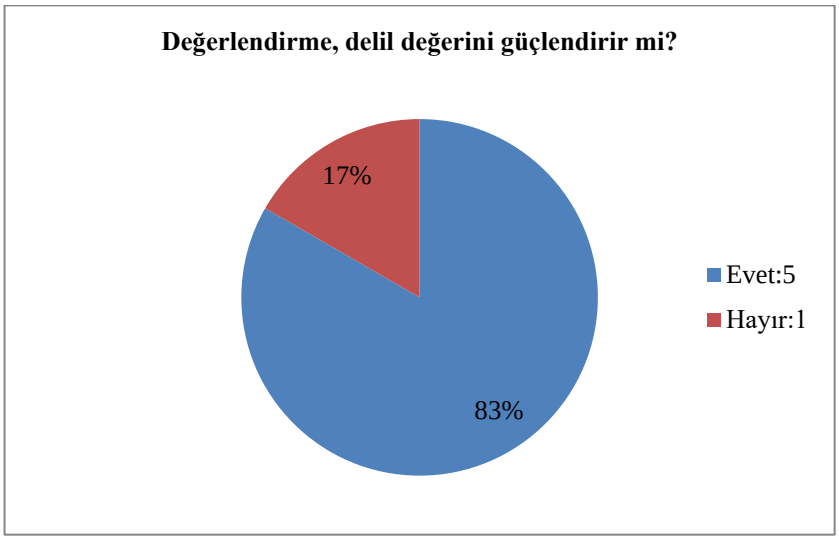
NİT03 ve NİT09, belgenin yaşam döngüsünü gösteren üstverilerin önemine dikkat çekmektedir. NİT03, "*üstverilerin belgenin oluşumundan nihai tasfiyesine kadar geçen süreçte belgelerin bütünsel gerçekliği açısından önemli verileri içerdiğini*" beyan etmiştir. NİT09, "*yaşam döngüsü ve belge süreklilik 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[35]. Üstverilerin belgenin delil değerini güçlendireceği kanaatinin saha uzmanları tarafından da paylaşıldığı görülmektedir. Verilen cevaplar neticesinde aşağıdaki gibi bir grafik oluşturulmuştur:



Şekil 13. Üstverilerle İlgili Görüşler

35 Görüş A (INTERPARES, **INTERPARES 2: Experiential, Interactive and Dynamic Records**, **a.g.e.** ; Yalçınkaya, "E-devlet Üstveri Standardının Oluşturulması ve Türkiye için Modellenmesi", **a.g.e.**).

Sorulan bir diğer önerme ise değerlendirmenin belgenin delil değerini güçlendirip güçlendirmediğidir. 6 kişiden 5'i evet, 1'i hayır cevabını vermiştir. Cevaplara ilişkin şöyle bir grafik oluşturulabilir:



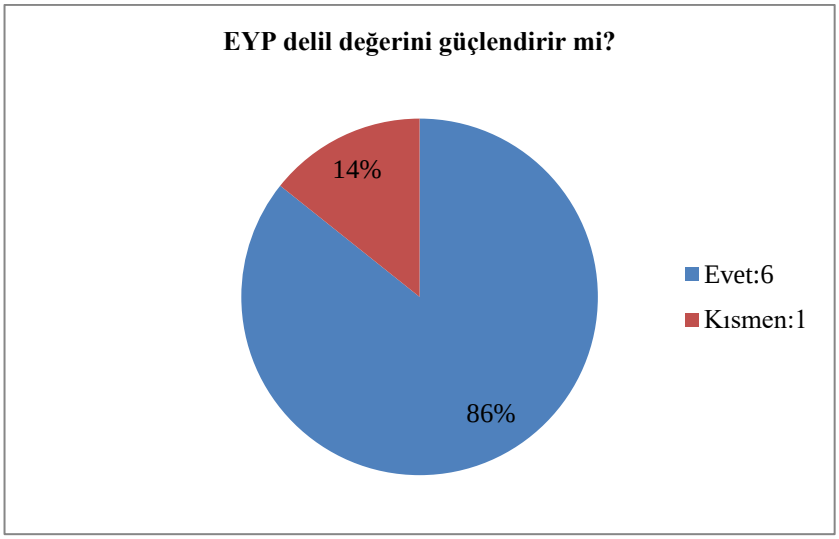
Şekil 14. Değerlendirme ve Delil Değeri İlişkisi

NİT01, "*değerlendirme yapmadan ayıklama-imha yapılamayacağını*" ifade etmiş, "*değerlendirme yaparken hukuki ve idari açıdan belgelere bir önem atfedildiğini*" açıklamıştır. NİT02, "*değerlendirmenin risk iştahını*[36] *belirlemeye yardımcı olarak delil değerini güçlendirdiğini*" belirtmiştir. NİT05 ve NİT08 de değerlendirmenin belgenin delil değerini güçlendireceği yönünde cevap vermiştir. NİT09, "*değerlendirmeyi arşivciliğin temel felsefelerinden biri*" olarak görmüştür. "*Neyin arşiv malzemesi olup olmayacağı hakkında fikir verdiğini*" ifade etmektedir. "*Değerlendirmeden daha uzun süreli saklanacak belgeler için kullanılacak üstverilerin belirlenmesinde faydalanılabileceğini*" dile getirmektedir. "*Değerlendirmenin sonucuna göre belgenin delil değerini etkileyecek arşiv imza, zaman damgası, kurumsal mühür ve arşiv mührü gibi uygulamaların kullanılabileceğini, uzun*

[36] Risk iştahı, kurumların faaliyetlerini yürütürken kabul edebilecekleri risk düzeyleri anlamına gelmektedir ("Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik", **R.G.**, S 29057, tar. 11.07.2014, (Çevrimiçi) https :// www. resmigazete. gov. tr/eskiler/2014/07/20140711-5.htm).

dönemli korumaya ilişkin üstverilerin eklenebileceğini" açıklamıştır[37]. NİT03 ise delil değeri ile bir ilişki kurulamayacağını belirtmiştir. NİT03'ün böyle düşünmesinin nedeninin kâğıt belgeler döneminde değerlendirmenin daha çok ayıklama ve imha süreçlerinde kullanılmasından kaynaklanabileceği düşünülmektedir. Değerlendirmenin belgenin delil değerini güçlendireceği kanaatinin saha uzmanları tarafından da paylaşıldığı görülmektedir.

Değerlendirmenin yanı sıra sorulan bir diğer soru EYP ile ilgilidir. Katılımcılara EYP'nin belgelerin delil değerini güçlendirip güçlendirmeyeceği sorulmuş, bu soruya yanıt veren 7 katılımcıdan 6'sı evet, 1'i kısmen cevabını vermiştir. EYP'nin delil değerini güçlendireceği kanaatinin saha uzmanları tarafından da paylaşıldığı görülmektedir. Bu soruda ifade edilen görüşlere ilişkin grafik şöyle belirtilebilir:



Şekil 15. EYP ve Delil Değeri İlişkisi

NİT01, "***EYP'yi delil değerinin korunmasında en güçlü unsur***" olarak değerlendirmiş, NİT08 "*EYP'deki bilgileri ayrı bir yerde de saklamanın gerekliliğine*" vurgu yapmıştır. NİT03, "*belgedeki üstverileri de içerdiğinden EYP'nin doğrulamada önemli bir fonksiyona sahip olduğunu*" belirtmiştir. NİT05 ve NİT07, "*EYP'nin delil değerini zenginleştireceğini*" ifade ederken, NİT05, "*EYP'siz belgelerin EYP'ye dönüştürülmesi gerekliliğine vurgu yapmış ve EYP 1.0 öncesi üretilen belgelerin*

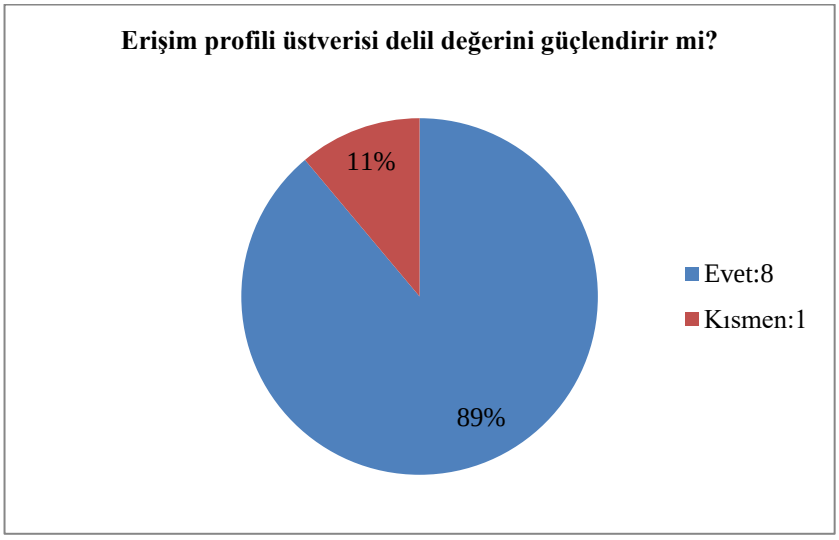
[37] Görüş A. Değerlendirmeyle delil değeri ilişkisi literatürde Duranti'nin çalışması üzerinden kurulabilir. Saha uzmanlarının aktardığı görüşlerin Duranti'nin ifade ettiği yaklaşımlarla uyumlu olduğu gözlenmektedir (Duranti, "Structural and Formal Analysis: The Contribution of Diplomatics to Archival Appraisal in the Digital Environment", **a.g.e.**).

akıbetine" dikkat çekmiştir. NİT02 ise "*EYP'nin tek başına yeterli olmayacağını ifade ederek yedek güvenilirlik unsuru olduğunu*" dile getirmiştir. NİT09, "***EYP'nin zenginleştirilerek arşivleme için kullanılabileceğini***" ifade etmiştir. "*Mevcut yapısında e-imza gibi belgelerin delil değerini işaret eden hususların olduğunu*" açıklamıştır. "*İçerisine koruma üstverisi, belgenin hangi donanım ve yazılımla açılabileceği, hangi yazılımın hangi versiyonuyla üretildiği bilgilerinin eklenmesini*" önermekte, "*EYP 3.0, hatta EYP 4.0'a hazırlık yapılmasını*" tavsiye etmektedir. "*Bunun için ZIP paketinin de ötesinde, ontolojik bir yapıyı gündeme alma zamanının geldiğini, aynı kurumda üretilmiş farklı EYP'lerin birbiriyle tanışıp konuşması gerektiğini*" aktarmıştır. Fakat, "*henüz dosyalamayı doğru gerçekleştiremeyen bir kamu düzeninde EYP'yi bu yönde kurgulamanın oldukça zor olduğunu*" söylemiştir[38].

Belge düzeyindeki son önerme sorusu, belgelere erişim profili üstverisi eklemenin delil değerini güçlendirip güçlendirmeyeceğidir. 8 kişi evet derken, 1 kişi kısmen cevabını vermiştir. NİT05, "*bu üstverinin delil değerini güçlendireceğini*" ifade etse de eksikliği hâlinde "*belgenin belge olma vasfının bozulmayacağını*" dile getirmektedir. Diğer katılımcılar, delil değerinin korunmasına katkı sağlayacağını beyan etmiştir. NİT09, "*genellikle üstverilerde bu hususun yer almadığını fakat log kayıtlarında mevcut olduğunu*" açıklamıştır[39]. Erişim profili üstverisinin delil değerini güçlendireceği kanaatinin saha uzmanları tarafından da paylaşıldığı görülmektedir. Cevapların dağılımına ilişkin grafik, aşağıdaki gibi oluşturulabilir.

[38] Görüş B. EYP'nin belgelerin delil değerinin korunmasında kullanılmasına ilişkin yaklaşımlar literatürde pek görülememektedir. Bu husus, tezin önerilerinden de biridir.

[39] Görüş A (INTERPARES, **INTERPARES 2: Experiential, Interactive and Dynamic Records**, **a.g.e.**).



Şekil 16. Erişim Profili Üstverisi ile İlgili Görüşler

Türk mevzuatında bir belgenin delil değerini koruyan en temel mekanizma e-imzadır. Durum böyle olunca, e-imzanın yanına başka mekanizmaların da eklenmesiyle delil değerinin daha güçlü korunabileceği düşünülmektedir. Bu kanaat katılımcılara da sorulmuştur. NİT01 ve NİT08, "*belgelerin özniteliklerinin korunmasının*" önemine vurgu yapmış, NİT01 "*tanımlamanın*" da bir güvenilirlik mekanizması olabileceğini ifade etmiştir[40]. NİT02, NİT05, NİT07 ve NİT09 "*üstverilerin*" bir güvenilirlik mekanizması olarak ele alınabileceğini belirtmiştir[41]. NİT01 ve NİT03, "*EYP*" 'den, NİT02 "*KEP*" 'ten bu konuda yararlanılabileceğini ileri sürmüştür[42]. NİT02, NİT07 ve NİT09 "*dosya planı ve dosyalamayı*" da bir güvenilirlik mekanizması olarak önermektedir[43]. NİT03, "*arşiv imzasının zorunlu hâle getirilmesini ve kurumsal mühür kullanılmasını*" tavsiye etmektedir. Yine bu konuda NİT04, "*arşiv mührünün kullanılabileceğini*" açıklamaktadır. "*Bu mührün yapısının e-imzalardan farklı olması gerektiğine*" dikkat çekmiştir[44]. NİT02, "*ülkemize özgü bir yazılımın belgelerin güvenilirliğini test edebileceğini*" ileri sürmektedir[45]. NİT07 ve

40 Görüş A (MacNeil, "Methods for Creating and Maintaning Reliable and Authentic Electronic Records", **a.g.e.**, s. 39-56).

41 Görüş A (INTERPARES, **INTERPARES 2: Experiential, Interactive and Dynamic Records**, **a.g.e.** ; Yalçınkaya, "E-devlet Üstveri Standardının Oluşturulması ve Türkiye için Modellenmesi", **a.g.e.**).

42 Görüş B. EYP ve KEP'in birer güvenilirlik mekanizması olarak kurgulanması aynı zamanda tezin önerilerinden biridir.

43 Görüş A (E-ARK, **a.g.e.**).

44 Görüş A (2017/21 sayılı Başbakanlık Genelgesi, **a.g.e.**).

45 Görüş A (Alpaydın, **a.g.e.**).

NİT08 "*log kayıtlarından*" bu konuda yararlanılabileceğini dile getirmektedir[46]. Güvenilirlik mekanizmalarına ilişkin görüşler, şu grafik ile gösterilebilir:

Şekil 17. Güvenilirlik Mekanizmalarıyla İlgili Öneriler

Elde edilen görüşler neticesinde üstverilerin bir güvenilirlik mekanizması olarak benimsenebileceği görüşünün ağırlık kazandığı görülmektedir. Durum böyle olunca, arşivsel güvenilirlik üstverisinin geliştirilmesine ihtiyaç duyulduğu anlaşılmaktadır.

Güvenilirlik mekanizması verileri değerlendirildiğinde üstverilerin ardından öne çıkan diğer bir mekanizmanın dosya planı ve dosyalama olduğu görülmüştür. Güvenilirlik mekanizması olarak açıklanan seçenekler içerisinde dosyalama işi, %16'lık bir orana karşılık gelmektedir. Hâliyle bu oran, dosyalamayı diğer seçeneklere göre öne taşımaktadır. Kurumların dosya planlarını oluşturup, dosyalama uygulamalarını bu plana göre yapmaları gerektiğinin saha uzmanları tarafından belirtildiği gözlenmektedir.

Bir diğer güvenilirlik mekanizmasının ise log kayıtları olabileceği ifade edilmiştir. Belgelerin hazırlanmasından düzenlenmesine, iletilmesinden dosyalanmasına kadar olan tüm süreçleri gösteren bu kayıtlar, seçenekler içerisinde üçüncü ağırlık noktayı oluşturmaktadır. %10'luk bir tercih oranıyla tanımlama ve KEP gibi araçlara göre daha öncelikli olduğu anlaşılmaktadır.

[46] Görüş A (ISO, **18829 Assessing ECM/EDRM Implementations: Trustworthiness**, **a.g.e.**).

Bu araçların yanı sıra güncelleştirilerek kullanılacak EYP'den ve belgelerin diplomatik özelliklerinden yararlanılabileceği belirtilmektedir. Bunların birer güvenilirlik mekanizması olarak benimsenmesi belgelerin delil değerini güçlendirebilir. Saha araştırmasında güvenilirlik mekanizması olarak benimsenebilecek diğer araçlar, tanımlama, KEP, arşiv imza ve e-mühür olarak açıklanmıştır. 2020 yılında güncellenen RYY'de kullanılması önerildiğinden arşiv imza ve e-mührün ilerleyen yıllarda mevzuat tarafından kabul edilmiş güvenilirlik mekanizması olarak benimsenebileceği düşünülmektedir.

Güvenilirlik mekanizmalarıyla ilgili dikkat çeken bir diğer görüş ise arşiv mührünün kullanılması ve yazılımsal güvenilirlik testlerinin yapılmasıdır. Bu mührün e-mühürden farklı bir yapıda olması önerilmektedir. Yazılımsal güvenilirlik testleri de dile getirilen bir diğer ciddi tavsiyedir. Kurumlarda milyonlarca belge oluşturulduğu göz önüne alındığında, bu testler insan eliyle değil yazılımlar aracılığıyla yapılmalıdır.

4.2.1.2. Teknolojik Koşullar Düzeyi

Delil değerinin korunmasına belgelerle ilgili olan dosyalama, arşivsel bağ ve üstveriler gibi hususların yanı sıra teknolojik yaklaşımların da önemli bir katkısı vardır. Bu yaklaşımların nelerden teşekkül edebileceği, saha uzmanlarının önermeleri ne derece benimsediği araştırılmak istenmiştir. Burada katılımcılara log kayıtları, belgelerin saklama konumları, EBYS kaynak kodları, teknolojik göç, e-imza, zaman damgası ve kullanılan donanım özellikleriyle ilgili sorular yöneltilmiştir.

İlk soru, delil değerinin korunmasında log kayıtlarından yararlanılıp yararlanılmayacağıyla ilgilidir. Tüm katılımcılar log kayıtlarının delil değerini güçlendireceği yönünde cevap vermiştir. Bu önermeye verilen cevaplara ilişkin şöyle bir grafik oluşturulabilir:

Şekil 18. Log Kayıtları ve Delil Değeri İlişkisi

Bu soru sorulurken katılımcılar log kayıtlarının bazı özelliklerine vurgu yapmıştır[47]. NİT03, NİT05 ve NİT09, "*log kayıtlarının belgedeki kişileri göstermesi gerektiğini*" ifade etmiş, NİT03 ve NİT09 "*bu kayıtların yapılan işlemin hangi görev dâhilinde ve ne zaman gerçekleştirildiğini göstermesine duyulan ihtiyacı"* dile getirmiştir. NİT03, "*log kayıtlarının kurumsal mühürle saklanmasını*" önermiştir[48]. Bununla birlikte, "*bu kayıtların anlamlı, anlaşılabilir ve sahih olmasının*" altını çizmiştir. NİT06, "*log kayıtlarının dışarıdan müdahaleye açık olmamasını ve zaman damgasıyla korunması zorunluluğunu*" beyan etmiştir. NİT05, "*bu kayıtların süresiz saklanmasını*" belirtirken, "*ISO 27001'e değil belge yönetimi yaklaşımına göre saklanmasını*" tavsiye etmektedir. Bunun için "***belge yönetiminde log standartlarının oluşturulmasının***" önemine vurgu yapmıştır[49]. NİT02, "*log kayıtlarının yeni formatlara ve yazılımlara aktarılabilir olmasını*", NİT04 ise "*belge bileşenlerine ilişkin log kayıtlarının tutulması gerektiğini*" ifade etmiştir. NİT09, "*log kayıtlarının provenansı göstererek dokümandan belgeye dönüş sürecini ispatlamasına*" dikkat çekmiş, "*belge hareketleri, sorumluluğu ve mülkiyetinin de takip edilmesini sağladığını*" açıklamıştır. Log kayıtlarını "*üstveriden sonra delil değeri açısından bakılması gereken ikincil konu*" olarak değerlendirmektedir. Fakat, "*Türkiye'de log kayıtlarının içerdiği bilgi*

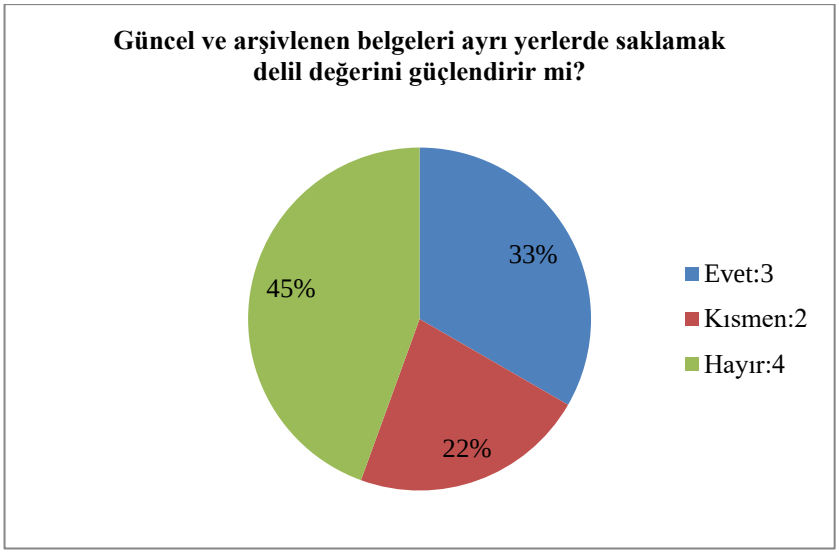
47 Görüş A (**a.g.e.**).
48 Görüş B. Log kayıtlarının kurumsal mühürle saklanması önerisi yeni bir yaklaşım olarak görülmektedir.
49 Görüş B. Belge yönetiminde log standartlarının oluşturulması bu çalışmanın önerilerinden biridir.

açısından istenilen seviyede olmadığını" ileri sürmektedir. Bununla birlikte, NİT08, "*log kayıtlarının silinip silinmediğini denetleyen bir mekanizmanın kurulmasını*" teklif etmektedir. NİT07 ve NİT09, "***log kayıtlarının belgeyle birlikte delil olarak kullanılabileceğini***" iddia etmektedir. Log kayıtlarının özellikleriyle ilgili belirtilen hususlar şöyle gösterilebilir:

Şekil 19. Log Kayıtlarıyla İlgili Görüşler

Teknolojik koşullar düzeyindeki bir diğer soru, güncel ve arşivlenen belgelerin ayrı yerlerde saklanmasının delil değerini güçlendirip güçlendirmediğiyle ilgilidir. 3 kişi evet, 2 kişi kısmen, 4 kişi hayır cevabını vermiştir. Kısmen cevabını verenler gerekli şartlar sağlanamadığı takdirde güncel ve arşivlenen belgelerin ayrı yerlerde saklanması gerektiğini belirtmiştir. Dolayısıyla, bu yönde verilen cevapların evete yakın olduğunu söylemek mümkünse de güncel ve arşivlenen belgeleri ayrı yerlerde

saklamanın sahada güçlü bir şekilde desteklenmediği görülmektedir. Cevaplara ilişkin grafik şu şekildedir:

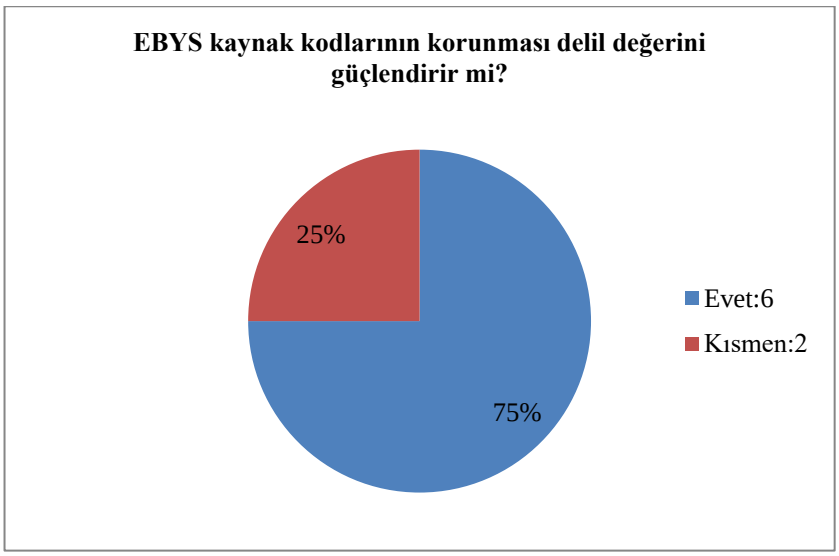


Şekil 20. Güncel ve Arşivlenen Belgelerin Ayrı Yerlerde Saklanmasına İlişkin Görüşler

Bu soruda NİT04, NİT08 ve NİT09 evet yönünde beyanda bulunurken, NİT08 bunun aksi durumunda, yani güncel ve arşivlenen belgeleri aynı yerlerde saklamak durumunda "*arşivi küçümsemek gibi bir yaklaşımla karşı karşıya kalınacağını*" ifade etmiştir. NİT09, "*uzun süre saklayacağımız belgelerle, kısa süreli saklayacaklarımız bir olur mu*" sorusunu sormaktadır. Bu nedenle "*belge yönetimi ile arşiv yönetiminin ayrıldığını*" belirtmektedir. NİT02, "*güncel belgelerle arşivlik belgeler arasındaki makasın daraldığına dikkat çekerek belgenin delil değerini ortamın değil, oluşma niteliklerinin belirlediğine*" vurgu yapmıştır. Fakat, "*bu niteliklerin kriter hâline getirilememesi durumunda güncel belgelerle arşivlenen belgeleri aynı yerde saklamanın delil değerini olumsuz etkileyeceğini*" ileri sürmektedir. NİT03, "*formatla ilgili bir değişiklik söz konusuysa bu iki türdeki belgelerin ayrı yerlerde saklanabileceğini belirtmiş, fakat elektronik ortamda bu makasın daraldığını*" dile getirmiştir. Durum böyle olunca, NİT02 ve NİT03'ün cevapları kısmen kategorisinde değerlendirilmiştir. Bu görüşlere rağmen, NİT01, NİT05, NİT06 ve NİT07 bu ayrımın pek de önemli

olmadığını ifade etmiştir. Bu görüşte olmalarının nedeni, belgenin delil değerini ortamın değil, oluşma niteliklerinin belirlediğine inanmalarıdır[50].

Bir diğer soru EBYS yazılımlarının kaynak kodlarını muhafaza etmenin belgelerin delil değerinin korunmasına olumlu bir etkisi olup olmadığı üzerinedir. 8 kişi soruyu cevaplamış; 6 kişi evet, 2 kişi kısmen cevabını vermiştir. EBYS kaynak kodlarını korumanın delil değerini güçlendireceği kanaatinin saha uzmanları tarafından da paylaşıldığı görülmektedir. Elde edilen cevaplar şöyle belirtilebilir:

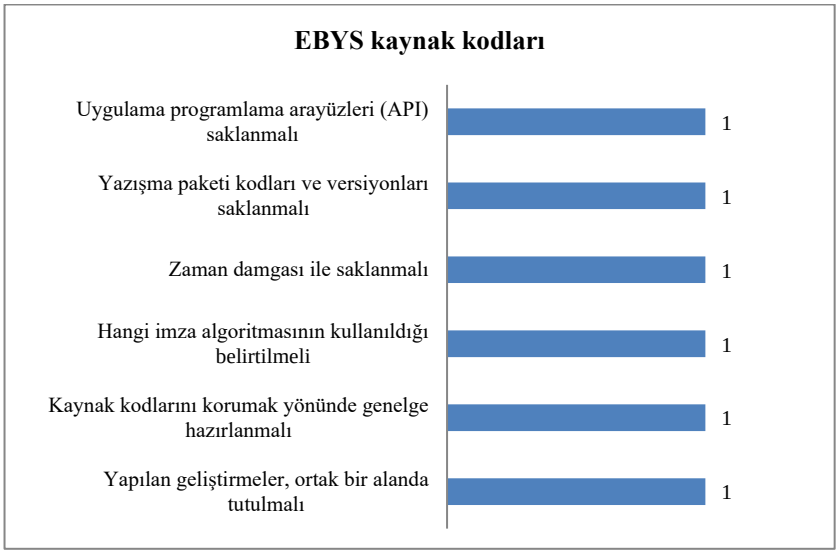


Şekil 21. EBYS Kaynak Kodları ve Delil Değeri İlişkisi

Bu soruya NİT01, NİT02, NİT03, NİT05, NİT06 ve NİT07 evet yönünde cevap verirken, NİT08 ise "*belgeyi tek başına değerlendirdiğimizde gerekli olmayabileceğini fakat sistemsel olarak ihtiyaç duyulacağını*" belirtmiştir. NİT09, "*kaynak kodlarının bir arşiv malzemesi olarak korunması gerektiğini fakat delil değerini etkilemeyeceği yönünde bir cevap veremeyeceğini*" aktarmıştır. NİT05, "*uygulama programlama arayüzleri (application programming interface [API]) ve yazışma paketi kodları ile*

50 Belge yönetimi standartlarında güncel belge ile arşivlik belgelerin saklama konumlarının farklı olmasıyla alakalı yönlendirici bir norm görülememiştir. Ancak ISO 27040'da stratejik varlıkları diğer varlıkların bulunduğu disklerden ayrı saklamak gerektiği belirtilmektedir. Bunun nedeni stratejik varlıkları diğer malzemelerden farklı koşullarda saklamak gerekliliğinden kaynaklanmaktadır. Böylece yaşanabilecek herhangi bir teknik ve teknolojik sıkıntıda zararların en aza indirilmesi hedeflenmektedir (ISO, **27040 Security Techniques: Storage Security**, **a.g.e.**, s. 43-44). Hâl böyle olunca arşivlenen malzemelerle güncel belgelerin ayrı yerlerde saklanması gerektiği düşünülmektedir.

versiyonlarının saklanmasını" önermiştir. NİT06, "*kaynak kodlarının zaman damgasıyla saklanmasına*" dikkat çekmiş, NİT03, "*EBYS'nin kaynak kodunda hangi imza algoritmalarının kullanıldığının belirtilmesini*" vurgulamıştır[51]. Aynı zamanda, "***kamunun farklı şirketler tarafından geliştirilen EBYS'lerin kaynak kodlarının korunması yönünde bir genelge hazırlamasını***" tavsiye etmiştir. Bu genelgede, "*yazılımcıların kaynak kodlarında yaptığı geliştirmelerin ortak bir alanda tutulması*" yönünde bir hükmün bulunması dile getirilmiştir[52]. Kaynak kodlarıyla ilgili görüşler şöyle resmedilebilir:



Şekil 22. EBYS Kaynak Kodlarının Korunmasına İlişkin Görüşler

Tüm bu sorularla birlikte, teknolojik göç ve delil değerinin korunmasında arşivsel güvenilirlik yaklaşımlarından nasıl faydalanıldığı sorulmuştur. Burada 4 katılımcı Devlet Arşivleri Başkanlığının kuralları belirlemesi gerektiğini ifade etmektedir. NİT07, "*öncelikle Milli Arşiv Kanunu'nun hazırlanmasını ve bu kanunda teknolojik göçle ilgili hususlara yer verilmesini*" dile getirmektedir. NİT09 da "*Milli Arşiv Kanunu'na vurgu yaparak teknolojik yatırımların yapılmasını ve politikalar geliştirilmesini*" önermektedir. NİT02, "***teknolojik göçte uygulanacak kuralları Devlet Arşivleri Başkanlığının belirlemesini***", NİT08, "*Başkanlığın kullanılacak*

51 Görüş A (UNESCO, **Software Heritage Web Sitesi**, **a.g.e.**).
52 Görüş B. NİT 03'ün dile getirdiği bu hususlar, aynı zamanda tezin önerilerinden biridir.

formatları belirleyerek hangi formatın geçersiz olacağını duyurmasının" önemine vurgu yapmıştır[53].

Bu hususların yanı sıra, NİT02, NİT03, NİT07 ve NİT09 "*göç ettirmenin onaylanmasına*" dikkat çekmiştir. NİT03, "***kurumların teknolojik göç sonrasında belgenin özniteliklerinin değişmediğini göstermesi gerektiğini***" belirtmiştir[54]. NİT09'un bu hususstaki görüşleri şöyle ifade edilebilir: "*Belge gelecekte başka bir formata dönüştürüldüğünde e-imza ve mühür doğrulanmalıdır. Quantum bilgisayarlarda dosya formatı yapısının değişebileceği öngörülmektedir. Belgenin gerçekliği ve sahihliği konusunda otorite bir makam olmalıdır. Eski teknolojiyle üretilmiş bir belgenin değişmezliğini ispatlayan bir veri varsa belgenin doğru olduğuna kanaat getiririz. Bugün, sağlam ve kristal bir saray gibi varlığını koruyan teknolojik yapı, yarın metruk bir hâlde göründüğünde bile burada üretilen belgelerin sağlamlığını gösteren bir mekanizmaya ihtiyaç duyulmaktadır*".

Bununla birlikte, NİT01, "*teknolojik göç sırasında içerik, kontekst ve yapının korunmasının*" altını çizmiştir. NİT02 ve NİT09, "***müstakil bir teknolojik dönüşüm süreci üstverisinin***" kurgulanabileceğini önermektedir[55]. NİT09, "*belgenin dosya formatları tarihçesini incelemenin gerekli olduğunu*" ifade etmiştir. "*Firma bağımlılığının ortadan kaldırılmasını, standartlaştırılmaya ihtiyaç duyulduğunu*" belirterek "*dosya formatlarının belgenin delil değeri açısından oldukça önemli olduğunu*" dile getirmiştir. NİT02, "*belge göç ettirilemiyorsa delil değerinden şüphe duyulacağını*" belirtmiştir. NİT03 ve NİT09 "*Birlikte Çalışabilirlik Esasları Rehberi'ne atıfta bulunarak uluslararası tanınırlığı olan formatların kullanılabileceğini*" ileri sürmüştür[56]. Burada belirtilen görüşler şöyle gösterilebilir:

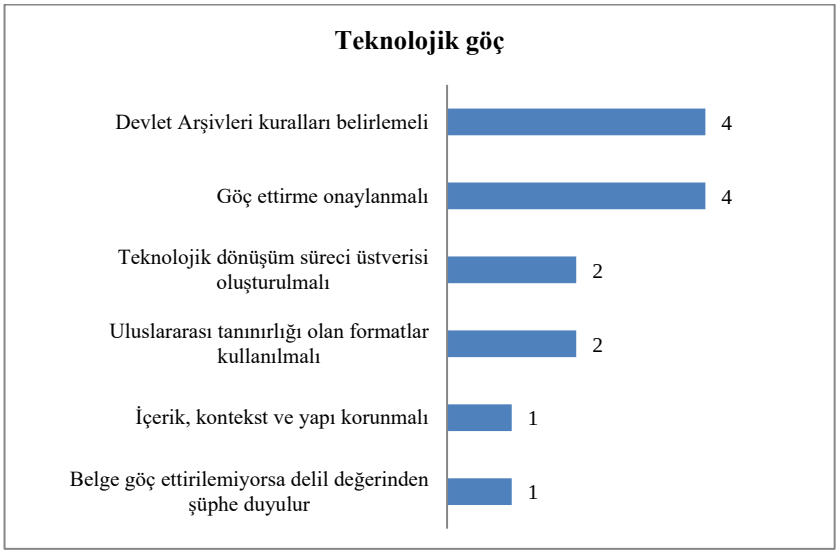
---

53 Görüş A. Çeşitli ülkelerde devlet arşivlerinin bu konulara öncülük ettiği bilinmektedir (Yunus Emre Arısoy, "Türkiye'de Elektronik Belge Yönetiminde Milli Arşiv Politikalarının Geliştirilmesi", Yayınlanmamış Doktora Tezi, Ankara, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı, 2018).

54 Görüş A (ISO, **13008 Digital Records Conversion and Migration Process**, **a.g.e.**).

55 Görüş A (Long Term Records Management Project, **a.g.e.**).

56 Görüş A (Arısoy, **a.g.e.**).



Şekil 23. Teknolojik Göçle İlgili Görüşler

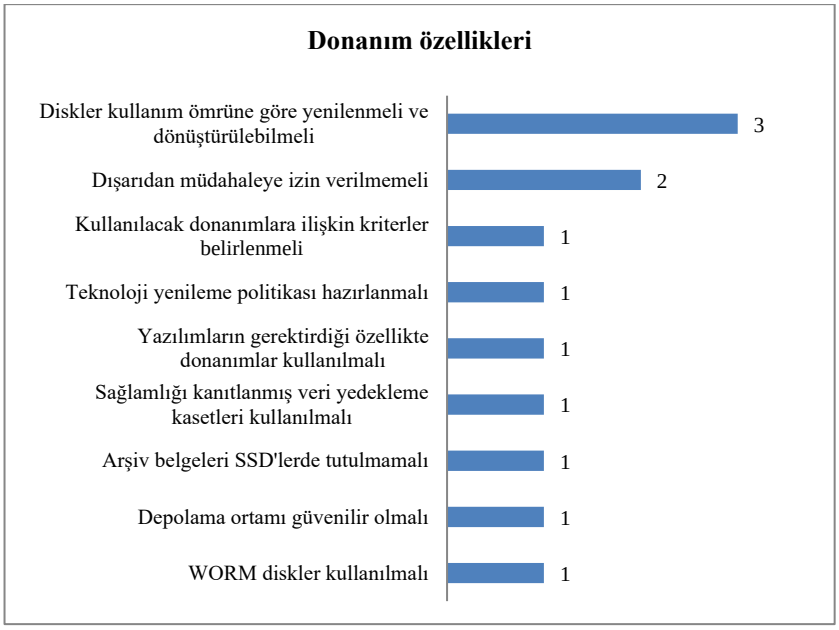
Bunların yanı sıra katılımcılara e-imza ve zaman damgasıyla ilgili sorunlar da sorulmuştur. NİT03 ve NİT09 "*imzaların kırılma ihtimalinden*" söz etmiş, NİT03 "*sertifikaların kontrol edilemediğini*" belirtmiştir. NİT02 ve NİT09 "*kuantum teknolojisinin şifreleri çözebileceğini*" dile getirmiştir. NİT09, "*kullanılan e-imza teknolojisinin eskiyebileceğine hatta yerle bir olabileceğine"* vurgu yapmıştır. NİT07, "*sertifika hizmeti veren kuruluşların faaliyetlerini durdurması ve siber saldırılara*" dikkat çekmiş, NİT01, "*doğrulama sorunları yaşandığını*" ifade etmiştir. NİT03, bunun için "*TÜBİTAK'ın kurumlardaki e-imza süreçlerini denetlemesini ve daha güçlü algoritmaların kullanılmasını*" önermiştir. NİT02, "*kamu belgelerinde sertifika geçerlilik süresinin söz konusu olmaması*" gerektiğini dile getirerek "*e-imza arşivlerinin yedeklenmesini*" tavsiye etmiştir. NİT09, "*zaman damgalarında sürtünme kuvvetinden kaynaklanan 100 yılda bir görülen* ***zaman sapmasına***" dikkat çekmiştir. NİT05, "*sunuculara ve felaket kurtarma merkezlerine erişilememesinin ihtimal dâhilinde olduğunu*" belirtirken, NİT04, "*e-imza altyapısından farklı olacak bir arşiv mührünün kullanılabileceğini* "dile getirmiştir[57]. Burada belirtilen görüşler şöyle gösterilebilir:

[57] Görüş A (2017/21 sayılı Başbakanlık Genelgesi, **a.g.e.**).

Şekil 24. E-imza ve Zaman Damgası Sorunlarına İlişkin Görüşler

Bununla birlikte, belgelerin delil değerinin başarılı bir şekilde korunması için hangi özelliklerde donanımların kullanılabileceği sorulmuştur. Bu soruda NİT02, "*kamunun kullanılacak donanımlara ilişkin kriterleri belirlemesini*", NİT09, "*teknoloji yenileme politikalarının hazırlanmasını*", NİT08, "*yazılımların gerektirdiği özellikte donanımlar kullanılmasını*", NİT03, NİT05 ve NİT09, "*kullanılan disklerin kullanım ömrü bitince yenilenmesini ve dönüştürülebilir olmasını*" ifade etmiştir. NİT09, "*harddisklere düzenli test yapılabileceğini, testten başarılı geçemeyenlerin imajının alınıp yeni bir diske aktarılabileceğini ve bu başarısız disklerin geri döndürülemeyecek şekilde imha edilebileceğini*" önermektedir. NİT05, "*sağlamlığı kanıtlanmış veri yedekleme kasetlerinin kullanılmasını*" tavsiye etmektedir. NİT01, "*arşivlik belgelerin Solid State Disk (*SSD - Katı Hâl Sürücüleri*)'lerde saklanmaması gerektiğini*" belirtmektedir. NİT01 ve NİT06, "*kullanılacak donanımların dışarıdan müdahaleye izin vermeyecek yapıda olmasının*" altını çizmektedir. NİT07, "*depolama ortamının da güvenilir olması gerektiğini ifade ederken, bir kez yazılabilir çok kez*

okunabilir (Write Once Read Many – WORM) disklerin kullanılmasını" önermektedir[58]. Donanım özellikleriyle ilgili görüşler şöyle resmedilebilir:



Şekil 25. Donanım Özellikleriyle İlgili Görüşler

Kurumlardaki e-belge yönetimi uygulamalarının belge yönetimi ve arşivcilikten ziyade daha çok bilgisayar biliminin bir parçasıymış gibi görülmesi sahada karşılaşılan sorunlardan biri olarak kabul edilmektedir. NİT09 da bu görüşü desteklemektedir. "*EBYS'lerin bilgisayar bilimiyle ilintili ilerlemesi, veri tabanı gibi düşünülmesi olumsuz sonuçlar doğurur*" demektedir. Bu hususun "*geri dönüşü olmayan hatalara yol açabileceğini, yapay zekâ, büyük veri gibi araçlarla soruna çözüm bulunacağı düşünülse de bunun çok maliyetli olduğunu ve başarı oranının %60'ı geçemeyeceğini*" ifade etmektedir[59].

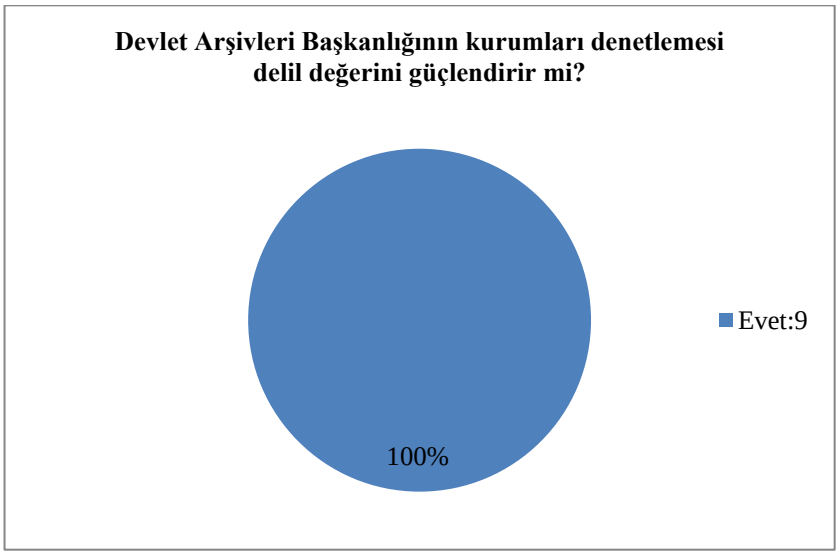
58 Görüş A (ISO, **18492 Long-term Preservation of Electronic Document-based Information**, **a.g.e.**). SSD'lerin kullanılmaması görüşü sahadaki pratiklerin bir yansıması olarak değerlendirilmektedir.

59 Görüş A. Bu görüş, Julie McLeod'un bilgisayar biliminin belge yönetiminde %20'lik bir işe öncülük etmekteyken, %80'ini yürütüyormuş gibi algılandığını ifade ettiği çalışmasıyla uyumluluk göstermektedir (Julie McLeod, "On Being Part of the Solution, not the Problem", **Records Management Journal**, C. 22, No: 3, 2012, s. 193).

4.2.1.3. Kurum Düzeyi

Saha araştırması kapsamında belge düzeyi ve teknolojik koşullarla alakalı nitel bulgular yanında bir diğeri kurum düzeyiyle alakalı olanlardır. Bu düzeyde Devlet Arşivleri Başkanlığının kurumları denetlemesi ve güvenilirliğin korunmasına katkısı, yedekleme ve log kayıtları rehberinin hazırlanması ile risk yönetiminin yapılması gibi sorular sorulmuştur.

Burada katılımcılara yöneltilen ilk soru, Devlet Arşivleri Başkanlığının kurumların belge yönetimi politikalarını denetlemesinin belgelerin delil değerinin korunmasına katkı sunup sunmadığı yönündedir. Tüm katılımcılar evet cevabını vermiştir. Başkanlığın kurumları denetlemesinin delil değerini güçlendireceği kanaatinin saha uzmanları tarafından paylaşıldığı görülmektedir. Bu önermeye ilişkin cevaplar şöyle gösterilebilir:



Şekil 26. Devlet Arşivleri Başkanlığının Kurumları Denetlemesi ve Delil Değeri İlişkisi

Kurum düzeyindeki bir diğer soru ise Devlet Arşivleri Başkanlığının bu süreçte neler yapabileceğiyle ilgilidir. Burada alınan cevaplar şöyle ifade edilebilir: NİT01 ve NİT09 "*Başkanlığın elektronik arşiv ve belge yönetimi politikası geliştirmesi gerektiğini*" dile getirmiştir. Ayrıca, NİT01 "***Başkanlığın kurumları denetleyip yaptırımlar uygulamasını***" önermiştir. NİT09, "*Başkanlığın çerçeve bir politika geliştirerek kurumlara özerklik tanımasını fakat kurumları bu politikanın dışına çıkmamak noktasında denetlemesini*" tavsiye etmektedir. Bununla birlikte, NİT01,

NİT02, NİT03 ve NİT07, "*Başkanlığın e-belge ve arşiv yönetimindeki süreçler hakkında standartlar ve teknik rehberler hazırlaması gerektiğini*" ileri sürmüştür. NİT03, "*Başkanlığın kendisine gelecek belgeler için kabul şartlarını belirleyip bu belgelere nasıl bir muamele yapacağını açıklamasının kurumlar için bir yol haritası oluşturulmasını sağlayacağını*" beyan etmektedir.

Bu hususlarla birlikte, NİT02, NİT06 ve NİT09 "***teknolojik öngörü politikasının hazırlanmasına***" dikkat çekmektedir. NİT02, "*Devlet Arşivleri Başkanlığının Dijital Vizyon Belgesi oluşturmasının gerekliliğine vurgu yaparak bu belgede yapay zekâ, Endüstri 4.0 ve 5G ile ilgili hususların bulunmasını*" teklif etmektedir. Bununla birlikte, NİT03, NİT04, NİT05 ve NİT06 "*Başkanlığın veri koruma politikası hazırlamasını*" tavsiye etmiştir. NİT02, "*zorunlu üstverilerin belirlenmesini*" önerirken, NİT01, NİT02 ve NİT08 "*milli bir format belirlenmesinin*" gerekliliğine vurgu yapmıştır. NİT08'in "*log kayıtlarının silinip silinmediğini denetleyen bir mekanizma kurulması*" ile NİT05'in "*API ve yazışma paketi kodları ile versiyonlarının saklanması*" önerisinin Devlet Arşivleri Başkanlığı tarafından gerçekleştirilebileceği düşünülmektedir.

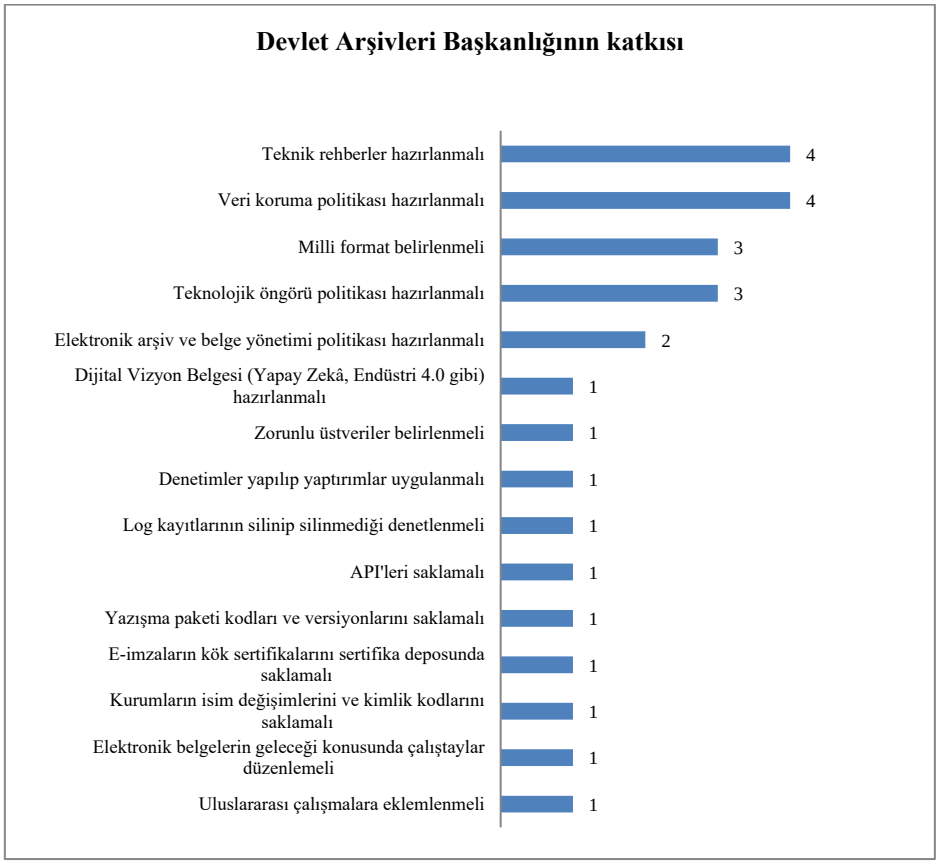
Aynı zamanda NİT05, "*Devlet Arşivleri Başkanlığının e-imzaların kök sertifikalarını sertifika deposunda saklamasını ve kurumların isim değişimleri ve kimlik kodlarını muhafaza etmesini*" önermektedir[60]. NİT09, "*Başkanlığın e-belgelerin geleceği konusunda bir çalıştay düzenleyerek bilim insanları, uzmanlar ve kamu kurumlarının bir araya getirilmesini*" tavsiye etmekte ve "*uluslararası çalışmalara eklemlenmesini*" dile getirmektedir[61]. Bu soruda NİT09, "***arşivlerin veri yığınından ziyade bir değer***" olduğunu öne sürmekte, "***Devlet Arşivlerinin o ülkenin en yüce noter kurumu***" olduğunu belirtmektedir. "*Manipülasyona uğramış, tahrif edilmiş herhangi bir sahte belgenin Devlet Arşivlerinde yer almamasını, tarihi değere sahipmiş gibi muamele görmemesi*" gerektiğini ifade etmektedir. "*E-belgelerin güvenilirliğini sağlamanın Devlet Arşivlerinin temel bir görevi*" olması gerektiğinin altını çizmiştir. Buna rağmen, "*Devlet Arşivleri Başkanlığının ilgili biriminde konuyla ilgili uzmanların çalışmadığını, bu konuda derin bilgiye sahip kişilerin artık bu*

---

60 Görüş B. NİT05'in görüşleri literatürde yeteri kadar görülememiştir. Bu görüşler, tezin önerileri arasında yer almaktadır.

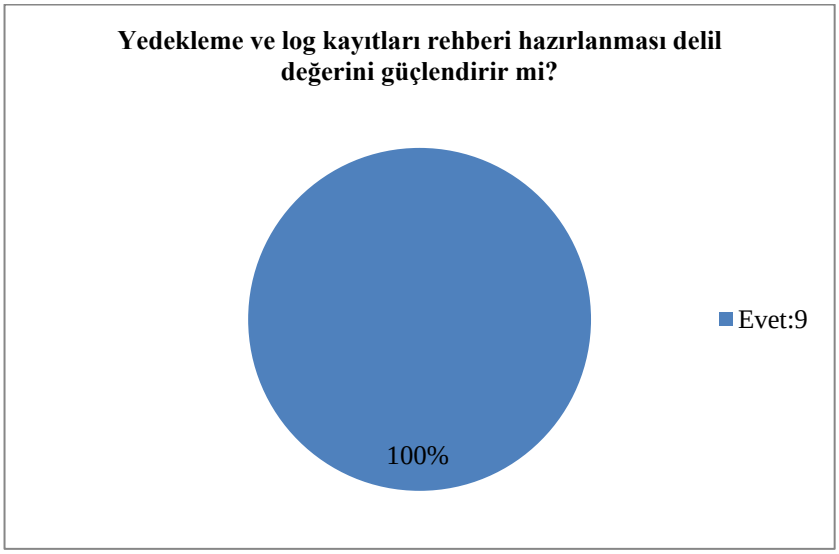
61 Görüş A (Arısoy, **a.g.e.**, s. 56-76. ; National Archives of Australia, **Legislation, Policies, Standards and Advice**, (Çevrimiçi) http :// www. naa. gov. au/ information-management/ information-governance/legislation-standards/index.aspx, 14 Ekim 2020).

birimde görev yapmadığını" açıklamaktadır. "*Farklı disiplinlerden gelen, e-belgelerin üretim mekaniğini kavrayamamış uzmanların çalışmasının olumsuz sonuçlara yol açacağını*" ileri sürmektedir. Devlet Arşivleri Başkanlığının sürece katkısıyla ilgili ifade edilen görüşler şöyle gösterilebilir:



Şekil 27. Devlet Arşivleri Başkanlığının Katkısına İlişkin Görüşler

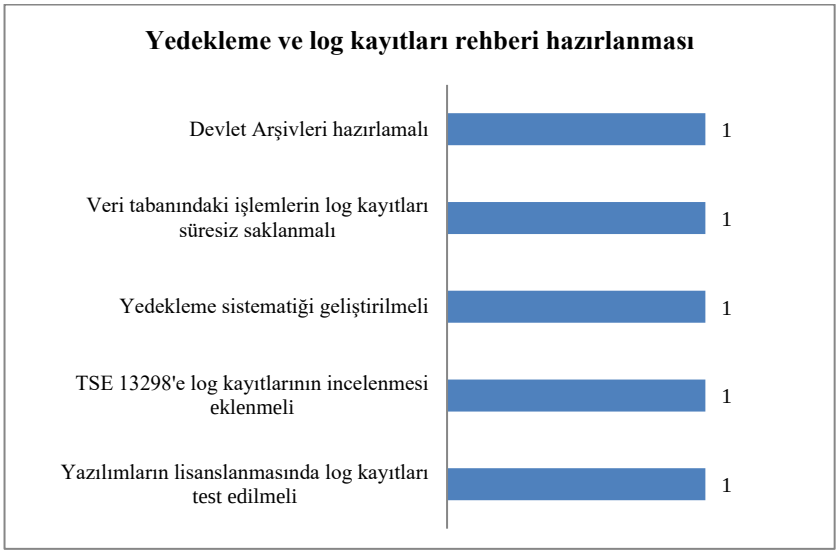
Kurum düzeyindeki bir diğer soru da kamunun yedekleme ve log kayıtları oluşturma işlemleri için bir genelge ya da rehber hazırlamasının belgelerin delil değerini koruyup korumayacağıyla ilgilidir. Bu soruya tüm katılımcılar evet cevabını vermiştir. Bu hususun delil değerini güçlendireceği kanaatinin saha uzmanları tarafından da paylaşıldığı görülmektedir. Bu konudaki cevaplara ilişkin grafik şöyle belirtilebilir:



Şekil 28. Yedekleme ve Log Kayıtları Rehberi ile Delil Değeri İlişkisi

NİT01, "*bu konuda kurumlarda veri merkezi oluşturulmasına dikkat çekerek Devlet Arşivleri Başkanlığının kurumların konuyla ilgili nasıl önlemler alacağını belirten rehberler hazırlamasını*" önermiştir. Böylece, "*kamu güveninin artacağını*" ifade etmiştir. "*Erişemediğin veri senin değildir*" demektedir. NİT02 de bu rehberi Başkanlığın oluşturması gerektiğini dile getirmiştir. Ayrıca, "*bazı hassas belgelerin teknolojik güvenilirlik meselesi geçene kadar fiziki ortamda üretilmesini*" ileri sürmektedir. NİT06, "*yazılımcıların kullandıkları log kütüphanelerinin her şeyi kayıt altına aldığı kabulüyle hareket etse de kayıtların değiştirilebilir olduğunun gözden kaçırıldığına*" dikkat çekmektedir. NİT05, "*veri tabanı düzeyinde yapılan işlemlere ilişkin log kayıtlarının süresiz saklanmasını*" önermektedir. NİT02, "bir *yedekleme sistematiği geliştirilmesine*" duyulan ihtiyacı vurgulamıştır. NİT09, log kayıtlarının incelenmesi meselesinin TS 13298'e eklenebileceğini belirterek yazılımların lisanslanması sürecinde log kayıtlarının da test edilmesini tavsiye etmektedir[62]. Bu soruda dile getirilen görüşler şöyle gösterilebilir:

[62] Görüş A (ISO, **18829 Assessing ECM/EDRM Implementations: Trustworthiness**, **a.g.e.** ; Arısoy, **a.g.e.**).



Şekil 29. Yedekleme ve Log Kayıtları Rehberinin Hazırlanmasıyla İlgili Görüşler

Kurum düzeyinde katılımcılara yönetilen son soru, risk yönetimi çerçevesinde geliştirilen önerilerin uygulanıp uygulanmamasıyla delil değerinin korunması arasında bir ilişki kurulup kurulamayacağı yönündedir. NİT06 bu soruya cevap vermemiş, diğer 8 katılımcı evet cevabını vermiştir. Risk yönetiminin delil değerini güçlendireceği kanaatinin saha uzmanları tarafından da paylaşıldığı görülmektedir. Alınan cevaplara ilişkin şöyle bir grafik oluşturulabilir:

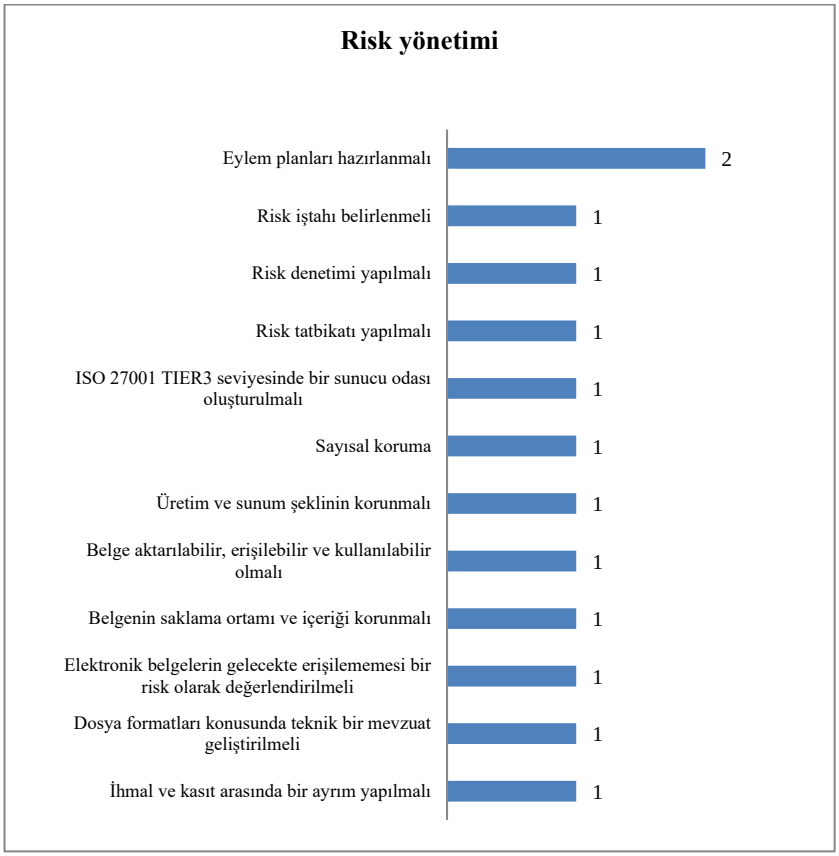
Şekil 30. Risk Yönetimi ve Delil Değeri İlişkisi

NİT02, "*risk iştahının belirlenmesine vurgu yapmış*", NİT07 "*risk denetimi yapılmasını*" önermiştir. NİT04, "*risk tatbikatlarının yapılarak eylem planlarının hazırlanmasını*" tavsiye etmiştir. NİT09, "*kurumların, müstakil olarak e-belgeler için risk yönetimi yapmalarından ziyade, afet planları içerisinde e-belgelerle ilgili hususları ifade edebileceğini*" dile getirmiştir. "*EBYS ile ilgilenen birime bu işin tevdi edildiğinde risklerin belirleneceğini fakat kâğıt üstünde kalabileceğini"* söylemektedir. "*ISO 27001 TIER3 seviyesinde bir sunucu odası oluşturulmasına*" dikkat çekmiştir.

Bu hususlarla birlikte, NİT09, "*sayısal korumayı risk yönetiminin bir parçası*" olarak kabul etmektedir. Bu konudaki görüşleri şöyle ifade edilebilir: "*Belgelerin erişilebilirlik, aktarılabilirlik, kullanılabilirlik gibi özelliklere sahip olması gerekir. Belgenin bulunduğu fiziki ortam ve içerik de muhafaza edilmeli; üretim ve sunum şekli korunmalıdır. Belgenin otantikliği meselesinin altında da bu husus yer almaktadır"*. NİT09, "*e-belgelerin gelecekte erişilememesini de bir risk*" olarak değerlendirmektedir. "*Dosya formatları konusunda teknik bir mevzuatın geliştirilebileceğini*" ileri sürmektedir. "*Mesela ürettiğimiz bir belgede farkında olmadan 30 yıl sonra ortaya çıkan ve tüm arşivi kemiren bir virüs ortaya çıkarsa veya bu virüs verileri değiştirirse ne yapacağız. Burada hayalperest bir yaklaşım ortaya koymak gerekiyor"* demektedir.

NİT09 bu görüşlerine ek olarak "***ihmal ve kasıt arasında bir ayrım***" yapılmasını savunmaktadır. Bu görüşünü şöyle açıklamaktadır: "*Bir saklama biriminin kendi kaderine bırakılması, belgenin delil değeri için bir tehdit oluşturur, hatta belgenin içeriğinin yok olmasına neden olabilir. Bu ihmal midir kasıt mıdır, tartışmalı bir mesele*". Bu nedenle "*bir yöneticinin e-belgeler için gerekli tedbirleri almaması bir kasıt olarak değerlendirilmeli*" görüşündedir. NİT09, "*bir yönetici kurumun peyzajı için 5 milyon TL harcayabiliyorken, sunucu kabini için 50 bin TL harcamamaktadır. Popülist politikalar terk edilerek optimal çözümler içeren teknolojik yatırımlar yapılmalıdır*" demektedir[63]. Bu soruda tüm katılımcıların ifade ettikleri görüşler şöyle gösterilebilir:

[63] Görüş A (Thurston, "Digitization and Preservation: Global Opportunities and Cultural Challenges", **a.g.e**., s. 32).



Şekil 31. Risk Yönetimiyle İlgili Görüşler

Risk yönetimiyle ilgili görüşlerde en çok öne çıkan öneri, eylem planlarının hazırlanmasıdır. Kurumlar, e-belgelere yönelik riskleri belirleyip bunlara karşı ne tür önlemler alınması gerektiğini açıklamalıdır. Bu hususun yanı sıra risk denetimleri ve tatbikatlarının yapılması, ISO 27001 Standardı'nın benimsenmesi, sayısal koruma politikalarının hazırlanması gibi öneriler de dile getirilmiştir.

4.2.2. Nicel Bulgular

4.2.2.1. Belge Düzeyi

Nicel araştırmada kurumlara sorulan 77 soru, belge düzeyiyle ilgilidir. Bunların 59'u zorunlu, 18'i seçmeli olarak belirlenmiştir. Zorunlu kriterleri ölçen soruların katsayısı 0.339 (20/59), seçmelileri ölçenlerin ise 0.277 (5/18) olarak hesaplanmıştır. Kurumlar, bu düzeydeki tüm sorulara olumlu cevap verirse puanları 25'e tamamlanmaktadır. Zorunlu kritik soruların olduğu durumlarda zorunlu soruların katsayısı 0.1356, seçmelilerin ise 0.1108 olmaktadır. Başarı düzeylerindeki yüzdelik

puanların ondalık kısmı iki basamak olarak verilmiştir. Belge düzeyindeki sorulara verilen cevaplar neticesinde oluşan tablo, EK 9'da gösterilmektedir. Bununla birlikte, kurumların ilgili sorularda elde ettikleri başarı oranı tablolarda belirtilmektedir.

Bu düzeyde, belge profilinde kullanılan üstveriler, dosya planı ve dosyalama pratikleri, belgelerin özgünlüğünün tasdik edilmesine ilişkin kontroller, tasfiye süreçleri, tanımlama uygulamaları gibi hususlarla ilgili sorular sorulmuştur. Bu sorular aracılığıyla kurumlarda kullanılan üstveriler incelendiğinde, araştırmaya katılan tüm kurumların üstverilere ilişkin hususların sorulduğu 2, 3 ve 4. sorulara aynı cevabı verdiği görülmektedir. Bunun nedeninin kurumların aynı yazılımı kullanması olduğu düşünülmektedir. Kurumların, yazılımın sunduğu üstverileri benimsediği, bu konuda yeni bir üstveri ekletmediği söylenebilir.

Değerlendirme kriterinde belgelerin form özelliklerinin üstveri olarak kurgulanmasında aranan hususların tüm kurumlarda benimsendiği gözlenmektedir. Ancak, hiçbir kurumda formatın bir üstveri olarak belirlenmediği görülmektedir. Bunun nedeni, EYP'de bu alanın "mime type"[64] olarak karşımıza çıkması olabilir. Fakat EYP ile e-belgeler farklı yapılara sahiptir. Belge üstverisinde de formatın yer alması, ileride gerçekleşecek teknolojik göç işlemlerinde kolaylık sağlayacak ve belgenin güvenilirliğinin sorgulanmasında bir karine sunabilecektir.

Ancak, kurumlarda belgenin güvenilirliğinin korunmasında yardımcı olacağı düşünülen üstverilerden bazılarının kullanıldığı, bazılarının ise kullanılmadığı görülmektedir. Mesela düzenleyen, referans numarası, sayı, e-imza ve zaman damgası bilgileri ile açıklama notları gibi alanlar birer üstveri olarak kurgulanmıştır. Fakat belgeye erişmek için asgari gereksinimler, kullanılan algoritmalar, saklama süresi, teknolojik göç işlemleri, belge, ekleri ve ilgilerin referans numaraları ile özet değerleri ve şifreleme bilgilerinin belge profilinde bir üstveri olarak tutulmadığı gözlenmektedir. Burada aranan üstverilerin sistemde bulunmasına rağmen, veri tabanında farklı yerlerde mevcut olduğu anlaşılmıştır. Arşivlenen belgeler profilleriyle birlikte görüntülenmesi gerektiğinden, güvenilirliğin başarıyla korunmasında önemli olan bu alanların belge profilinde yer alması gerekir. Yoklukları güvenilirlik açısından ciddi bir tehdit oluşturabilir.

---

64 EYP'de dosya formatları mime type alanında belirtilmektedir (CBDDO, **e-Yazışma Teknik Rehberi**, **a.g.e.**, s. 21).

Aynı zamanda, kullanılan üstveri alanlarının sorgulandığı 2, 3 ve 4. sorular ile arşivlenen belgeler için kullanılması düşünülen üstverilerle ilgili 12. soru birlikte değerlendirilebilir. Bu sorulara tüm kurumların aynı cevaplar verdiği görülmektedir. Kurumların hiçbirinde arşivlenen ya da arşivlenecek belgelere ilişkin yeterli üstveri hazırlığının bulunmadığı gözlenmektedir.

Kurumlar, 2. sorudan azami 2.712 puan kazanabilirken, 2.373 puan kazanmış, 3. sorudan ise en fazla 7.735 puan kazanabilirken, 1.7628 puan elde etmiştir. Bunun nedeninin, kritik zorunlu olarak belirlenen belgenin ait olduğu işlem-dosya-seri ve birimin seçilmemesi, kullanılan algoritmalar ve teknolojik göç işlemlerine ilişkin üstverilerin belge profilinde yer almamasından kaynaklandığı değerlendirilmektedir.

Kurumların her biri, 4. sorudan en çok 1.294 puan elde edebiliyorken, 0.678 puan kazanmıştır. Bu durumun, kurumlarda belge bileşenlerini üreten algoritmalar ve bileşenlere erişmek için asgari gereksinimlere ilişkin bir üstverinin mevcut olmamasından kaynaklandığı düşünülmektedir. Bununla birlikte, arşive devredilecek belgelerle ilgili üstverilerin sorulduğu 12. sorudan azami 1.568 puan kazanmak mümkünken, kurumlar bu sorudan hiç puan elde edememiştir. Çünkü kurumların henüz arşive e-belge devretmediği gözlenmiştir.

Her bir kurumun üstverilerle ilgili elde ettiği puan 4.8138 olmuştur. Bu sorulardan kazanılabilecek toplam puan ise 13.309'dur. Belge düzeyindeki üstverilerle ilgili sorulardan elde edilebilecek puanların %36'sına erişen kurumların bu konuda çok zayıf bir başarıya sahip olduğunu ifade etmek mümkündür.

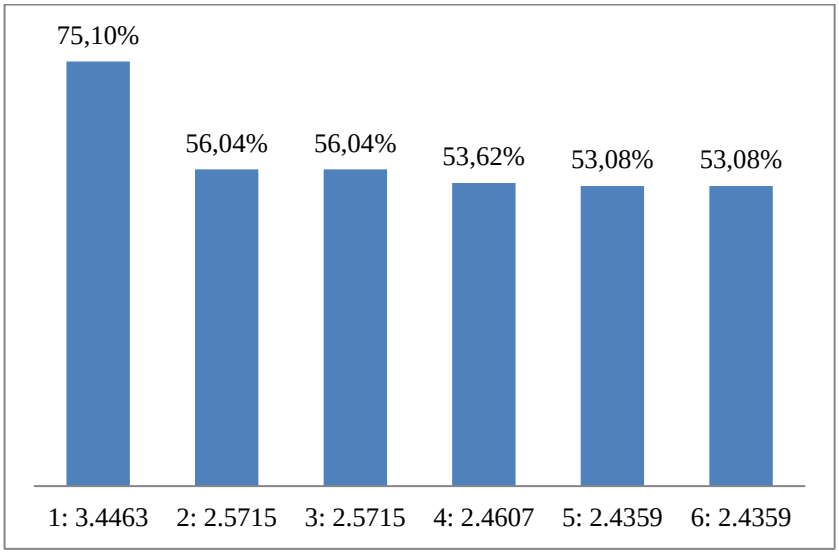
Üstverilerle ilişkili olduğu değerlendirilen bir diğer husus ise tanımlamadır. Çünkü tanımlama, üstverilere dayanarak yapılır. Saha araştırmasında kurumların arşivlenen belgelerin tanımlanması için bir standart kullanıp kullanmadığı sorulmuştur. Tüm kurumlar hayır cevabını vermiştir. Sahada bu konuda yeterli farkındalığa sahip olunmadığı gözlenmektedir.

Analiz edilen bir diğer kriter, dosyalama uygulamalarıdır. Tüm kurumların bu soruya aynı cevabı verdiği görülmektedir. Ancak, dosyalamada belgeyi üretirken belgenin hangi işlem, dosya, seri ve birime ait olduğunu seçmek temel bir gereklilik olarak kabul edilse de kurumlarda bu adımın uygulanmadığı gözlenmektedir. Bu hususun kurumlarda yeteri kadar anlaşılamadığı ifade edilebilir.

Bununla birlikte bu soruda benimsenen bir diğer zorunlu kriter, dosya türü ayrımının yapılmasıdır. Böylece, konu ve vaka dosyasına yapılacak muamelelerin birbirinden ayrılması hedeflenir. Kurumlarda dosya türü ayrımının yapıldığı görülmüştür. Aynı zamanda, konu dosyalarının sene sonunda otomatik olarak kapandığı, vaka dosyasına giren bir belgenin çoğaltılmadan konu dosyasıyla da ilişkilendirildiği, belgeler ve dosyalar için dosya kodunun yanı sıra özel kodların da kullanıldığı gözlenmiştir. Ayrıca, birim belge yöneticisinin belgeyi dosyasına gönderebildiği, dosyaların üstverilerinde ait olduğu seri ve birimin belirtildiği, dosyaların ait olduğu bir seriden başka bir seriye taşınabildiği ve aynı dosyanın parçası olup, kâğıt ortamda saklanan belgelerin yerinin belirtildiği anlaşılmıştır. Belgede ve dosyada değişen dosya kodu eski ve yeni hâliyle birlikte gösterilmektedir.

Dosyalama uygulamalarıyla ilgili bu pratiklerin yanı sıra kurumların dosya planlarına ilişkin hususlar da analiz edilmiştir. Dosyalamanın başlangıç adımlarından biri olarak kabul edilen ve kritik zorunlu olarak benimsenen fonksiyon analizi yapılarak belge hiyerarşisi oluşturulması pratiğinin sadece 1 nolu kurumda gerçekleştirildiği görülmektedir. Dört kurumda, dosya ve seri kodları için bir referans numarası oluşturulmuşken, 5 ve 6 nolu kurumlarda bu işlem gerçekleştirilmemiştir. Bununla birlikte, 4 nolu hariç tüm kurumlarda saklama süresi sonunda yapılacak tasfiye işlemlerinin kararlaştırıldığı görülmektedir. Tüm kurumlarda, Standart Dosya Planı'nın (SDP) kurum ihtiyaçlarına göre şekillenerek kullanıldığı anlaşılmaktadır.

Dosyalama pratiklerinin sorgulandığı 6. soruda kurumlar asgari 3.357 puan alabiliyorken, 2.2143 puan elde edebilmiştir. Dosya planlarıyla ilgili olan 8. sorudan ise en fazla 1.232 puan elde etmek mümkündür. Bu soruda 1 nolu kurum 1.232, 2 ve 3 nolu olanlar 0.3572, 4 nolu 0.2464, 5 ve 6 nolular ise 0.2216 puan kazanabilmiştir. Kurumlar bu sorulardan toplam 4.589 puan elde edebilmektedir. 1 nolu kurumun başarılı olduğu ifade edilebilir. Diğerlerinin ise orta düzey bir başarıya sahip olduğu anlaşılmaktadır.

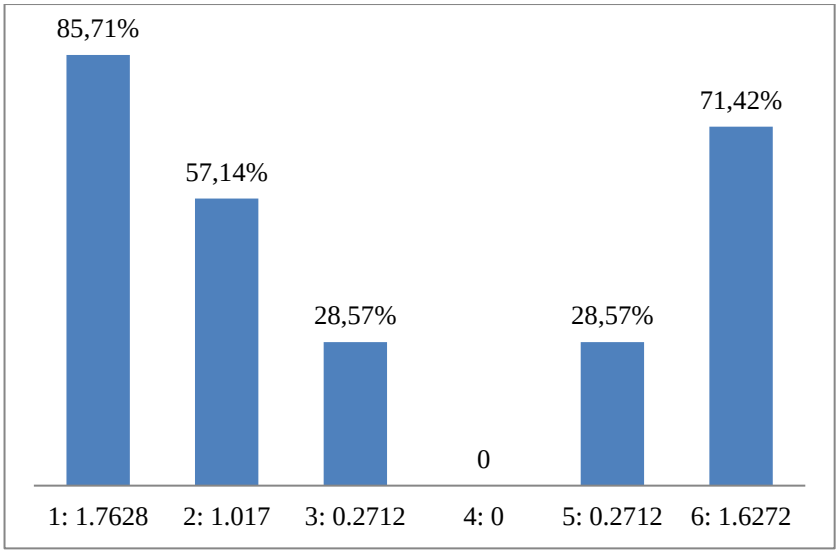


Şekil 32. Dosyalama

Dosyalamayla ilgili hususların yanı sıra, saha araştırmasında belgelerin tasfiyesine ilişkin uygulamalar da incelenmiştir. 4 nolu haricinde tüm kurumların belgelere oluşturulmadan önce bir saklama süresi tayin ettiği anlaşılmaktadır. Sadece 6 nolu kurumun belgeleri arşive devrederken dosyalarıyla birlikte devredileceğini belirttiği gözlenmektedir. Çünkü bu kurum, arşiv yönetimi yazılımına da sahip olup çeşitli denemeler gerçekleştirmektedir. Bu pratik, belge ile dosya arasındaki ilişkinin korunması için başlangıç adımlarından biri olarak kabul edildiğinden kritik zorunlu olarak benimsenmiştir.

İnceleme sırasında 1, 3, 5 ve 6 nolu kurumların, saklama süresinin aşımının gerekçesini belirttiği görülmektedir. 1, 2 ve 6 nolu olanların belgeleri, belge profili ve üstverileriyle birlikte arşive devretmek konusunda denemeler yaptığı; belgeleri tasfiye ederken de yine belge profili ve üstverilerini de tasfiye ettiği gözlenmektedir. Belge ile üstveriler arasındaki ilişkinin kopmaması tasfiye sürecinin başlangıç adımlarından biri olarak kabul edildiğinden bu soru, kritik zorunlu olarak benimsenmiştir. Ayrıca, aynı şekilde kritik zorunlu olarak benimsenen belge tasfiye edildiğinde referans numarasını belge yönetimi sisteminde tutup, akıbeti hakkında bir bilgi notu bulundurulmasının sadece 1 nolu kurumda uygulandığı görülmektedir. 1 ve 2 nolu kurumların belgeleri dosyalarıyla birlikte arşive transfer ettikten sonra belge yönetim sisteminden kaldırmayı benimseyeceği anlaşılmaktadır.

Araştırmaya katılan kurumların, kendi ihtiyaçları neticesinde tasarılar geliştirerek denemeler yapsa da e-belgeleri arşive devretmek konusunda yeteri kadar tecrübeye sahip olmadığı anlaşılmaktadır. Bunun, Devlet Arşivleri Başkanlığının konu hakkında yeteri kadar tasarrufta bulunmamasından kaynaklandığı düşünülmektedir. Kurumlar bu sorudan en fazla 2.373 puan elde edebilirken aşağıdaki tabloda belirtilen puanları kazanmıştır.



Şekil 33. Tasfiye

Tasfiye uygulamaları konusunda 1 nolu kurumun çok başarılı, 6 nolunun ise başarılı olduğu ifade edilebilir. 2 nolu kurumun orta düzey, 3 ve 5 nolu olanların ise zayıf bir başarıya sahip olduğu görülmektedir. 4 noluda tasfiye işleminin sorulan sorular ışığında yürütülmediği gözlenmektedir.

Belge düzeyiyle ilgili olarak sorulan bir diğer soru özgünlüğün tasdik edilmesine ilişkindir. Kurumlarda oluşan belgeler, ait olduğu işlemin türüne göre belirli bir form özelliğine sahip olur. Dolayısıyla form özellikleri, her işlemde aynı şekilde ortaya çıkmaz. Bu özelliklere bakılarak belgenin ait olması gereken işlemle ilişkisi tespit edilebilir. Belgelerin zaman içerisinde özgünlüğünün tasdik edilmesi için doğduğu fonksiyonun işlemlerini göstermesi gerekir.

Ancak, belgelerin form özelliklerinden biri olan kimlik tespiti araç/ları belge türüne göre değişiklik gösterebilmektedir. Örneğin, üniversitedeki bir idari personelin hareket onayı belgesinde personel daire başkanı, genel sekreter ve rektörden oluşmak

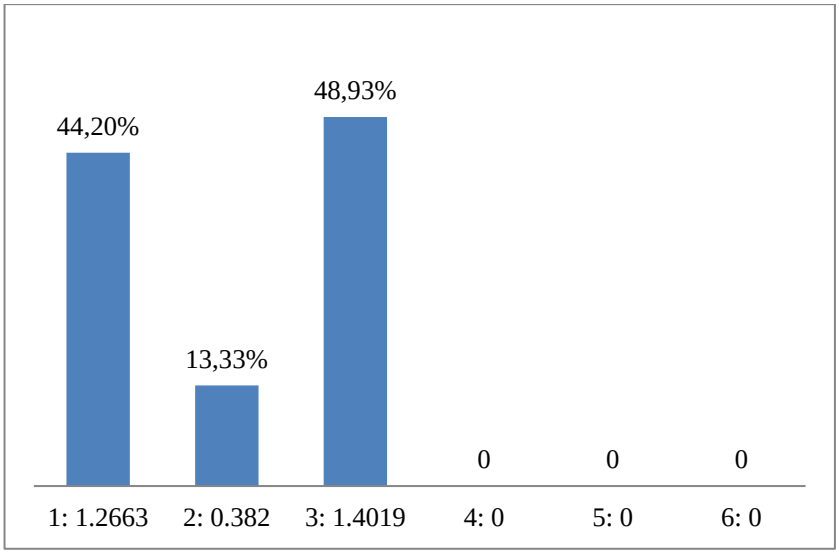
üzere üç imzanın bulunması gerekir. Piyasa araştırma tutanaklarında da piyasa araştırma komisyonu üyelerinin imzasına ihtiyaç duyulur. Belgeleri kim/lerin düzenleyip, imzalayarak onaylayacağı işlemin hukuki gerekçesi olan fonksiyonun ait olduğu mevzuatta belirtildiği gibi buradaki kuraldan hareket edilerek de kurumların imza yetkileri yönergesinde düzenlenmektedir. Hâliyle belgede var olan kişiler ve onların kimlik açıklama şekilleri bu prosedürlere bakılarak anlaşılır. Sadece 2 ve 3 nolu kurumda bu yönde bir uygulamanın olduğu görülmüştür.

Tüm bu hususlarla birlikte, e-belgeler arşive devredilirken özniteliklerinin korunarak devralındığını gösteren bir mekanizmaya ihtiyaç duyulmaktadır. Bu mekanizmalardan biri de e-mühürdür. Kurumların hiçbirinde bu mührün kullanılmadığı gözlenmektedir. Bununla birlikte, sorgulanan bir diğer mekanizma belgelerin tanımlama bilgilerinin incelenmesidir. Sadece 2 nolu kurumda bu yönde bir yaklaşımın benimsendiği görülmüştür. Özgünlüğün korunmasında kullanılabilecek mekanizmalardan biri de dosya sistemi ve veri tabanında belgelerin birbiriyle ilişkilendirilmesi ve bunun muhafazasıdır. Sadece 1 nolu kurumda bu yönde bir pratiğin mevcut olduğu anlaşılmıştır.

E-imzalı belgelerin özgünlüğünü etkileyen imza sertifikalarının belirli bir geçerlilik süresinin olduğu bilinmektedir. Bu süreden sonra belge üzerinde herhangi bir değişiklik yapılıp yapılmadığını kontrol edebilmek için bazı mekanizmalara ihtiyaç duyulmaktadır. Bunlardan biri, belge üzerindeki imzaların geçerliliği bitmeden belgeye ait olan EYP'nin zaman damgası ile damgalanmasıdır. Bununla birlikte, 2020 yılında güncellenen RYY'ye göre belge üzerindeki imzaların arşiv imzası tipine dönüştürülmesi gerekir. Bundan dolayı bu pratik, kritik zorunlu olarak benimsenmiştir. Böylece, uzun dönemli saklanacak belge üzerindeki imzaların geçerliliği bittikten sonra da eklenen zaman damgasıyla delil değerinin güçlendirilmesi hedeflenmektedir. 1 ve 3 nolu kurumlarda bu yönde bir uygulamanın mevcut olduğu görülmektedir.

Özgünlüğün tasdik edilmesinde kritik zorunlu olarak benimsenen bir diğer husus, belgelerin zaman içerisinde değiştirilmemesi için bütünlük analizinin yapılmasıdır. Bunun kurumlarda düzenli aralıklarla incelenmesi beklenir. Bununla birlikte, bütünlük bozulması riskine karşı bir risk değerlendirmesi ve riskten kaçınma raporunun hazırlanması kurumların bu konuda farkındalık sahibi olduğunu gösteren

araçlardan biri olarak kabul edilmektedir. Fakat, kurumlarda bu yönde bir pratiğin mevcut olmadığı gözlenmektedir.



Şekil 34. Özgünlüğün Tasdik Edilmesi

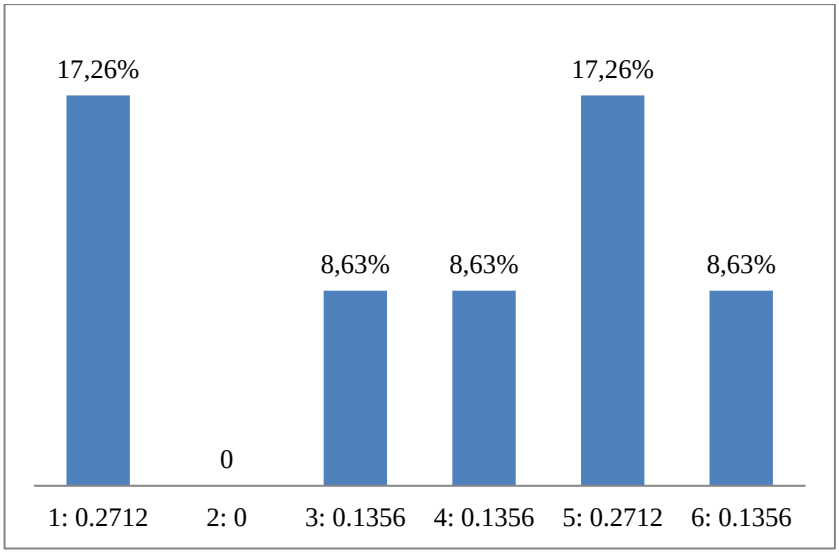
Kurumlar bu soruda en fazla 2.865 puan elde edebilmektedir. Elde edilen cevaplar neticesinde, 1 ve 3 nolu kurumların orta düzey bir başarıya sahip olduğu gözlenmektedir. 2 nolunun başarı düzeyi ise çok zayıf olarak değerlendirilmektedir. Sorulan sorular ışığında, 4, 5 ve 6 nolu kurumların özgünlüğün tasdik edilmesine ilişkin işlemlerinin mevcut olmadığı görülmektedir.

Belge düzeyindeki güvenilirlik analiziyle ilgili son soruda kurumda oluşan belgelerin form özellikleri, yapısı ve içeriğinin değiştirilmemesine yönelik yaklaşımların var olup olmadığı incelenmektedir. Bu kapsamda belge üretildikten sonra özet değeri kontrolü yapılıp yapılmadığı bütünlük analizinde gerçekleştirilen eylemlerden biridir. 1, 3 ve 5 nolu kurumların bu yönde bir pratikleri olduğu görülmektedir.

Belge formatlarının tanımlanarak onlara otomatik bir özet değeri atayan, oluşan bir belgenin ilerleyen zamanlarda da form özellikleri ve bütünlüğünün korunup korunmadığını inceleyen JHOVE ve DROID gibi programlar çeşitli ülkelerde sıklıkla kullanılmaktadır. Bu nedenle bu pratik, kritik zorunlu olarak benimsenmiştir. Fakat incelenen kurumların bu yönde bir uygulamasının mevcut olmadığı gözlenmiştir.

Bu hususların yanı sıra özgünlüğü korumak için log kayıtları da başvurulan yöntemlerden biridir. 1, 4, 5 ve 6 nolu kurumların log kayıtlarını bu amaçla incelediği

gözlenmektedir. Buna rağmen, elektronik delil elde etme yöntemlerinin kullanılmadığı ve döngüsel artıklık denetimi yapılmadığı görülmüştür.



Şekil 35. Özgünlüğü Koruma

Kurumlar, bu soruda en fazla 1.571 puan elde edebilmektedir. 2 nolu kurumun sorulara verdiği cevaplardan anlaşıldığı kadarıyla belgelerin özgünlüğünün korunmasına ilişkin bir işleminin mevcut olmadığı görülmektedir. Diğer 5 kurumun her ne kadar birtakım cevaplar vererek özgünlüğü koruma adına küçük de olsa adım attıkları anlaşılsa da verilen olumlu cevapların oranları %60'ın altında kaldığından başarı düzeylerinin çok zayıf olduğu söylenebilir.

4.2.2.2. Teknolojik Koşullar Düzeyi

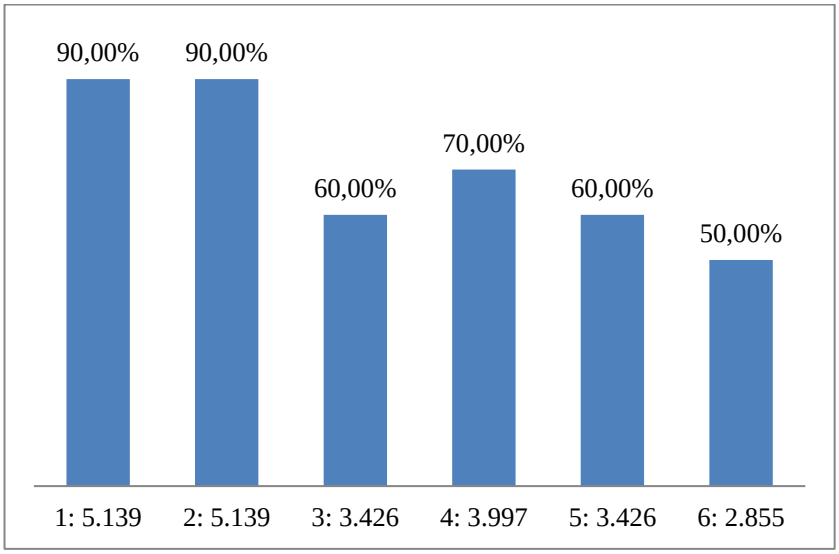
Teknolojik koşullar düzeyinde, e-imzalı belgelerin güvenilirliğini etkileyen log kayıtları, teknolojik göç, yedekleme, kullanılan yeni teknolojiler, EBYS yazılımı ile donanım koşulları, sistemsel üstveriler ve denetim günlükleri gibi hususlar kritik edilmektedir. Belge düzeyinde olduğu gibi burada da zorunlu ve seçmeli kriterler bulunmaktadır. Zorunlu kriterleri ölçen soruların katsayısı 0.571 (20/35), seçmelileri ölçenlerin ise 0.357 (5/14) olarak hesaplanmıştır. Kurumlar, bu düzeydeki tüm sorulara olumlu cevap verirse puanları 25'e tamamlanmaktadır. Zorunlu kritik soruların olduğu durumlarda ise zorunlu soruların katsayısı 0.2284, seçmelilerin ise 0.1428 olarak belirlenmiştir. Başarı düzeylerindeki yüzdelik puanların ondalık kısmı,

iki basamaklı olacak şekilde değerlendirilmiştir. Tüm kurumlarda KEP, UETS ve EYP'nin kullanıldığı görülmüştür. Teknolojik koşullar düzeyinde verilen cevaplar, EK 10'da belirtilmektedir. Bununla birlikte, kurumların elde ettiği başarı düzeyleri tablolarda gösterilmektedir.

Teknolojik koşulların güvenilirliğe katkısını incelemek için 8 ana başlıkta toplam 49 soru sorulmuştur. Bu ana başlıklardan ilki log kayıtlarıyla ilgilidir. Bu kayıtlarla ilgili olarak dokümanın belgeye dönüşme tarihi ve zamanı, belgeye erişim istekleri, iletim geçmişi, sistem arıza/bakımları ve paraf bilgileri ile paraflayanın yaptığı işlemler gibi bilgiler sorulmuştur. Burada amaç, log kayıtlarında belge üzerinde yapılan işlemlerin bulunup bulunmadığını değerlendirebilmektir. Alınan cevaplara göre log kayıtlarıyla ilişkili olduğu belirtilen bu bilgilerin tüm kurumların uygulama yazılımlarında yer aldığı görülmüştür. Bunun bir nedeninin, saha çalışmasına dâhil edilen kurumların kamuda yaygın olan belli başlı yazılım ürünlerini kullanmaları, tedarikçilerin de log kayıtlarına ilişkin bu hususları bir paket hâlinde sunmalarından kaynaklandığı düşünülmektedir.

Ancak, katılımcıların verdikleri cevaplardan anlaşıldığı kadarıyla belgede format değişikliği gibi yaşanabilecek teknolojik değişimlere ilişkin verilerin log kayıtları ile ilgili olarak uzun dönemde riskler doğurabileceği gözden uzak tutulmamalıdır. Format değişikliğinin log kayıtlarında bulunmasının yanı sıra sorulan bir diğer husus, üstveriler ve saklama sürelerinde yapılan değişikliklerin bu kayıtlarda yer alıp almadığıdır. Bunlar, sadece 1 ve 2 nolu kurumların log kayıtlarında bulunmaktadır. Benzer bir şekilde, belgeyle ilgili açıklama notları kısmının 1, 2 ve 4 nolu kurumların log kayıtlarında mevcut olduğu gözlenmektedir. Bu hususlarla birlikte, belgede yapılan işlemler ve bu işlemleri yapan kullanıcılara dair veriler, 6 nolu hariç tüm kurumların log kayıtlarında yer almaktadır.

Kurumlar, bu soruda en fazla 5.71 puan elde edebilmektedir. 1 ve 2 nolu kurumun bu konuda çok başarılı, 3, 4 ve 5 noluların başarılı olduğu görülmektedir. 6 nolu kurum ise orta düzey bir başarıya sahiptir.



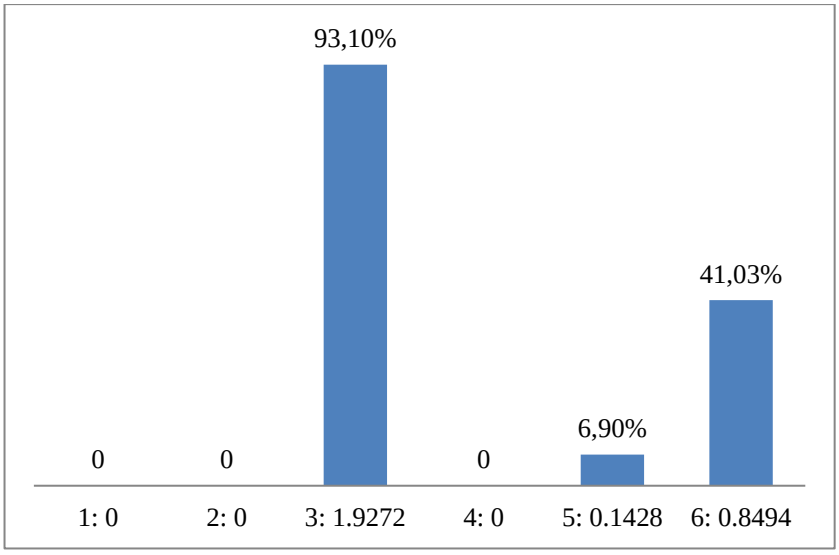
Şekil 36. Log Kayıtları

Log kayıtlarının yanı sıra kurumlarda analiz edilen bir diğer husus teknolojik göç meselesidir. Burada belgelerin taşıyıcı ortamının değiştirilmesine yönelik düzenli incelemeler yapılması, teknolojik göç sonrası belgelerin erişilebilirliği ve okunabilirliğinin kontrol edilmesi, bu göç işleminin belge profiline eklenmesi ile risk analizinin yapılmasına yönelik sorular sorulmuştur. Sadece 5 nolu kurumda belgenin taşıyıcı ortamının değiştirilip değiştirilmemesi hususunda düzenli aralıklarla incelemelerin yapıldığı görülmüştür. Bununla birlikte sadece 3 nolunun, teknolojik göç sonrası belgelerin erişilebilirliği ve okunabilirliğini kontrol ettiği ve bu konuda risk analizi yaptığı anlaşılmıştır. Bu yaklaşımın, kurumun bu konuda geçmişte yaşadığı tecrübelerden kaynaklandığı ifade edilmiştir. Teknolojik göçün başarılı olup olmadığını göstermesi nedeniyle bu kriter, kritik zorunlu olarak değerlendirilmiştir.

Benimsenen bir diğer kritik zorunlu uygulama ise belge profiline yeni ortam ve göçün gerçekleştiği tarihin eklenmesidir. Bu bilgiler, belgenin teknolojik göç işlemlerine uğradığını gösterdiğinden diğerlerine göre ön plana çıkmaktadır. Tarih ve yeni ortam bilgileri, göçün gerçekleşme zamanını belirttiğinden bu işlemin uygulandığı belgelerin güvenilirliğinin diğer belgelerden farklı yöntemlerle incelenmesi gerekir. Bu bilgilerin varlığı, belgelerin delil değerini kuvvetlendiren bir unsurdur. Söz konusu uygulamanın sadece 3 ve 6 nolu kurumlarda mevcut olduğu

görülmektedir[65]. Bu bilgi, "belge … tarihinde daha önce kullanılan EBYS'den aktarıldı" şeklinde 3 nolu kurumdaki belge profilinde belirtilmektedir.

Kurumlar, bu soruda en fazla 2.07 puan elde edebilmektedir. 1, 2 ve 4 nolu kurumlardan alınan cevaplardan anlaşıldığı kadarıyla bunların bu hususla ilgili bir pratiklerinin olmadığı görülmüştür. Bununla birlikte küçük de olsa belgelerin teknolojik göçüyle alakalı birtakım işlem yapanlardan 5 nolu kurumun başarı oranı %6,9 çıkmıştır. Bu oran, gerekli başarının yakalanamadığı 1-19 yüzdelik dilimine tekabül ettiğinden 5 nolu kurumun beklenen performansın altında kaldığı düşünülmektedir. 6 nolu kurumun performansı %41,03 şeklinde çıktığı için orta düzey bir başarıya sahip olduğu ifade edilebilir. Kritik zorunlu kriterleri gerçekleştiren tek yer olan 3 nolu kurum, %93,1'lik bir orana ulaştığından bu konuda oldukça başarılı bulunmuştur.



Şekil 37. Teknolojik Göç

Kurumlarda analiz edilmeye çalışılan bir diğer husus ise yedekleme uygulamalarıdır. Burada yedeklemelere sadece yetkili personelin erişmesi, belgelerin profilleri ve üstverileriyle birlikte düzenli aralıklara yedeklenmesi, yedeklemenin başarılı gerçekleşip gerçekleşmediğinin kayıt altına alınması gibi hususlar incelenmiştir. Saha araştırmasında elde edilen cevaplar neticesinde tüm kurumlarda yedeklemelere

65 Bu duruma rağmen, 3 ve 6 nolu kurumlar söz konusu bilginin bir üstveri olarak yer alıp yer almadığını sorgulayan 3. soruda hayır cevabını vermiştir.

sadece yetkili personelin erişebildiği gözlenmektedir. Bununla birlikte, 6 nolu hariç tüm kurumlarda son yedeklemelerin ardından bir sonraki yedeklemeye kadar geçen süre içerisinde, zaman damgası ve arşiv imza güncellemeleriyle alakalı açıklamalar ve işlemlerin denetim günlüklerine kaydedildiği anlaşılmaktadır. Sadece 1 ve 4 nolu kurumlar denetim günlüklerine yedeklemenin başarılı bir şekilde gerçekleşip gerçekleşmediğini eklemektedir. Gerçekleşmemişse yedekleme işlemleri tekrar başlatılmaktadır.

Kurumlarda belgeler, belge profilleri ve üstverilerin düzenli aralıklarla yedeklendiği görülmüştür. Aynı zamanda sistem yedeklemesi de düzenli olarak yapılmaktadır. Bu işlemler, mevcut sistemde bir sorun yaşandığında eski sistem devreye alındığından oldukça önemlidir. Çünkü sistemi devam ettirmek belge profili ve üstverilerin yedeklenmesiyle mümkündür. Durum böyle olunca, bu pratikler kritik zorunlu olarak benimsenmiştir.

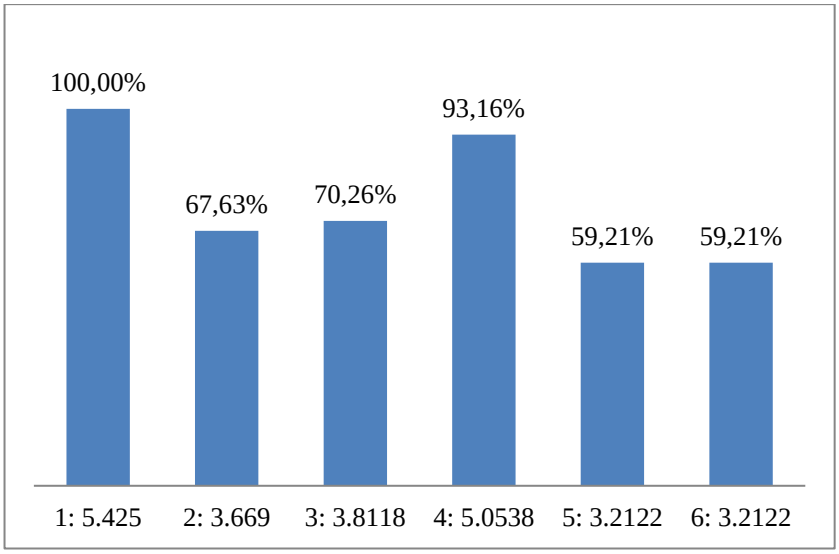
Bu hususların yanı sıra, 1, 3 ve 5 nolu kurumlarda son üç yedeklemenin muhafaza edildiği gözlenmektedir. 4 nolu haricindeki tüm kurumların herhangi bir sorun karşısında bir önceki yedeklemeyi devreye alabildiği anlaşılmıştır. 4 nolu kurum, bu yönde iyileştirmeler yapma sürecinde olduğunu ifade etmiştir.

Bu sorularla birlikte, kurumlarda yedeklemelerle ilgili tarihi ve zamanı, onaylayanı, saklama konumu ve referans numarası gibi üstverilerin bulunup bulunmadığı da incelenmiştir. 5 nolu kurumda bu üstverilerin kullanılmadığı görülmüştür. Aynı zamanda yedeklemenin tarihi ve zamanı ile konumu üstverilerinin, 5 nolu haricindeki tüm kurumlarda bulunduğu anlaşılmaktadır.

Üstverilerle ilgili hususlardan yedeklerin kim tarafından onaylandığının belirtilmesi güvenilirliğin korunmasında oldukça önemlidir. Çünkü mevcut sistemde herhangi bir sorun olduğunda yedekler devreye alınmaktadır. Yapılan yedeklemelerin kim tarafından onaylandığı bilgisi, herhangi bir sorun yaşandığında sorumluyu işaret edeceğinden kritik zorunlu olarak benimsenmiştir. Sadece 1 ve 4 nolu kurumlarda yedeklemeyi onaylayan üstverisinin bulunduğu gözlenmiştir. 5 ve 6 nolu haricindeki diğer kurumlarda, yedeklemelere bir referans numarası verilmektedir.

Kurumlar, yedekleme pratikleriyle ilgili sorulardan en fazla 5.425 puan elde edebilmektedir. 1 nolu kurumun bu konudaki tüm pratikleri gerçekleştirerek oldukça başarılı olduğu görülmektedir. Bu kurumla birlikte %93,16'lık performansıyla 4 nolunun da çok başarılı olduğu dikkat çekmektedir. Grafikteki orana bakıldığında 2 ve

3 nolu olanların da başarıyı yakaladıkları söylenebilir. 5 ve 6 nolu olanlar ise orta derecede başarılı bulunmuşlardır.



Şekil 38. Yedekleme

Kurumlarda blokzincir, yapay zekâ, derin öğrenme ve e-delil elde etme yöntemleri gibi yaklaşımların kullanılma durumu da incelenmiştir. Bunların kullanılması yönünde bir düşünce olup olmadığı sorulmuş ve tüm kurumlar, hepsine hayır cevabını vermiştir. Hâliyle bu konuda bir başarı düzeyi belirlenememiştir.

Kurumlara sorulan bir diğer soru ise kullandıkları donanım ve yazılımlarla ilgilidir. Kullanılan yazılımın algoritma ve kaynak kodlarının kurumda saklanması, veri tabanının arşivlenebilir yapıda olması ve bir kez yazılabilir ortamların kullanılması gibi sorular sorulmuştur. Bir yazılımın nasıl çalıştığı, onun belgeleri nasıl üretip sakladığı algoritmalar ve kaynak kodları aracılığıyla öğrenilebilmektedir. Hâliyle bu hususlar, güvenilirliğin korunmasında önemli bir uygulama olarak değerlendirildiğinden kritik zorunlu bir kriter olarak benimsenmiştir. Ancak, kurumların hiçbirinde bunun benimsenmediği görülmüştür.

Bunun yanı sıra, belgelerin saklanma ortamları da güvenilirliğin korunmasında dikkat edilen hususlardan biridir. Belgelerin bir kez yazılabilir, çok kez okunabilir ortamlarda saklanması tercih edilse de sadece 3 nolu kurumda bu pratiğin geçerli olduğu görülmüştür. Bununla birlikte, 2 nolu haricindeki tüm kurumlarda kullanılan donanımlar, üreticilerinin tavsiye ettiği kullanım ömründen sonra devre dışı

bırakılmaktadır. Aynı zamanda belgelerin üretildiği cihazlardaki (bilgisayar, mobil telefon vb.) donanım ve yazılım özelliklerinin kayıt altına alınıp alınmadığı sorulmuş; bu uygulamanın 1, 2 ve 4 nolu kurumlarda geçerli olduğu anlaşılmıştır.

Saha araştırmasında bu hususların yanı sıra veri tabanlarının arşivlenebilir bir yapıya sahip olup olmaması ile güncel belgelerle arşivlenenlerin saklama konumları arasında bir ayrım yapılıp yapılmadığı da sorulmuştur. 1, 2 ve 3 nolu kurumlarda veri tabanının arşivlenebilir bir yapıya sahip olduğu görülmüştür. Ancak, sadece 5 noluda güncellerle arşivlenenlerin saklama konumları arasında bir ayrım yapılacağı belirtilmiş; çeşitli denemeler yaptıkları ifade edilmiştir.

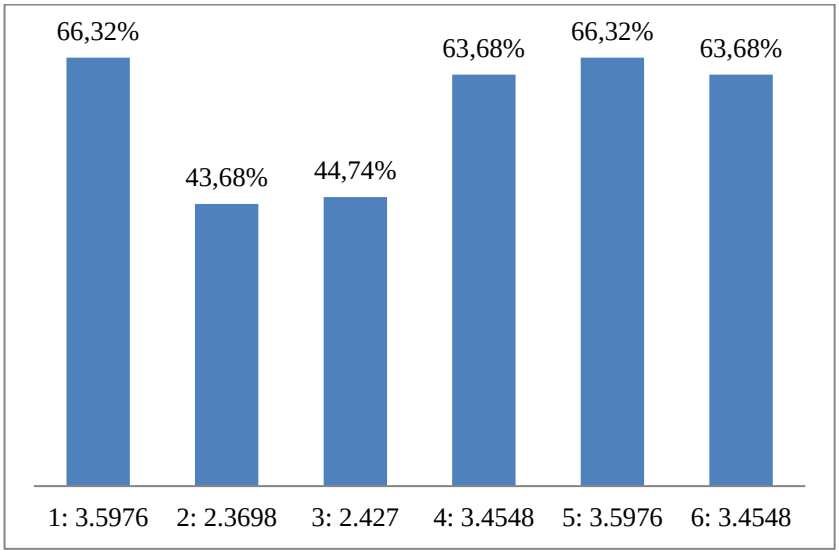
Belgelerin her türlü yazılım ortamında erişilebilirliği konusu, diğer bir soruyu oluşturmaktadır. Tüm kurumlarda yazılımlar değiştirilse de belgelere erişilebildiği ifade edilmiştir. Belgelerin delil değeri niteliklerinden olan okunabilirliği etkileyen bu işlem, kritik zorunlu olarak benimsenmiştir.

Güvenilirliğin korunmasında dikkat edilen bir diğer husus, ekler ve üstveriler gibi belge bileşenlerinin belgeyle birlikte bütüncül olarak korunmasıdır. 4 nolu haricindeki diğer kurumlarda bu uygulamanın benimsendiği görülmektedir. Bu kurumda belge ve bileşenler farklı konumlarda saklandığından aradaki ilişkinin yeteri kadar tesis edilemediği düşünülmektedir.

Saha araştırmasında log kayıtlarının zaman damgası ile damgalanıp damgalanmadığı da incelenmiştir. RYY'de yer alması nedeniyle bu pratik, kritik zorunlu olarak değerlendirilmektedir. 2 ve 3 nolu dışındaki tüm kurumların log kayıtlarında zaman damgası kullanıldığı görülmüştür.

Aynı zamanda, kurumların teknolojik koşullara ilişkin standartlaşma süreçlerinin incelenmesine de gayret edilmiştir. 1 nolu haricindeki tüm kurumlarda 27001 Bilgi Güvenliği Sertifikası alınması yönünde girişimler yapılmaktadır. Bununla birlikte kullanılan uygulama yazılımları, TS 13298 Standardı sertifikasına sahiptir.

Kurumlar, bu soruda en fazla 5.425 puan elde edebilmektedir. 2 ve 3 nolu kurumların bu konudaki başarısı orta düzeydeyken, diğerlerinin daha başarılı olduğu söylenebilir.



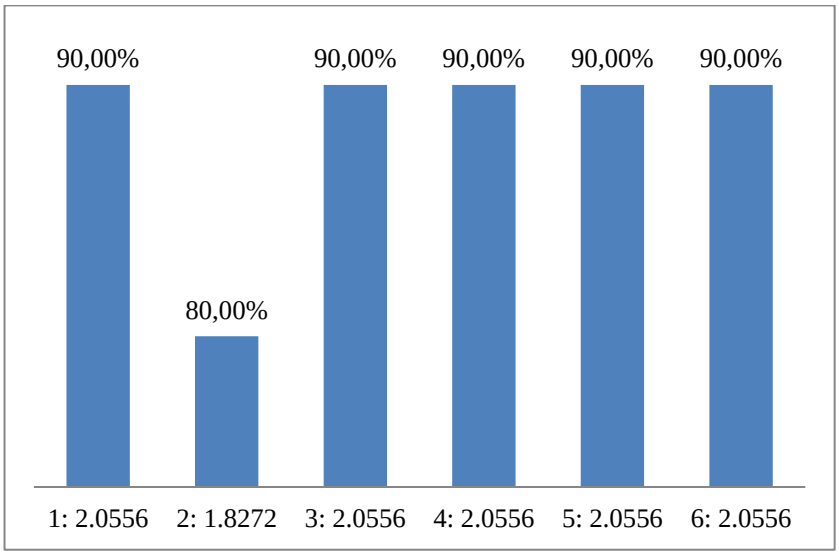
Şekil 39. Yazılım ve Donanımlar

Teknolojik koşullarla ilgili olarak kurumlara üstverilerin teknik altyapısına ilişkin kullanılan format, üstverilerle belgelerin birlikte hareket etmesi gibi sorular da sorulmuştur. Üstverilerde günümüz için XML ya da Javascript Object Notation (JSON - Javascript Nesne Gösterimi) formatının kullanılması önerilmektedir. Bu formattaki üstveri dosyasının belgeden ayrı olarak da saklanması gerekir. Böylece muhtemel bir risk durumunda üstverilerin de belge kadar etkilenmemesi ve güvenilirliğin zarar görmemesi hedeflenir. Tüm kurumlarda, üstverilerin XML ya da JSON formatında belgeden ayrı olarak saklandığı gözlenmiştir.

Üstveri dosyasının belgeden ayrı olarak saklanmasının yanı sıra onunla birlikte de hareket etmesi gerekir. Bu gereklilik, semantik ilişkinin kurulamaması ihtimaline karşı bir önlem alma amacı taşıdığından kritik zorunlu olarak kabul edilmiştir. Bununla birlikte, incelenen tüm kurumlarda belgenin konumu değiştirildiğinde üstverilerin de onunla birlikte hareket ettiği görülmüştür. Ancak kurumlarda üstveri dosyasının belgenin referans numarasından farklı bir numaraya sahip olduğu anlaşılmıştır. Oysa belge ile üstveri dosyasının aynı referans numarasına sahip olması durumunda, veri tabanında belge ile üstveri arasındaki ilişki daha sağlıklı ve kolay bir şekilde kurulabilirdi.

Kurumlarda, yöneticilerin üstverilerde değişiklikler yaptığı bilinmektedir. Bu değişikliklerin sonucunda yeni bir üstveri kaydı oluşurken öncekinin de muhafaza edilmesi gerekir. Böylece, önceki üstveriler güvenilirliğin korunmasında bir karine olarak kullanılabilir. 2 nolu dışındaki tüm kurumlarda bu pratiğin mevcut olduğu gözlenmiştir.

Kurumlar, bu soruda en fazla 2.284 puan elde edebilmektedir. Tüm kurumların oldukça başarılı olduğu görülmektedir. 2 nolunun diğerlerine göre daha az başarılı olmasının nedeni üstveri değişikliklerinde eski üstveri kayıtlarının muhafaza edilmemesidir.



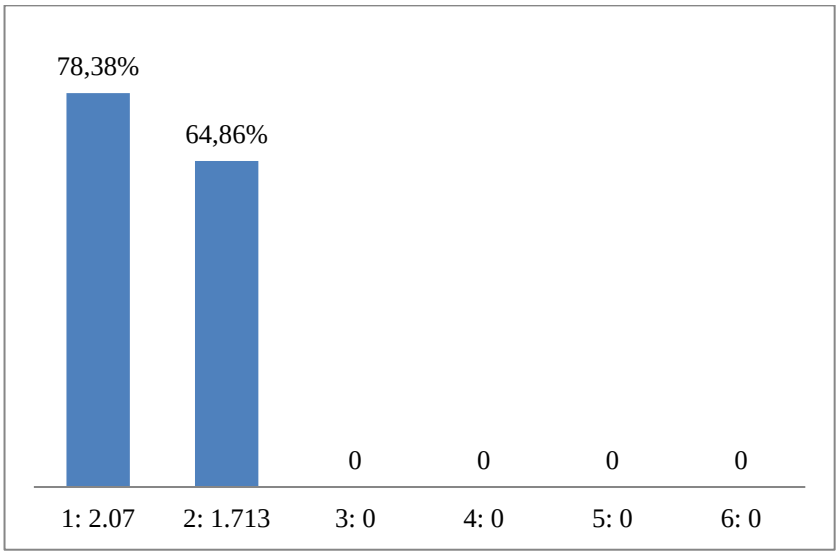
Şekil 40. Teknolojik Koşul Düzeyindeki Üstveriler

Teknolojik koşullardaki son soru denetim günlükleriyle ilgilidir. Bu günlüklerde hangi kullanıcının ne tür işlemi nasıl yaptığı açıklanır. Log kayıtlarının daha ayrıntılı bir şeklidir. Burada tüm belgeler için denetim günlüklerinin otomatik olarak oluşması, bu günlüklerin yapılan işlemlerin tarih ve saatini içermesi, erişimlerinde bir sorun yaşanıp yaşanmadığının düzenli aralıklarla kontrol edilmesi gibi hususlar incelenmiştir.

Sadece 1 nolu kurumda tüm belgeler için denetim günlükleri tutulmaktadır. Bunlar tutulmaya karar verildikten sonra otomatik olarak oluşturulmalıdır. Çünkü söz konusu süreçlerin insan eliyle değil, algoritmalarla yönetilmesi beklenir. Bununla birlikte, denetim günlüklerinde hangi işlemin yapıldığı yanı sıra bu işlemin tam olarak ne zaman gerçekleştiği de yer almalıdır. Aynı zamanda, denetim günlükleri bir kez oluşturulduktan sonra hiç değiştirilmemelidir. Böylece, teknolojik koşulların güvenilirliği ne derece koruduğu yönünde bir karine sunulabilir. Sadece 1 ve 2 nolu kurumlarda bunun uygulandığı anlaşılmaktadır.

Denetim günlüklerine erişimde bir sorun yaşanıp yaşanmaması için bu amaca yönelik geliştirilmiş otomatik araçlar kullanılır. Çünkü milyonlarca belgenin mevcut

olduğu kurumlarda bu işi insan eliyle yapmak pek mümkün görünmemektedir. Bu araçlar, düzenli aralıklarla erişimde sorun olup olmadığını kontrol eder. Kurumlarda bu tür işlemlerin yeterli olmadığı görülmüştür.



Şekil 41. Denetim Günlükleri

Kurumlar, bu soruda en fazla 2.641 puan elde edebilmektedir. 3, 4, 5 ve 6 nolu olanların bu konuda bir işleminin bulunmadığı görülmüştür. Kurumlar, denetim günlükleri oluşturmayı gerekli görmediklerini ifade etmiştir. Bu konuda uygulamaları bulunan 1 ve 2 nolu kurumların başarılı olduğu söylenebilir.

4.2.2.3. Kurum Düzeyi

Kurumlarda hazırlanan belge yönetimi politika ve prosedürleri ile kapasite geliştirme programı gibi araçlar, e-belgelerin güvenilirliğini etkileyen diğer hususlar arasındadır. Bunlar, e-belgelerin güvenilirlik analizinin kurum düzeyini oluşturmaktadır. Saha araştırmasında bu düzeyle ilgili pratikler incelenirken e-belge ve e-arşiv politikasının varlığı, fonksiyonlar ve iş süreçlerinin planlanması, dosya tasnif ve saklama planlarının hazırlanması, belgelerin üretilme, iletilme, dosyalanma ve arşivlenmesine ilişkin kurallarının belirlenmesi ile alan uzmanlarının istihdam edilmesi gibi uygulamaların varlığı araştırılmıştır. Kurumlar, bu işlemlerin yapılıp yapılmamasına göre değerlendirilmiştir.

Bu düzeyde 28 soru sorulmuştur. Bunların 19'u zorunlu, 9'u seçmelidir. Zorunlu kriterleri ölçen soruların katsayısı 1.052 (20/19), seçmelileri ölçenlerin ise 0.555 (5/9) olarak hesaplanmıştır. Kurumlar, bu düzeydeki tüm sorulara olumlu cevap verirse puanları 25'e tamamlanmaktadır. Zorunlu kritik soruların olduğu durumlarda zorunlu soruların katsayısı 0.4208, seçmelilerin ise 0.222 olarak ele alınmıştır. Başarı düzeylerindeki yüzdelik puanların ondalık kısmı, iki basamak olacak şekilde değerlendirilmiştir. Bu düzeyde kurumlara yöneltilen 28 soruya verilen cevaplar neticesinde oluşan tablo, EK 11'de gösterilmektedir. Cevaplara göre ortaya çıkan başarı düzeyleri tablolarda (Şekil 42, 43 ve 44) belirtilmektedir.

Kurum düzeyinde analiz edilen ilk husus, kurumların EBYS'yi uygulamaya almadan önce gerçekleştirdikleri işlemler olmuştur. Bu işlemlerden bazıları, başarılı bir belge yönetimi için temel gereklilikler arasında bulunduğundan kritik zorunlu kriterler olarak benimsenmiştir. Bu pratikler, doğru bir şekilde gerçekleştirilmediği takdirde diğer aşamaların da aksayacağı kabul edilmektedir. Mesela bunlardan biri kurumun e-belge ve e-arşiv yönetimi politikasının belirlenmesidir. Bu politikalar aracılığıyla sürecin idari dayanağı oluşturulacağından belgelerin güvenilirliğinin daha başarılı bir şekilde korunacağı düşünülmektedir. Sahada yapılan incelemelerde 2 ve 3 nolu kurumlarda e-belge yönetimi politikasının belirlenerek hareket edildiği görülmektedir. Ancak, 2015'de yayınlanan TS 13298 Standardı'nda[66] yer almasına rağmen kurumların hiçbirinde e-arşiv yönetimi politikasının belirlenmediği gözlenmiştir. Örgütlerde politika belirsizliği, belge yönetimi ve arşiv hizmetlerinin sağlıklı işlemesine engel teşkil edebilir[67]. Önceden belirlenecek politikalar ise belge yönetimi fonksiyonlarının kurallar ışığında yürütülmesinde kurumsal kararlılığı ortaya koyar.

Belge ve arşiv yönetiminde kurumsal bilgi varlıklarının organizasyonu gerçekleştirilirken, aynı zamanda belgelerin zarar görmesi engellenip bütünlük içerisinde muhafaza edilmesi sağlanır. Provenanstan koparılmayarak belgenin oluştuğu fonksiyon korunur. Başka bir deyişle, arşiv uygulamaları sadece belgelerin

66 TSE, **13298 Elektronik Belge Yönetim Sistemi Standardı**, **a.g.e.**, s. 42.

67 Arısoy, "Türkiye'de Elektronik Belge Yönetiminde Milli Arşiv Politikalarının Geliştirilmesi", **a.g.e.** ; Çiçek, "E-Devlet Stratejisi Bağlamında Elektronik Belge Yönetimi için "Yazılı Politika" Gereksinimi: Türkiye'deki Uygulamalar Üzerine Bir İnceleme", **a.g.e.**

değil faaliyetlerin de arşivlenmesi manasına gelir. Çünkü arşiv süreci, belgeleri doğduğu kaynağa göre olduğu gibi muhafaza etmeyi gerektirir.

Örgütlerde belge yönetimi sistemi kurulurken yapılması gereken öncelikli işlerden biri fonksiyonları analiz etmektir. Bu analiz yapılarak fonksiyon kapsamındaki iş süreçleri açığa çıkarılır. İş süreçleri yürütülen işlem adımlarını işaret ederken, aynı zamanda o adımda üretilen belgelerin tespit edilmesine yarar. Böylece iş süreci ile belgeler ilişkilendirilir. Analiz sırasında tespit edilen belgelerin doğduğu fonksiyona ait idari işlemlerle ilgili izler taşıdığı görülür. Antetin oluşturulmasından paraf ve imza adımlarının belirlenmesine kadar belgenin form özelliklerini oluşturan unsurlar fonksiyonu işaret eder. Hâliyle fonksiyonların iş süreçlerini tanımlayıp belgeyle ilişkilendirmek, kritik zorunlu bir kriter olarak benimsenmiştir.

Fonksiyona ilişkin bu açıklamaların ardından kurumlara iş süreçlerinin dokümantasyonunu oluşturup oluşturmadıkları sorulmuştur. İdari ve hukuki prosedürlere göre hangi belgenin kim tarafından düzenleneceği bu dokümantasyona yansıtılır. Hâliyle bu işlem, sürecin başarısına katkıda bulunan uygulamalardan biridir. Ancak, sadece 1 nolu kurumun bu yönde bir uygulamasının olduğu görülmüştür.

Tüm bu aşamaların ardından belge form ve şablonlarının oluşturulduğu bilinmektedir. Sistem kurulup belge yönetimi uygulamalarının gerçekleştirilmesiyle kurumsal fonksiyonlar kapsamında üretilecek belgeler ve sahip olmaları gereken form özellikleri bu şablonlara göre belirlenir. Önceden tanımlanmış türe özel bu form yapısı, üretilecek belgelerin karakteristik unsurlarındandır. Örneğin diplomaları diğer türlerdeki belgelerden ayıran hususların başında onun form özellikleri gelmektedir. Belgeler, önceden tanımlanmış bu şablonlara göre şekillendiğinden bu adım delil değerininin analizinde önemli ipuçları verecektir. Bundan dolayı form ve şablon oluşturma sorusu, kritik zorunlu olarak benimsenmiştir. Saha araştırmasında kurumların bu soruda daha başarılı olduğu gözlenmiştir. Tüm kurumların bu işlemi gerçekleştirdiği görülmüştür.

Belge türüne göre oluşturulan şablonlara bir kontrol numarası verilerek sürecin daha başarılı yürütüldüğü kabul edilmektedir. Bu numara, binlerce tür arasında belgeleri birbirinden ayırıp yönetmeye yaradığı gibi güncellemelerde kontrol sağlar. Böylece işlem görmüş bir belgenin hangi kontrol numarasında kayıtlı olanla karşılaştırılması gerektiği kolaylıkla belirlenebilir. Hâliyle bu pratiğin varlığı saha

araştırmasında da sorgulanmıştır. Sadece 2 ve 3 nolu kurumların bu yönde bir uygulamasının olduğu görülmüştür.

Bu adımların yanı sıra, belge türlerine göre üstveri şemaları oluşturmak güvenilirliğin korunmasına katkıda bulunan adımlardan biridir. Ancak, her belge türünde aranan bilgiler aynı olmadığından spesifik üstveri şemalarına ihtiyaç duyulabilmektedir. Bu işlemin 1, 3 ve 5 nolu kurumlarda uygulandığı görülmüştür. Bununla birlikte, belgedeki kişiler, antet ve format gibi belge profilindeki form özelliklerinin üstverilerle ilişkilendirilerek tanımlanması, belge yönetimi sürecinin sağlıklı bir şekilde yürütülmesine katkıda bulunur. 6 nolu haricindeki diğer kurumlarda bunun gerçekleştirildiği gözlenmiştir.

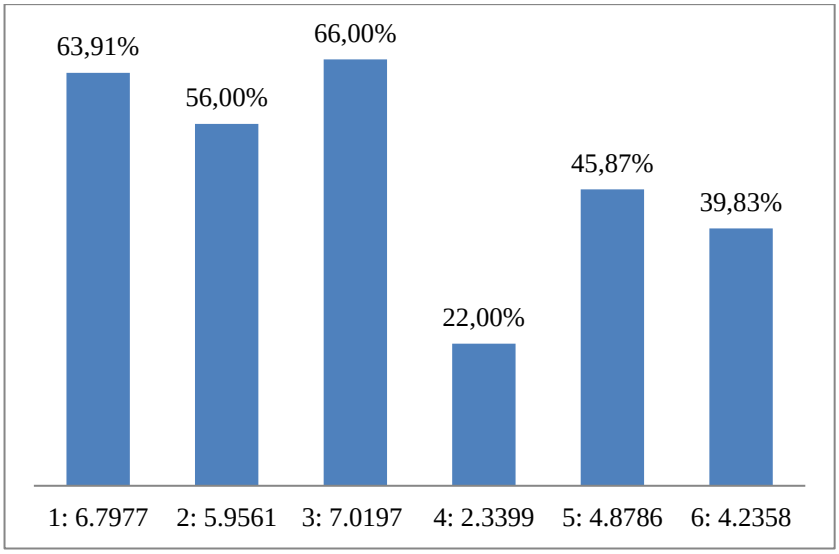
Bir fonksiyon bağlamında oluşan belgelerin bu ilişkisi tasnif planlarına bakılarak açığa çıkarılabilmektedir. Başka bir deyişle, tasnif planları aracılığıyla belgelerin hangi fonksiyon, faaliyet ve işlem çerçevesinde üretildiği anlaşılabilir. Bu nedenle kurumun gerçekçi fonksiyonları ışığında uygulanabilir bir tasnif planının hazırlanması kritik zorunlu bir kriter olarak benimsenmiştir. Tasnif planında işlerin yani dosyaların saklama süreleri de belirtilebilir. 4 nolu haricindeki diğer kurumlarda dosya tasnif ve saklama planlarının hazırlandığı görülmüştür.

Bununla birlikte, dosyalamanın dosya planına uygun yapılması belgelerin arşive devrinde önemlidir. 2 nolu haricindeki diğer kurumların bu dosyalama kuralına uygun hareket ettikleri gözlenmiştir. Bu süreci kolaylaştıran bir diğer uygulama ise kontrollü terminoloji kullanmaktır. Sadece 3 nolu kurumda bu yönde bir yaklaşımın mevcut olduğu görülmüştür.

Bu hususların yanı sıra, kurumların bir felaket (olağanüstü durum) karşısında nasıl davranacağı, hangi belgeleri nasıl yedekleyeceğine ilişkin bir planı olması beklenir. Böylece, muhtemel felaketler karşısında da güvenilirliğin başarıyla korunabileceğine dair bir karine sunulur. 4 nolu haricindeki diğer kurumlarda olağanüstü durum yönetimi ve yedekleme planının oluşturulduğu görülmüştür. 4 nolu kurum, hâlen böyle bir uygulamanın mevcut olmadığını ancak bu yönde hazırlıkların da yapıldığını ifade etmiştir.

Kurumlar, bu sorudan en fazla 10.636 puan elde etmektedir. Bu kritere göre 1 ve 3 noluların bu konuda başarılı olduğu görülmektedir. Verilere bakıldığında 2 ve 5

nolu kurumların orta düzey bir başarıya sahip olduğu anlaşılmaktadır. 4 ve 6 nolu olanların ise bu konuda yeterli performans göstermedikleri söylenebilir.



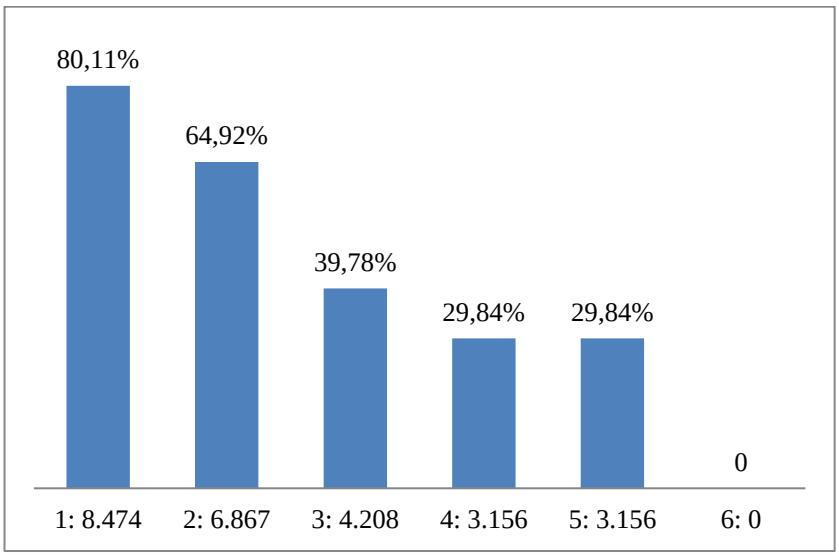
Şekil 42. Belge Yönetim Sistemine Geçerken Hazırlanan Prosedürler

Belge yönetimiyle ilgili hazırlanan prosedürlerin, belgenin üretiminden iletimine, dosyalanmasından arşive kaldırılmasına kadar olan adımlarla ilgili kurallar içermesi beklenir. Böylece, yapılan tüm işlemlerin bir dayanağının olması hedeflenir. Yaşam döngüsünün bütün süreçlerini kapsayan prosedürlerin oluşturulması, güvenilirliğin başarıyla korunmasında önemli bir karine olarak kabul edilmektedir. Belgenin üretilme ve iletilmesiyle alakalı ve dışarıdan gelen belgelerin sisteme kaydedilmesiyle ilişkili kuralların 6 nolu haricindeki diğer tüm kurumların prosedürlerinde yer aldığı görülmüştür. Dosyalama kuralları ise sadece 1 ve 2 noluların prosedürlerinde yer almaktadır. Bununla birlikte, belgeyi arşive devretme kurallarının sadece 1 nolu kurumun prosedüründe bulunduğu gözlenmiştir.

Bu kuralların yanı sıra belgelerin teknolojik göçünün nasıl gerçekleştirileceği ve bu işlemin nasıl tasdik edileceğine ilişkin kurallarla alakalı prosedürlere ihtiyaç vardır. Fakat kurumların bu yönde bir yaklaşımının henüz mevcut olmadığı görülmüştür. Bununla birlikte, e-belgelerin delil değeri için önemli bir referans kaynağı olan log kayıtları ve denetim günlüklerine ilişkin hususların da prosedürlerde yer alması beklenmektedir. Sadece 1 ve 2 nolu kurumlarda bu yönde bir pratiğin mevcut olduğu anlaşılmıştır.

Prosedürlerde donanımların çalışma şartları ve bilgi güvenliğinin nasıl korunacağına ilişkin hususların varlığı, güvenilirliğin başarıyla korunmasına katkıda bulunmaktadır. Sadece 1 nolu kurum, donanımların çalışma şartlarıyla ilgili kuralların kendi prosedüründe mevcut olduğunu belirtmiştir. Bilgi güvenliğiyle ilgili hususların ise 1, 2 ve 3 nolu kurumların prosedürlerinde yer bulduğu görülmüştür.

Kurumlar, bu sorudan en fazla 10.578 puan elde edebilmektedir. 1 nolunun bu konuda çok başarılı, 2 nolunun orta, 3, 4 ve 5 noluların ise zayıf bir dereceye sahip olduğu görülmüştür. Sorulan sorular ışığında 6 nolu kurumun bu konudaki uygulamalarının oldukça yetersiz olduğu anlaşılmıştır.



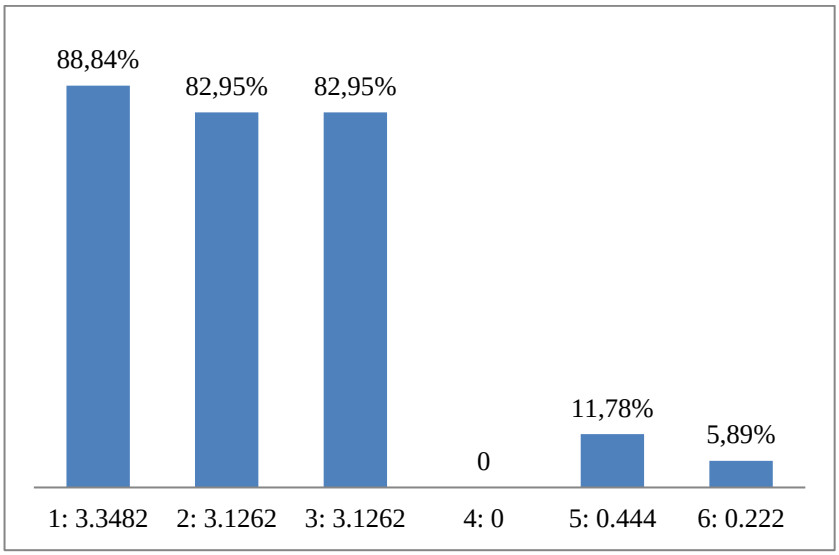
Şekil 43. Belge Yönetimi Prosedürleri

Kurum düzeyinde incelenmeye çalışılan son konu, kurumsal belge yönetimi kapasitesinin geliştirilmesine yönelik pratiklerdir. Burada, kurumsal belge yönetimi politikasının oluşturulması, alan uzmanlarının istihdam edilmesi, kurum çalışanlarının belge yönetimi birimi tarafından eğitilmesi ve TS 13298 Kurumsal Sertifikasyon'un alınması gibi uygulamaların varlığı sorgulanmıştır. Bunlardan belge yönetimi politikasının oluşturulması kapasite geliştirmede temel adımlardan biri kabul edildiğinden kritik zorunlu olarak benimsenmiştir. 1, 2 ve 3 nolu kurumların belge yönetimi politikası bulunmaktadır. Ancak, 1 nolu olan e-belge yönetimi süreci devreye alındıktan sonra politikasını hazırlamıştır.

Saha araştırmasında varlığı sorgulanan bir diğer yaklaşım, alan uzmanlarının yani bilgi ve belge yönetimi bölümü mezunu kişilerin ilgili birimde istihdam edilip edilmediğidir. Sadece 1 nolu kurumda bölüm mezunu istihdamının benimsendiği görülmüştür. Bununla birlikte, çalışanların görev yaptıkları alanla ilgili eğitimler almaları kurumsal gelişime destek sağlar. Belge yönetimiyle ilgilenen personelin eğitimi de bu yönde değerlendirilmektedir. 4 ve 6 nolu dışındaki kurumların bu yönde uygulamalarının bulunduğu anlaşılmıştır.

Bunun yanı sıra güvenilirliğe etkisi araştırılan bir diğer husus, kurum çalışanlarının belge yönetimi birimi tarafından eğitilmesidir. Böylece süreçlerin başarılı bir şekilde yürütülmesine katkı sağlanabileceği düşünülmüştür. 4 nolu haricindeki tüm kurumlarda bunun benimsendiği görülmüştür.

Belge yönetimi kapasitesinin geliştirilmesiyle ilgili olarak sorulan son soru, kurumsal sertifikasyonlar üzerinedir. Bunlar, ilgili sürecin kurum tarafından başarılı bir şekilde gerçekleştirildiğini gösteren araçlardan biridir. Türkiye'de belge yönetimi konusundaki kurumsal sertifikasyon, TS 13298 Standardı'dır. Yazılımların sertifika alabildiği gibi, kurumlar da bu sertifikaya sahip olabilmektedir. Söz konusu sertifikanın hak edilmesi, güvenilirliğin başarıyla korunduğunu gösteren karinelerden biri olarak değerlendirilebilir. Fakat kurumların bu yönde bir uygulamasının bulunmadığı gözlenmiştir.



Şekil 44. Belge Yönetimi Kapasitesi Geliştirme

Kurumlar, bu soruda en fazla 3.769 puan elde edebilmektedir. %80'nin üzerinde performans gösteren 1, 2 ve 3 nolu kurumların çok başarılı, %20'nin altında performans gösteren 5 ve 6 noluların ise yeterli düzeyi sağlayamadığı görülmüştür. 4 nolu kurumun bu konuda bir uygulamasının bulunmadığı anlaşılmıştır.

4.2.3. Nicel Bulguların Değerlendirilmesi

Saha araştırmasında katılımcılardan alınan cevapların neticesine göre kurumlara puanlar verilmiştir. Bu puanlar, soruların ait olduğu düzeylere göre değişiklik göstermektedir. Bir düzeyde en fazla 25 puan elde edilebilmektedir. Başarı sonuçlarını kolay hesaplayabilmek için "elde edilen ham puanı" 100'e tamamlamak gerekmiştir. Bu sebeple kurumlara 25 puan eklenmiştir. Burada amaç, kurumun aldığı toplam puana göre başarısını ortaya çıkarmaktır.

Kurum	Belge Düzeyi Puanı	Teknolojik Koşullar Düzeyi Puanı	Kurum Düzeyi Puanı	Elde Edilen Puan	Toplam Puan	Sıralama	Sonuç
1	11.5604	18.2872	18.6169	48.4675	73.4675	1	Başarılı
2	8.7845	14.718	15.9493	39.4516	64.4516	2	Orta
3	9.194	13.6476	14.3539	37.1955	62.1955	3	Orta
4	7.4101	14.5612	5.4959	27.4672	52.4672	5	Zayıf
5	7.7921	12.4342	8.4786	28.7049	53.7049	4	Zayıf
6	9.0125	12.427	4.4578	25.8973	50.8973	6	Zayıf

Tablo 1. Kurumların Başarı Sıralaması

Tezin her bir alt hipotezini test etmek için sadece ilgili düzeyi değerlendirmenin yeterli olmayacağı kanaatiyle diğer düzeyler de incelenmiştir. Çünkü bu düzeyler belgenin delil değeriyle alakalı tek başlarına bir niteleme oluştururken, diğer taraftan bütünü de etkilemekte, toplam içerisinde bir değere sahip olmaktadır. Bundan dolayı, hipotezi doğrulamak için kurumların bir düzeyde aldıkları puan ile tüm sorular sonucunda elde ettikleri toplam puanın birlikte değerlendirilmesi gerekli görülmüştür. Kurumlar, toplam puanları 0-25 aralığındaysa değerlendirme dışı, 26-40 arasındaysa başarısız, 41-55 arasındaysa zayıf, 56-69 arasındaysa orta, 70-84 arasındaysa başarılı ve 85-100 arasındaysa çok başarılı kabul edilmiştir.

Tezde incelenen her bir güvenilirlik düzeyinde başarılı kabul edilebilmek için "düzeylerde başarılı olma oranı" olan ve eşik değer kabul edilen %60'a ulaşmak

gerekmektedir. Bir düzeyde başarılı olabilmek için gereken asgari puan, her bir düzeyde elde edilebilecek toplam puan olan 25'in %60'lık oranına karşılık gelen 15'dir. Bir kurum, düzeylerde bu değer ve bunun üzerine çıkarsa başarılı kabul edilmektedir.

Hiçbir kurum belge düzeyinde bu eşik değeri aşacak yeterli puana sahip olamamıştır. Bu duruma, kurumların kritik zorunlu olarak belirlenen belgenin ait olduğu işlem, dosya, seri ve birimi seçmemesi, kullanılan algoritmaları ve teknolojik göçle ilgili işlemleri birer üstveri olarak tutmaması ve özgünlüğün tasdik edilmesine yönelik yeterli fonksiyonları gerçekleştirmemenin neden olduğu düşünülmektedir.

Belge düzeyindeki uygulamalarıyla %60 oranını yakalayamayan örgütlerde belgelerin arşivsel bağının yeteri kadar etkin kurulamadığı söylenebilir. Bu durum, diğer düzeylerle birlikte değerlendirildiğinde yeterli performansı gösteremeyen kurumlarda e-imzalı belgelerin delil değerinin ilerleyen yıllarda zayıflayabileceği kanaatini oluşturmaktadır. Arşivsel bağın başarılı kurulamamasıyla ilgili hipotezin, 1 nolu hariç diğer kurumlar için geçerli olduğu görülmüştür.

Tezin teknolojik koşullarla ilgili hipotezini test etmek için kurumların bu düzeyde aldıkları puanla tüm uygulamalar neticesinde elde ettikleri sonucu birlikte değerlendirmek gerekmektedir. Tüm düzeylerde olduğu gibi başarılı olabilmek için gereken %60 'lık asgari puan şartı (15 puan) burada da geçerlidir. Sadece 1 nolu kurumun bu seviyeye ulaştığı gözlenmiştir. Bunun nedeni, 1 nolu kurumun bu konuda daha fazla pratiğinin bulunması olabilir. %60'lık orana ulaşamayan kurumların ise doğru teknolojik koşullara yeteri kadar sahip olmadıkları söylenebilir. Tüm düzeyler göz önünde bulundurulduğunda buradaki hipotezin tüm kurumlar için geçerli olduğu görülmüştür.

Tezin kurum düzeyiyle ilgili olan hipotez test edilirken, başarı seviyesi olan %60'lık orana sadece 1 ve 2 nolu kurumların ulaştığı görülmüştür. Böyle bir başarıda bu konuda daha fazla uygulama yapmalarının etkili olduğu düşünülmektedir. Kurum düzeyiyle ilgili yeterli pratiği bulunmayanların burada yeteri kadar başarılı olamadığı söylenebilir. Tüm düzeylerdeki uygulamalarla birlikte değerlendirildiğinde bu düzeyde başarılı bir sonuca ulaşamayan kurumlarda e-imzalı belgelerin delil değerinin ilerleyen yıllarda zayıflayabileceği kanaati oluşmuştur. Bu düzeyde başarılı olmasına rağmen genel olarak yeterli performans gösteremeyen 2 nolu hariç tutulduğunda, hipotezin diğer kurumlar için doğrulandığı ileri sürülebilir.

4.3. Tartışma

4.3.1. Belge Düzeyi

Nitel ve nicel araştırmada belge düzeyini oluşturan üstveriler, dosyalama ve arşivsel bağ gibi konularla ilgili sorular sorulmuştur. Bazı katılımcılar tarafından e-belge yönetiminin temel direği şeklinde ifade edilen üstveriler, delil değerinin ortaya çıkarılmasında da en kritik nokta olarak görülmüştür. Belge düzeyiyle ilişkili olarak diplomatik özelliklerin ve belgenin üretilme gerekçesi olan mevzuatın bir üstveri olarak kurgulanabileceği dile getirilmiştir. Bununla birlikte, belgenin hangi faaliyet ve fonksiyonlar kapsamında üretildiğine dair bir üstverinin oluşturulabileceği de ifade edilmiştir. Saha araştırmasının nicel kısmında ise kurumlardaki uygulama yazılımlarında diplomatik özelliklerin birer üstveri olarak kurgulandığı gözlenmesine rağmen belgenin üretilme gerekçesi olan mevzuat ve ait olduğu fonksiyona ilişkin üstverilerin mevcut olmadığı anlaşılmıştır.

İncelenen bu üstverilerin aslında bilinmesine rağmen bir üstveri biçiminde kurgulanmadığı ve bu bağlamda bir araya getirilmediği dikkat çekmiştir. Bu durum cevaplara yansımış; kurumların %36'lık bir oranla başarılı kabul edilen %60'lık dilimin altında kaldıkları, bu sebeple üstverilere ilişkin uygulamalarda yeterli performans sergileyemedikleri anlaşılmıştır. Aynı zamanda, delil değeri teyidi için kritik rol üstlendiği düşünülen özgünlüğün onaylanması teknikleri ile belgedeki kişiler gibi üstverilerin hiçbir kurumda mevcut olmadığı görülmüştür. Bunların eksikliği delil değerini zayıflatabilecek bir risk olarak değerlendirilmektedir.

Saha araştırmasında kritik edilen bir diğer husus, dosyalamanın delil değerine etkisidir. Araştırmanın nitel kısmında, provenansı ispatlayıp sahihliği gösterdiği için dosyalama pratiklerinin belgenin delil özelliklerinden biri olduğu ifade edilmiştir. Seri-dosya ve belge hiyerarşisinin bozulması durumunda belgelerin fonksiyonla ilişkisinin zarar göreceği ve bu durumda hangi faaliyetin işlemi kapsamında doğduğunun anlaşılamayacağı, bu yüzden delil değerinin açığa çıkarılmasının güçleşeceği dile getirilmiştir.

Saha araştırmasının nicel kısmında elde edilen sonuçlara göre, kurumlarda gerçekleştirilen dosyalama uygulamalarının provenansı yeteri kadar gösteremediği anlaşılmıştır. Çünkü belgeler üretilirken her ne kadar birim belli olsa da o birimin görevi bağlamında belgenin ait olduğu fonksiyonun önceden analizi yapılarak faaliyet ve işlemlerin

belirlenmediği yerlerde hatalı uygulamalar yapılabilmektedir. Mesela belge üretilirken doğduğu fonksiyona bağlı seri, faaliyet ve işlemin doğru seçilemediği görülmüştür. Bunun yanı sıra özellikle birden fazla görevi yürütmek durumunda olan kişilerin hazırladığı evraklarda sorunlar yaşanabilmektedir. Kişiler asıl yetkilendirildikleri rolün dışında, verilen görev gereği farklı fonksiyonlara ait işlemleri de yapabilmektedir. Bu durumda belgelerin ilişkili olduğu faaliyet ve işlem yanlış seçilebilmektedir. Bunun neticesinde aidiyeti belirlenemeyen öksüz belgeler oluşmaktadır. Belgenin provenansını ispatlayıp sahihliğini gösterecek bir araç olarak kabul edilen bu adımların yokluğunun ilerleyen yıllarda kurumlarda üretilen belgelerin delil değerinden şüphe duyulmasına neden olabileceği ileri sürülebilir.

Dosya planlarının, fonksiyon analizi neticesinde tespit edilecek faaliyet ve işlemlere göre hazırlanması gerekir. Böylece hazırlanan belgeler, dikkatlice seçilecek dosya kodları sayesinde ait oldukları faaliyetle ilişkilendirilir. Ancak, kurumlardaki uygulamaların pek de belirtildiği şekilde olmadığı, çoğu yerde bu kodların usulen verildiği görülmüştür. Oysa doğru dosya kodu tercihi, belgenin provenansını kaynağa göre oluşturmada önemli bir referanstır. Sürecin bu şekilde işletilmesi gerektiğine rağmen, e-belge yönetimi uygulamalarında dosya kodlarının belgeye bir etiket olarak tanımlandığı, bunun neticesinde belgenin bir işlem, faaliyet ve işle ya ilişkilendirilmediği ya da yanlış ilişkilendirildiği bilinmektedir. Bu tür yanlış uygulamalar neticesinde belgelerle ait oldukları fonksiyon ilişkisi kurulamadığından aidiyet zincirinin tesis edilememesi sonucuyla karşılaşılmaktadır. Hâliyle aidiyet zinciri kurulamamış belgelerin delil değerinde şüphe oluşabilmektedir. Durum böyle olunca, kurumlarda dosyalamanın entelektüel boyutunun yeteri kadar anlaşılmadığı fark edilmiştir.

Nitel araştırmadaki bir katılımcı, dosyalama meselesini Türkiye'nin gelecek 20 yılda karşılaşacağı en büyük sorunlardan biri olarak tanımlamıştır. Bu yaklaşım, sahadaki pratiklerle uyumludur. Fonksiyonla serinin, işle dosyanın eşleşmesi gerektiği göz önüne alındığında, sadece 1 nolu kurumda fonksiyon analizi yapılarak belge hiyerarşisi oluşturulduğu ve bu eşleşmenin yapıldığı görülmüştür. Nicel araştırma sonucunda, kurumlardaki belgelerin ait oldukları faaliyet ve fonksiyonlarla ilişkisinin yeteri kadar kurulamadığı, arşivsel bağın tesis edilemediği gözlenmiştir. Nitel araştırmada başka bir katılımcı, EBYS'lerde bugüne kadar oluşmuş e-belgelerin yeni

baştan tasnif edilmesinin gerekeceğini ifade etmiştir. Sahadaki uygulamaların bu kanaati doğruladığı düşünülmektedir.

Dosyalamanın yanı sıra incelenen bir diğer konu değerlendirmeyle ilgilidir. Araştırmanın nitel kısmında değerlendirmede risk iştahını belirlemenin belgelerin delil değerini güçlendirdiği ileri sürülmüştür. Değerlendirmenin sonucuna göre delil değerini etkileyecek arşiv imza, zaman damgası, kurumsal mühür ve arşiv mührü gibi uygulamaların kullanılabileceği dile getirilmiştir. Bununla birlikte, uzun dönemli korumaya ilişkin üstverilerin eklenebileceği de ifade edilmiştir. Fakat bu uygulamaların sahada yeteri kadar yer bulamadığı görülmüştür. Nicel araştırmada katılımcılardan elde edilen cevaplar neticesinde kurumların hiçbirinde bütünlük analizinin düzenli kontrol edilip, bunun bozulmasına karşı risk değerlendirmesi yapılmadığı, arşive devredilecek belgeler için özgünlük değerlendirme raporunun oluşturulmadığı ve bu belgeler için kullanılacak yeni üstverilerin tasarlanmayıp bir tanımlama standardının düşünülmediği anlaşılmıştır. Bu eksikliklerin, ilerleyen yıllarda e-imzalı belgelerin delil değerini zayıflatma riski taşıdığı söylenebilir.

Saha araştırmasında incelenen bir diğer konu EYP ile ilgilidir. Araştırmanın nitel kısmında bir katılımcı, EYP'nin belgelerin delil değerinin korunmasında e-imzadan sonra en güçlü mekanizma olabileceğini ifade etmiştir. Başka bir katılımcı ise EYP'siz belgelerin EYP'sinin oluşturulması gerekliliğine vurgu yapmıştır. 2020 yılında güncellenen RYY'ye göre yeni üretilecek tüm belgelerin EYP kapsamında hazırlanması bir zorunluluktur.

Araştırmanın nicel kısmında tüm kurumlarda üretilen belgelerin bir EYP'ye sahip olduğu gözlenmiştir. Fakat sadece iki kurumda (1 ve 3) belge üzerindeki imzaların geçerliliği bitmeden EYP'nin zaman damgası ile damgalandığı görülmüştür. Bununla birlikte saha araştırmasının nitel kısmında katılımcılardan biri, koruma üstverisi, belgenin üretildiği yazılım versiyonu ile hangi donanım ve yazılımla açılabileceği bilgileriyle zenginleştirilecek EYP'nin arşivleme için kullanılabileceğini ifade etmiştir. Bu yaklaşımın sahada görülen yetersiz üstveri sorununun çözümüne katkı sağlayacağı düşünülmektedir. Böylece, belgelerin delil değerinin güçlendirilebileceği söylenebilir.

Saha araştırmasında kritik edilen bir diğer konu, belgelerin özgünlüğünün tasdik edilmesiyle ilgilidir. 2 kurumun (1 ve 3) 2020 yılında güncellenen RYY'de yer

bulan e-imzaların arşiv imzası tipine dönüştürülmesi adımını uyguladığı görülmüştür. Fakat hiçbir kurum, bütünlük analizini düzenli olarak kontrol etmemektedir. Bu husus, saha araştırmasının nitel kısmında da katılımcılara sorulmuş ve katılımcılar, tanımlama bilgilerinin incelenmesi, arşiv mührü, kurumsal mühür ve yazılımsal güvenilirlik testlerinin özgünlüğün tasdik edilmesinde kullanılabileceğini belirtmiştir. Bunlardan sadece tanımlama bilgilerinin incelenmesi uygulamasının bir kurumda (2 nolu kurum) benimsendiği gözlenmiştir. Tüm bunlarla birlikte, kurumlarda JHOVE ve DROID gibi dosya tanımlayıcıların kullanılmadığı anlaşılmıştır.

Özgünlüğün korunması yönünde uygulamalar geliştiren kurumlarda ise bu sürecin özet değeri ve log kayıtları kontrolüyle gerçekleştirildiği belirlenmiştir. Yapılan incelemeler neticesinde kurumların özgünlüğün tasdik edilmesi uygulamalarında yeterli performansı gösteremediği görülmüştür. Bu durumun, ilerleyen yıllarda belgelerin delil değerini zayıflatma riski taşıdığı söylenebilir.

Saha araştırmasında belge düzeyiyle ilgili olarak kritik edilen bir diğer konu, tasfiye meselesidir. Doğru dosyalama, her ne kadar belgelerin güncel dönemleri için önemli gözükse de arşive devirleri hatta tasfiye için de ehemmiyetli bir konudur. Çünkü saklama süreleri sonunda gerçekleştirilecek tasfiye işlemi, belge düzeyinde değil dosya düzeyinde düşünülmelidir. Bu yapılarak imhalıklar ayıklanırken, arşiv malzemesi olması gerekenler de açığa çıkarılır. Durum bu şekilde olmasına rağmen, bu konuda kurumların yeterli performansı gösteremediği görülmüştür. Bu durum, belgelerin ait oldukları dosyalarıyla birlikte arşive devredilmesi gibi uygulamalarda yeteri kadar farkındalığın mevcut olmamasından kaynaklanabilir.

Belge düzeyindeki sorular analiz edildiğinde hiçbir kurumun eşik değer seviyesi olan 15 puana erişemediği görülmüştür. Ancak, 1 nolu kurum belge düzeyindeki uygulamaları açısından en başarılısıdır. Bunun nedeni bu kurumun fonksiyon analizi yaparak belge hiyerarşisi oluşturması, belgeyi sistemden tasfiye ettikten sonra akıbeti hakkında bir bilgi notu tutması gibi diğer kurumların gerçekleştirmediği pratikleri sahaya yansıtması olabilir.

Buraya kadar elde edilen sonuçlar, kurumlarda oluşan belgelerin arşivsel bağının yeteri kadar iyi korunamadığına işaret etmektedir. Bu durumun bir nedeni de kurumların belge yönetimini bir süreç olarak değil yazılım olarak değerlendirmesi olabilir. Örneğin belge yönetimini bir süreç olarak ele almış olsalardı kurumların kullandıkları

üstverilerde farklılıklar olması gerekirdi. Araştırma sırasında uygulama yazılımının sunduğu üstverilerle yetinildiği, kurumsal ihtiyaçlara göre geliştirmek için yeni ve farklı alanlar açmanın pek düşünülmediği görülmüştür.

Hâliyle tüm bu değerlendirmeler ışığında, dosyalamanın düzenli yapılmamasının, üstverilerin yeteri kadar geliştirilmemesinin ve kurumsal politika ve prosedürlerin yetersizliğinin arşivsel bağın korunmasını güçleştirdiğini söylemek mümkündür. Tüm bu olumsuzluklar, arşivlenen belgelerin delil değerinin korunmasını engelleyen faktörler olarak gözükmektedir.

4.3.2. Teknolojik Koşullar Düzeyi

Saha araştırmasının hem nitel hem de nicel kısmında log kayıtları, kurumların belge yönetimi uygulamalarının TS 13298 ve 27001 standartlarına uyumluluğu, yazılımların kaynak kodlarının saklanması, teknolojik göç ve yedekleme işlemleri gibi arşivsel güvenilirliğin teknolojik koşullar düzeyini oluşturan konular kritik edilmiştir. E-imzalı belgelerin güvenilirliği meselesi, bilgi teknolojilerinin sunduğu fırsat ve tehditlerle doğrudan ilişkili olduğundan teknolojik koşullar düzeyi, kurum ve belge düzeyine göre nicel kısımda biraz daha ön plana çıkmaktadır.

E-ortamda oluşturulmuş bir belgenin bütün işlem izlerinin görülebildiği log kayıtları, teknolojik koşullarda ilk ele alınması gereken hususlardan biridir. Saha araştırmasının nitel kısmında bu kayıtların zenginliğinin belgelerin delil değerini güçlendirebileceği ifade edilmiştir. Katılımcılar, bu kayıtların belgedeki kişileri ve yapılan işlemin ne zaman gerçekleştirildiğini göstererek zaman damgasıyla damgalanmasına vurgu yapmıştır. Araştırmanın nicel kısmında ise 6 nolu haricinde diğer kurumlardaki log kayıtlarının belgedeki kişileri gösterdiği anlaşılmaktadır. Tüm kurumlarda bu kayıtlar aracılığıyla işlemlerin ne zaman gerçekleştirildiğinin belirlenebildiği görülmüştür. Bununla birlikte 2 ve 3 nolu haricinde diğer kurumlarda log kayıtlarının zaman damgası ile damgalandığı gözlenmiştir.

Belge yönetimi sürecindeki her aşamayı barındırdığından log kayıtları, delil değerinin sorgulanmasında başvurulabilecek temel araçlardan biri olarak değerlendirilmektedir. Durum böyle olunca, belgelerin delil değerinin korunabilmesi için bu kayıtların da belirli bir standarda sahip olması gerekir. Ancak, sahada yapılan incelemelerde kurumların log kayıtlarının belge varlığının bütün referans kaynaklarını

ihtiva ettiği bilgiler açısından %70'lik bir başarı oranına sahip olduğu görülse de yeteri kadar standartlaşmanın mevcut olmadığı söylenebilir. Bundan dolayı, bu kayıtların her kurumda asgari olarak içermesi gereken özelliklerinin belirlenmesine ihtiyaç duyulmaktadır. Nitel araştırmadaki bir katılımcı, log kayıtlarının belge yönetimi ilkeleri çerçevesinde değerlendirilerek TS 13298'in bir parçası olması gerektiğini ifade etmektedir.

Log kayıtlarının yanı sıra araştırmanın nitel kısmında belgelerin delil değerini güçlendirebileceği ifade edilen bir diğer husus, yazılımların kaynak kodlarının saklanmasıdır. Ancak kurumların bu yönde bir uygulamasının bulunmadığı görülmüştür. Bu durumun her ne kadar yazılımı üreten firmaya duyulan güvenden kaynaklanabileceği düşünülse de uzun dönemde yaşanabilecek sorunların çok da tartışılmadığı değerlendirilmektedir. Başka bir deyişle, bu durum kurumların belgelere gelecekte de erişebilmeyi değil, sadece güncel dönemde üretip kullanmaya odaklanmalarından kaynaklanabilir. Hâl böyle iken yazılımı üreten firma hizmet vermeyi sürdüremezse; teknik veya teknolojik bir sıkıntı nedeniyle kaynak kodlarını koruyamazsa kurumlar faaliyetlerinin delili olan belgeleri nasıl muhafaza edecektir? Bundan dolayı olsa gerek nitel araştırmada bir katılımcı, kamunun farklı şirketler tarafından geliştirilen EBYS'lerin kaynak kodlarının korunması yönünde bir genelge hazırlamasını önermiştir. Bu öneri, belgelerin delil değerinin korunmasında başarıyı artırabilecek bir unsur olabilir.

Saha araştırmasında incelenen bir diğer konu, kurumların teknolojik göç uygulamalarıdır. Üç kurumun bu konuda bir tecrübeye sahip olduğu görülmüştür. Sadece bir kurum (Kurum 5), belgenin taşıyıcı ortamının ne zaman değiştirileceği hususunda inceleme yapmakta; yine başka biri (Kurum 3), teknolojik göç sonrası belgelerin erişilebilirliğini ve okunabilirliğini kontrol etmektedir. İki kurumda (Kurum 3 ve Kurum 6) belgenin ne zaman göç ettirildiği bilgisi, belge profilinde yer almaktadır. Diğerlerinde bu konuda yeteri kadar tecrübe olmaması, kurumların yaklaşık on beş yıldır e-imzalı belge üretmesinden kaynaklanabilir. İlerleyen yıllarda format değişiminin kurumların gündeminde daha fazla yer edineceği düşünülmektedir.

Kurumlarda henüz bu konuda yeterli uygulama görülmese de saha araştırmasının nitel kısmına dâhil olan katılımcıların çeşitli önerileri dikkat çekmektedir. Katılımcılar, Devlet Arşivleri Başkanlığının teknolojik göçte uygulanacak kuralları belirleyerek, göçün Başkanlık tarafından onaylanması gerektiğini ifade etmiştir. Ancak bu onay kim

tarafından yapılırsa yapılsın, göç sonrasında belgelerin özniteliklerinin değişmediğini gösterecek mekanizmalara ihtiyaç duyulmaktadır. Burada, otonom araçlarla EYP'lerin karşılaştırılması, üstveriler ve log kayıtlarının kontrol edilmesiyle e-delil elde etme yöntemlerinin kullanılabileceği düşünülmektedir. Bununla birlikte, katılımcılardan birinin ifade ettiği gibi teknolojik dönüşüm süreci üstverisi kurgulanmalıdır. Böylece, bu üstveri delil değerinin korunmasına yönelik bir mekanizma olarak kullanılabilir.

Saha araştırmasında kritik edilen bir diğer husus yedekleme uygulamalarıdır. Araştırmanın nicel kısmında incelenen kurumların yedekleme işlemlerinin başarılı olduğu söylenebilir. Ancak, bazı kritik üstverilerin kullanılmadığı gözlenmiştir. Örneğin yedeklemeyi onaylayan üstverisinin sadece iki kurumda (Kurum 1 ve Kurum 4) mevcut olduğu görülmüştür. Kişilerin yedeklemeleri onaylamasından ziyade bir süreç yönetimi benimsenerek e-mührün başarılı gerçekleşen yedeklemelerin tasdik edilmesinde kullanılabileceği düşünülmektedir. Böylece, belgelerin delil değerinin başarıyla korunduğuna ilişkin bir karine sunulabilir.

Güvenilirliğin başarıyla korunmasında etkili olan etmenlerden biri de uygun donanım koşullarıdır. Saha araştırmasının nitel kısmında katılımcılar, donanımların kullanım ömrü bittikten sonra yenilenmesi gerektiğini belirtmiş, bir katılımcı WORM disklerin kullanılmasını önermiştir. Nicel kısımda ise biri haricinde (Kurum 2) tüm kurumlarda donanımlar, kullanım ömrü bittikten sonra yenilenmektedir. Ancak, sadece birinde (Kurum 3) WORM disklerin kullanıldığı görülmüştür. Saha araştırmasının nitel kısmında bir katılımcının belirttiği üzere teknoloji yenileme politikalarının hazırlanmasına ihtiyaç duyulduğu anlaşılmaktadır.

Belgelerin delil değerinin korunmasında blokzincir teknolojisi, yapay zekâ, derin ve yapay öğrenme ile e-delil elde etme yöntemleri gibi teknolojik yaklaşımlardan faydalanıldığı bilinmektedir. Kurumların bu uygulamaları da sorgulanmış, söz konusu teknolojilerin kullanılmadığı görülmüştür.

Teknolojik koşullar düzeyinde güncel belgelerle arşivlenenlerin farklı konumlarda saklanıp saklanmadığı da incelenmiştir. Sadece 5 nolu kurumda bu yönde bir uygulamanın bulunduğu görülmüştür. Bu husus, saha araştırmasının nitel kısmında da üzerinde uzlaşmanın bulunmadığı bir adım olarak öne çıkmıştır. Bu ayrımın delil değerine bir etkisi olmadığını düşünen katılımcılar, oluşum ve arşivcilik boyutu itibariyle güncel belgelerle arşivlenenlerin arasında artık büyük farkların

bulunmadığına dikkat çekerek delil değerini ortamın değil, oluşma niteliklerinin belirlediğini ifade etmiştir. Aksini savunanlar ise uzun süre saklanacak belgelerle kısa süreli saklanacaklara yapılacak muamelelerin aynı olmayacağını belirterek belge yönetimi ve arşiv yönetiminin birbirinden ayrıldığını dile getirmiştir. Arşivlenenlere yapılacak üstveri eklemeleri, format değişiklikleri ve zaman damgası güncellemesi gibi işlemlerin güncel belgelerden farklılık arz ettiği bilinmektedir. Bu işlemleri başarılı bir şekilde gerçekleştirmek için arşivlenenlerle güncel olanlar ayrı saklama ortamlarında tutulmalıdır.

Saha araştırmasının nicel kısmında kurumların teknolojik koşullarla ilgili uygulamalardaki başarı oranının belge düzeyindekine göre daha yüksek olduğu görülmüştür. Bunun kurumların e-belge yönetimi uygulamalarını bir süreçten ziyade daha çok bir yazılım olarak algılamalarından kaynaklandığı düşünülmektedir. Hâliyle bir yazılım geliştirmenin gereklerinin sahaya daha iyi yansıtıldığı ifade edilebilir.

4.3.3. Kurum Düzeyi

Belge ve teknolojik koşullar düzeyinde başarılı olmak için gerekli olan birtakım adımlar atılsa da belgelerin delil değerinin korunması için bunların yeterli olmadığı değerlendirilmektedir. Çünkü kurumlarda belgelerin üretilmesi, iletilmesi, dosyalanması gibi prosedürlerin bulunması da delil değerini etkilemektedir. Belge yönetiminin başlıca fonksiyonları olan bu uygulamalara ilişkin kurallar, kurum düzeyinin başarısını yakından ilgilendirmektedir.

Saha araştırmasında güvenilirliğin kurum düzeyini oluşturan e-belge ve e-arşiv yönetimi politikasının belirlenmesiyle belgelerin üretilmesi, iletilmesi, imzalanması ve dosyalanması gibi prosedürlerin varlığı kritik edilmiştir. Nicel kısımda kurumlara belge yönetim sistemine geçerken yürüttükleri uygulamalar sorulduğunda sadece ikisinin (Kurum 2 ve Kurum 3) e-belge yönetimi politikası belirlediği görülmüş; buna karşın hiçbir kurumda e-arşiv yönetimi politikasının bulunmadığı anlaşılmıştır. Bununla birlikte, kurumların belge yönetimiyle ilgili prosedürlerinde belgenin tanımlanmasına ilişkin kurallar ve teknolojik göçün geçerlilik yöntemleri gibi hususların yer almadığı gözlenmiştir. Dosyalama kurallarının sadece bir (Kurum 1), arşive devretme kurallarının ise iki kurumda (Kurum 1 ve Kurum 2) yer aldığı görülmüştür.

Bu kurallar, belgelerin nasıl yönetilmesi gerektiğine ilişkin idari ya da hukuki bir dayanak oluşturmaktadır. Bunların eksikliği, log kayıtlarında nelerin bulunması gerektiğini açıklayan prosedürler gibi, delil değerinin korunamamasına neden olabilecek mahiyettedir. Ancak kurumlar, genellikle bu eksiklikleri arşiv iş ve işlemleri konusunda bağlı oldukları kurum olan Devlet Arşivleri Başkanlığının kendilerini yönlendirmemesine bağlamaktadır. Bu yaklaşım, saha araştırmasının nitel kısmında ifade edilen hususlarla benzerlik göstermektedir. Nitel araştırmada katılımcılar, Başkanlığın kurumların belge yönetimi politika ve prosedürlerini denetlemesinin belgelerin delil değerini güçlendireceğini ifade etmiştir. Başkanlığın e-belge ve arşiv yönetimi politikası geliştirmesi, standartlar ve teknik rehberler hazırlaması, teknolojik öngörü politikası oluşturması katılımcıların ifade ettiği görüşler arasındadır. Bununla birlikte, zorunlu üstverilerin kararlaştırılması, milli bir format benimsenmesi, log kayıtlarının denetlenmesi, e-imza kök sertifikaları ve kaynak kodlarının saklanması gibi öneriler de dile getirilmiştir.

Kurumlarda oluşan e-imzalı belgelerin delil değerinin başarıyla korunabilmesi için arşivsel bağ, teknolojik koşullar, kurumsal politika ve prosedürlerle ilgili ciddi uygulamalara ihtiyaç duyulmaktadır. Bunlar başarılı bir şekilde yerine getirilmediğinde, delil değerinin de o derece zayıflama ihtimalinin bulunduğu söylenebilir. Bu sorunun kurumların belge yönetimini daha çok yazılımsal bir mesele gibi görmesinden kaynaklandığı düşünülmektedir. Tüm kurumların, teknolojik koşullar düzeyinde aldığı ortalama puanın, diğer düzeylere göre daha fazla olmasının bu kanaati doğruladığını ifade etmek mümkündür.

SONUÇ

Arşivlenen e-imzalı belgelerin uzun süre muhafazaları sırasında özniteliklerini koruyamama durumu bir problem olarak güncelliğini sürdürmektedir. Bilim insanları ve saha uzmanlarına göre bu problem, belgelerin delil değerini tartışmalı hâle getirebilir. Bu durumun, standartlara uygun geliştirilmemiş uygulama yazılımlarının ürünü e-belgelerin idari, hukuki ve teknik açıdan gerekli bileşenlere sahip olamaması, olanların da uzun süre muhafaza edilememesinden kaynaklanabileceği dile getirilmektedir. Bu sorunlar, belgelerin güvenilirliğinden şüphe duyulması riskini barındırmakta; özgünlük, bütünlük ve kullanılabilirlik gibi karakteristik özelliklerin devam edip etmeyeceğinin tartışılmasına neden olmaktadır. Tezde Türkiye'deki kurumların EBYS'lerinde oluşan e-imzalı belgelerin delil değerinin arşivsel güvenilirlik açısından nasıl korunabileceği ele alınmıştır. E-imza, zaman damgası ve e-mühür gibi yapıların kırılganlıklarına rağmen kurumların gerekli denetimleri uygulamamasından dolayı belgelerin delil değerinde kayıplar yaşanabilir hipoteziyle yola çıkılmıştır. Hipotezi doğrulamak için seçilen örnekler ışığında kurumların bu konudaki uygulamaları değerlendirilmiştir.

Sahada yapılan gözlemlerde e-belgelerin arşivlenmesi sürecinde risk ve tehditlere bağlı sorunlarla henüz yeteri kadar yüzleşilmediğinden, Türkiye'de ilgililerin güvenilirlik meselesine çok da öncelik vermediği anlaşılmıştır. Bu sebeple uzun vadede oluşabilecek riskler henüz sorun olarak görülmediğinden öncelikle problemin keşfedilmesine ihtiyaç duyulmuştur. Bu keşif için gerek sahada yapılan gözlemler gerekse literatür okumaları sırasında dikkat çeken sorular konuyla ilgili kanaatleri pekiştirmiştir. Bu kanaatleri sınamak amacıyla saha araştırması yapılmıştır.

Araştırma gerçekleştirilirken tezde problemin önce uzmanlarla görüşülüp keşfedilerek, sonrasında belirlenen örneklemde probleme ilişkin değişkenlerin saptanıp sayısal olarak değerlendirilmesi fikri benimsenmiştir. Bu yapılarak problemin daha iyi analiz edilebileceği düşünülmüştür. Bunun için farklı kurumlardaki e-belge yönetimi sistemini kurup yürüten ve süreci değerlendirip denetleyen 9 saha uzmanıyla görüşmeler yapılmış; 6 kurumdan oluşan bir örneklemde de analizler gerçekleştirilmiştir.

Elde edilen bulgular, nitel ve nicel olmak üzere iki aşamada değerlendirilmiştir. Nitel kısımda üstverilerin zenginleştirilmesi, dosyalamanın usulüne uygun gerçekleştirilmesi, EYP'nin bir güvenilirlik mekanizması olarak kurgulanması, konu

ve vaka dosyası ayrımına dikkat edilip arşivsel bağın muhafaza edilmesi, güncel belgelerle arşivlenenlerin ayrı yerlerde saklanması, yedekleme ve log kayıtları rehberinin çıkarılması, bu kayıtların standartlaştırılması, uygulama yazılımlarının kaynak kodlarının korunması, risk yönetiminin benimsenmesi ve Devlet Arşivleri Başkanlığının kurumları denetlemesiyle ilgili sorular sorulmuştur. Bunlar içerisinde güncel belgelerle arşivlenenlerin ayrı yerlerde saklanması düşüncesinin yeteri kadar benimsenmediği görülmüştür. Bunun nedeni katılımcıların, "belgelerin delil değerini saklandığı konumun değil, oluşma şeklinin belirlediği" düşüncesine sahip olmalarıdır. Böyle bir kanaatin, katılımcıların daha çok güncel belgelerle muhatap olup, arşivlenen e-belgelerin gereksinimleriyle çok da karşılaşmamalarından kaynaklandığı düşünülmektedir. Diğer soruların saha uzmanları tarafından benimsendiği anlaşılmıştır.

Araştırmanın nitel kısmında katılımcılar, kurumlarda oluşan e-imzalı belgelerin delil değerinin arşivsel güvenirlik yaklaşımıyla nasıl incelenebileceği hakkında birtakım görüşler ileri sürmüşlerdir. Saha uzmanları, dosyalama ve üstverilerin önemine dikkat çekerek belgelerin zenginleştirilmiş bir EYP ve log kayıtlarıyla birlikte arşivlenebileceğini ifade etmişlerdir. Bununla birlikte, Devlet Arşivleri Başkanlığının teknolojik dönüşüm süreci üstverisi oluşturarak log kayıtlarıyla ilgili standartları belirlemesi gerektiği dile getirilmiştir. Delil değerinin korunması için e-imzanın tek başına yeterli olamayacağı vurgulanarak, kök sertifikaların yedeklenmesi ve TÜBİTAK'ın kurumlardaki e-imza süreçlerini denetlemesi önerilmiştir. Aynı zamanda kurumların EBYS kaynak kodlarını saklaması ve kamunun bu yönde bir genelge hazırlaması tavsiye edilmiştir. Bununla birlikte, EBYS'lerin sadece bir veri tabanı gibi düşünülmesinin ciddi olumsuzluklara neden olduğu aktarılmıştır. Devlet Arşivleri Başkanlığının güvenilirliği onaylayacak en üst kurum olduğu, bunun için teknik rehber hazırlanması gerektiği vurgulanmıştır.

Araştırmanın nicel kısmında 6 kurum özelinde e-imzalı belgelerin delil değerinin mevcut e-belge yönetimi uygulamalarında hangi oranda korunduğu analiz edilmiştir. Burada 3 alt hipotez belirlenmiştir. Bu hipotezler aynı zamanda arşivsel güvenilirliğin belge, teknolojik koşullar ve kurum düzeyiyle ilişkilendirilmiştir.

Belge düzeyiyle ilişkili olan hipotez, arşivsel bağın başarılı bir şekilde kurulamadığı örgütlerde delil değerinin zayıflayacağı şeklindedir. Kurumlarda arşivsel bağın yeteri kadar korunamadığı anlaşılmıştır. Bunun nedenlerinden biri, kurumların

belge yönetimini bir süreç değil, yazılım olarak görmeleridir. Uygulama yazılımlarının sunduğu üstverilerle yetinildiği, kurumsal ihtiyaçlara göre geliştirmek için yeni ve farklı alanlar açmanın pek düşünülmediği gözlenmiştir. Elde edilen veriler ışığında, kurumlarda düzensiz dosyalama, yeteri kadar geliştirilmemiş üstveriler ile kısıtlı politika ve prosedürlerin arşivsel bağı koruyamayabileceği kanaati oluşmuştur. Arşivsel bağ hipotezinin, 1 nolu dışında diğer kurumlarda doğrulandığı görülmüştür.

Arşivsel güvenilirliğin teknolojik düzeyiyle ilgili olan hipotez, doğru koşulların mevcut olmadığı kurumlarda delil değerinin zayıflayacağı şeklindeydi. Belge ve kurum düzeyindekilere göre burada bakanlıkların daha başarılı olduğu tespit edilmiştir. Bu başarının, kurumların EBYS'yi bir uygulama yazılımı olarak görüp gereklerini yerine getirmelerinden kaynaklandığı düşünülmektedir. Örneğin EBYS yedeklemelerinin düzenli yapıldığı, donanımların da güncel olduğu gözlenmiştir.

Kurum düzeyiyle ilişkili olan hipotez ise belge yönetimi konusunda politika ve prosedürlerin yetersiz olduğu örgütlerde delil değerinin zayıflayacağı şeklindeydi. Kurumsal politika ve prosedürler çıkarılmadığında, delil değerinin de o derece zayıflama ihtimalinin bulunduğu görülmüştür. Örneğin kurumlarda e-arşiv yönetimi politikasının hazırlanmadığı, belgelerin tanımlama kurallarının belirlenmediği ve teknolojik göç prosedürlerinin oluşturulmadığı anlaşılmıştır. Buradaki hipotezin 2 nolu hariç diğer kurumlarda geçerli olduğu gözlenmiştir. Belge ve kurum düzeyiyle ilgili hipotezler bir bakanlık dışında diğerlerinde gerçeklendiğinden, ana hipotezin doğrulandığı kabul edilebilir.

Sadece 1 nolu kurumda delil değerinin diğerlerine göre daha az zayıflama riskinin bulunduğu görülmüştür. Kurumun delil değerini daha iyi koruyacak pratikler benimsemesinin bunda etkili olduğu düşünülmektedir. Diğerlerinin gerekli çözümleri yeteri kadar geliştiremedikleri anlaşılmıştır. Bunun nedenlerinden biri, elektronik belge yönetimi iş geliştirme süreçlerinin olması gereken sistem kriterleri ışığında yürütülmemesidir. Bundan dolayı, kurumların fonksiyonlar ve iş süreçlerini tanımlayıp bunları belgelerle ilişkilendirmedikleri, fonksiyon analizi neticesinde belge hiyerarşisi oluşturmadıkları, iş süreçlerine dair bir dokümantasyon hazırlamadıkları, belgeyi arşive devretme kuralları belirlemedikleri, özgünlüğün korunmasına yönelik strateji geliştirmedikleri gözlenmiştir. Bu yüzden uzun dönem korunmaları sürecinde

belgelerin ait olduğu faaliyet ve fonksiyon belirlenemeyebilir. Bu olumsuzluk sebebiyle özgünlüğün tasdik edilmesi güçleşir.

Delil değerinin korunmasında başarılı olan 1 nolu kurumun e-belge yönetimiyle ilgili biriminde uzman olarak bilgi ve belge yönetimi mezunlarının istihdam edilmiş olması dikkat çekmektedir. E-belgelerin yönetilmeleri sırasında delil değerine ilişkin kritik unsurların neler olması gerektiğini fark eden bu uzmanlar, arşiv pratiklerini bildiklerinden belgelerin uzun dönemli muhafazaları sırasında da bu kritik unsurların korunması için gerekli koşullarla alakalı öngörüde bulunabilmektedirler. E-belgeler, teknoloji-yoğun ürünler olsa da delil değerinin muhafazası için bilgisayar mühendisleriyle bilgi ve belge uzmanlarının birlikte çalışmaları gerektiği açıktır. Tüm bu değerlendirmelerin ardından delil değerinin korunması için şunlar önerilebilir:

1. Her ne kadar belgelerin delil değeri konusunda hukukun öngördüğü genel kriterler bulunsa da belgenin kullanıldığı sektöre göre farklı hususiyetler aranabilmektedir. Kanada'da görüldüğü gibi ortak bir referans niteliğinde "Elektronik Belgelerin Delil Değeri Özellikleri" prosedürü çıkarılabilir.
2. Milli Arşiv, TÜBİTAK, BTK ve TSE gibi otorite kurumlar, e-imzalı belgelerin delil değerinin korunması için ihtiyaç duyulan kılavuz, teknik rehber ve standartları hazırlamalıdır. E-imza kök sertifikaları, merkezi bir depoda saklanmalıdır. Teknolojik öngörü politikaları oluşturulmalıdır. E-imzalı belgelerin teknolojik göçünü onaylayacak prosedürler düzenlenmelidir. Log kaydı standartları çıkarılmalıdır. Devlet Arşivleri Başkanlığı, delil değeri konusunda kurumları denetlemelidir.
3. Arşivlenen e-imzalı belgelerin teknolojik eskimeye uğramamaları için formatlarının değiştirilip, e-imzaların yenilenme süreçlerinin çok da planlanmadığı anlaşılmıştır. Bu belgelerin hangi formatta olduklarını ve e-imza algoritmalarını tespit edebilen, İngiliz Milli Arşivinde kullanılan DROID ve Açık Koruma Vakfı tarafından geliştirilen JHOVE gibi yazılımlar hazırlanmalıdır.
4. Delil değeri sorgulamasında e-imza yanı sıra EYP ve oluşturulacak güvenilirlik üstverisi de kullanılabilir. EYP'de belgenin doğduğu işlem, faaliyet, fonksiyon ve birim üstverileri zorunlu olmalıdır.

5. TS 13298 Standardı'na güvenilirlik üstverisi eklenmelidir.

Belgelerin delil değerinin korunmasında uygulama yazılımlarının vazgeçilmez bir yeri olduğu bilinmektedir. Saha çalışmasında bu yazılımların kabiliyetlerinin, kurumların teknolojik koşullar düzeyindeki başarısını doğrudan etkilediği görülmüştür. Yazılımlara yönelik çeşitli öneriler şu şekildedir:

1. Kurumların genellikle paket programlar tercih ettikleri anlaşılmıştır. İlk işletildiği yerin fonksiyonlarına göre şekillendirilen bu programların, diğer kurumların faaliyetleri analiz edilmeden kullanıldığı görülmüştür. Bu yüzden örgütlerde belgenin işlem, faaliyet, iş, fonksiyon, seri ve birim ilişkisinin kurulmasında güçlük yaşanmaktadır. Aynı yazılım kullanılsa dahi fonksiyonlar gerçek senaryolar üzerinden tekrar yapılandırılmalıdır.
2. Yazılımların kaynak kodları, kamu kurumlarıyla paylaşılmalıdır. Telif hakkı ihlallerinden kaynaklanabilecek çekinceler nedeniyle bunun pek tercih edilmediği düşünülse de sözleşmelerde belirli bir süre sonunda kurumların erişimine açılacağı hüküm altına alınmalıdır.
3. Daha önce farklı akademik ve bilimsel çalışmaların ortaya koyduğu "bilgi sistemlerinde bilgi ve belge yönetimi uzmanı gereksinimi" bu tezde de açığa çıkmıştır. Belgelerin delil değeriyle alakalı arşivsel güvenilirlik analiz edilirken yazılım geliştiricilerin üzerinde fazlaca durmadıkları, süreç analizleri sırasında da yeteri kadar anlaşılmayan belge yönetimi ve arşiv disiplinine ait uygulamaların bilgi ve belge yönetimi profesyonelleri eliyle gerçekleştirilebileceği bir kez daha görülmüştür.

Her ne kadar bu tez, belli bir problematik üzerine odaklanmış hipotezi sınamak için yapılmış olsa da elde edilen bulgular, sahada farklı problemlerin bulunduğuna işaret etmiştir.

1. Kurumlardaki EBYS'lerde oluşan log kayıtları standart yapıda olmadığı için e-imzalı belgelerin delil değerinin analizinde yetersiz kalmaktadır. Farklı karinelerle desteklenmelidir.

2. Bilgi güvenliği sistemleri, bazı örgütlerde belge güvenilirliği sistemi olarak algılanmaktadır. Oysa bilgi güvenliği, daha çok sistemin risklerle alakalı açıklarını kritik etmekte; belgelerin özniteliklerinin ilk üretildiği gibi korunduğuyla ilgilenmemektedir. Hâliyle ya bilgi güvenliği sistemi yeniden yapılandırılmalı ya da arşivsel güvenilirlik yaklaşımı ayrıca ele alınmalıdır.
3. Uygulama yazılımlarında güvenilirliğin korunduğunu gösterecek bir algoritma geliştirilmelidir.
4. EYP'nin belgelerin delil değerinin sorgulanmasında bir mekanizma olarak nasıl kullanılabileceği incelenmelidir.
5. Kullanıcıların e-imzalı belgelere nasıl güven duyduğu ve benimsedikleri güvenilirlik araçları araştırılmalıdır.
6. E-imzalı belgelerin dışında dokümanlar, sosyal medya paylaşımları ve fotoğraflar gibi elektronik malzemelerin delil değeri, arşivsel güvenilirlik açısından analiz edilmelidir.
7. E-belgeler için teknolojik göç gereksinimleri belirlenmelidir.
8. Blokzincir, yapay zekâ ve derin öğrenme gibi teknolojik yöntemlerin e-belgelerin delil değerinin korunmasına katkıları örnek olaylar üzerinden incelenmelidir.
9. E-imzalı belgelerin güvenilirliğine yönelik standart geliştirilmelidir.
10. Avrupa'daki milli arşivlerin katılımıyla elektronik arşivlemedeki teknik ve yöntemleri geliştirmek için oluşturulan E-ARK Projesi'ne Türkiye de dâhil olmalı veya ülkede böyle bir proje başlatılmalıdır.

Arşivlenen e-imzalı belgelerin delil değerini korumak için arşiv malzemesi olmaları beklenmemelidir. Sürecin güncel dönemde, daha belge üretilmeden EBYS uygulama yazılımlarında planlanması gerektiği görülmüştür. Doğru dosya kodunun seçilmesi, ait olduğu dosyada bütünlük içerisinde tutulması, üstverilerinin eksiksiz girilmesi, bunlara ait log kayıtlarının korunması ve belge hiyerarşisinin muhafazasının bir belgede e-imzanın varlığı kadar önemli olduğu anlaşılmıştır. E-arşiv döneminde güvenilirlik karinesi olarak kullanılabilmesi için tüm bu delil değeri unsurlarının güncel dönemde düşünülmesi gerekmektedir. Bunu yapabilmek için kurumlar, arşivsel bağı kuracak üstverileri olması gerektiği gibi tanımlamalı, teknolojik koşulları doğru

sağlamalı ve tüm bunları tesis edecek kurumsal politika ve prosedürleri çıkarmalıdır. Aksi hâlde, bir bilgi sisteminde e-imzalı belgenin hukuki sonuca yönelecek bir işi gerçekleştirmesi ve işlemi sonuçlandırması, e-arşiv döneminde karşılaşılabilecek muhtemel olumsuzlukları ortadan kaldıramayacaktır. Çünkü e-imza, zaman damgası ve e-mühür gibi yapıların kırılganlıkları hâlâ giderilmiş değildir. Bundan dolayı, e-imzalı belgelerin delil değerini koruyabilmek için belirtilen kimlik tespiti araçları dışında organik bağ, diplomatik analiz ve üstveriler gibi farklı arşivsel güvenilirlik unsurları geliştirilmelidir. Türkiye dışındaki ülkelerde, tezin temas ettiği konularda çeşitli araştırmalar yapılsa da henüz e-imzalı belgelerin delil değerinin yapay ve derin öğrenme yöntemleriyle korunmasına yönelik yaklaşımların yeteri kadar tartışılmadığı gözlenmiştir. Tezin bu yöndeki yaklaşımları literatüre bir katkı olarak ifade edilebilir. Türkiye'de ise e-imzalı belgelerin delil değerinin sorgulanmasında zenginleştirilerek kullanılacak EYP ve KEP'ten yararlanılabilir. Aynı zamanda tezde oluşturulması önerilen arşivsel güvenilirlik üstverisi, belgelerin delil değeri analizinde kullanılabilir.

KAYNAKÇA

Mevzuat:

"Anayasa Mahkemesi Kararı": Karar No: 2011/3, Esas No: 2008/96, tar. 06.01.2011, **Resmî Gazete [R.G.]**, S 27934, tar. 14.05.2011, (Çevrimiçi) https:// www. resmi gazete. gov. tr/ eskiler/ 2011/ 05/ 20110514-6.htm, 19 Mayıs 2020.

"Annexe au décret n° 2011-573 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine (Décrets en Conseil d'Etat et en conseil des ministres) et au décret n° 2011-574 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine(livres Ier à VI)": **Journal Officiel de la Republique Française [JORF]**, 26 Mayıs 2011, (Çevrimiçi) https:// www. legifrance. gouv. fr/ affichTexte. do; jsessionid= B75F6F567F3B039148A0DF7317AEDCB.tplgfr 29s_2?cidTexte=JORFTEXT000024232917&date Texte=20110526, 14 Ekim 2018.

"Bağımsız Denetim Kanıtları": **R.G.**, S 30443 Mükerrer, tar. 06.06.2018, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2018/ 06/ 20180606M1-18.pdf, 11 Mart 2019.

"Bankacılık Kanunu": Kanun No: 5411, **R.G.**, S 25983 Mükerrer, tar. 01.11.2005, (Çevrimiçi) http:// www. mevzuat. gov. tr/ MevzuatMetin/1.5.5411.pdf, 18 Şubat 2019.

"Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik": **R.G.**, S 31069, tar. 15.03.2020, (Çevrimiçi) https :// www. resmigazete. gov. tr/ eskiler/ 2020/ 03/ 20200315-10.htm, 9 Nisan 2020.

"Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik": **R.G**., S 29057, tar. 11.07.2014, (Çevrimiçi) https :// www. resmigazete. gov. tr/ eskiler/ 2014/ 07/ 20140711-5.htm.

"Bankaların Muhasebe Uygulamalarına ve Belgelerin Saklanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik": **R.G.**, S 26333, tar. 01.11.2006, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2006/ 11/ 20061101.htm, 19 Şubat 2019.

"Belge Yöneticisi (Seviye 6) Ulusal Meslek Standardı": **R.G.**, S 31406 Mükerrer, tar. 21.02.2020, (Çevrimiçi) https :// www. resmigazete. gov. tr/ eskiler/ 2020/ 02/ 20200221M1-2-1.pdf, 6 Ağustos 2020.

"Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ": **R.G.**, S 28841, tar. 04.12.2013, (Çevrimiçi) http :// www. resmigazete. gov. tr/ eskiler/ 2013/ 12/ 20131204.htm, 18 Şubat 2019.

"Bilgi Edinme Hakkı Kanunu": Kanun No: 4982, **R.G.**, S 25269, tar. 24.10.2003, (Çevrimiçi) http:// www. mevzuat. gov. tr/ MevzuatMetin/1.5.4982.pdf, 1 Mayıs 2018.

Bilgi Teknolojileri Kurumu [BTK]: **Elektronik İmza Kullanım Profilleri Rehberi**, (Çevrimiçi) https :// www. btk. gov. tr/ uploads/ pages/ elektronik- imza- kullanim-profilleri-rehberi-5a33ff5b59f93.pdf, 5 Nisan 2020.

BTK: **Kayıtlı Elektronik Posta Hizmet Sağlayıcılarının Birlikte Çalışabilirliğine İlişkin Usul ve Esaslar**, 2014, (Çevrimiçi) https:// www. btk. gov. tr/ uploads/ pages/ kephsbirliktecalisabilirlikusulesas-5a3406e891d77.pdf, 10 Mart 2019.

BTK: **Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar**, 2019, (Çevrimiçi) https :// www. btk. gov. tr/ uploads/ boarddecisions/ kurumsal-sifreleme-ve-elektronik-muhur-sertifikalarina-iliskin-usul-ve-esaslar/ 160-2019-web.pdf, 11 Mayıs 2020.

"Bölge Adliye ve Adlî Yargı İlk Derece Mahkemeleri ile Cumhuriyet Başsavcılıkları İdarî ve Yazı İşleri Hizmetlerinin Yürütülmesine dair Yönetmelik": **R.G.**, S 29437, tar. 06.08.2015, (Çevrimiçi) https :// www. resmigazete. gov. tr/ eskiler/ 2015/ 08/ 20150806-3.htm, 28 Nisan 2018.

"Canada Evidence Act": **Revised Statutes of Canada**, Chapter 5, 1985, (Çevrimiçi) http:// laws-lois. justice. gc. ca/ eng/ acts/C-5/, 20 Mayıs 2018.

"Ceza Muhakemesi Kanunu" [CMK]:	Kanun No: 5271, **R.G.**, S 25673, tar. 17.12.2004, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2004/ 12/ 20041217.htm#1, 28 Nisan 2018.
"Code of Federal Regulations, Title 36, Chapter XII, Subchapter B Records Management":	**Government Publishing Office [GPO]**, (Çevrimiçi) https:// www. gpo. gov/ fdsys/ pkg/ CFR-2017-title36-vol3/ pdf/ CFR-2017-title36-vol3-chapXII-subchapB.pdf, 24 Mayıs 2018.
"Code of United States, Title 44, Chapter 21, National Archives and Records Administration":	**GPO**, (Çevrimiçi) https:// www. gpo. gov/ fdsys/ pkg/ USCODE-2016-title44/ pdf/ USCODE-2016-title44-chap21.pdf, 26 Mayıs 2018.
"Code of United States, Title 44, Chapter 31, Records Management by Federal Agencies":	**GPO**, (Çevrimiçi) https:// www. gpo. gov/ fdsys/ pkg/ USCODE-2016-title44/pdf/USCODE-2016-title44-chap31.pdf, 24 Mayıs 2018.
"Commission Decision of 29 November 2001 amending its Internal Rules of Procedure":	**Official Journal [OJ]**, L 317/3, 29.11.2001, (Çevrimiçi) https :// publications.europa.eu/s/lhdE, 25 Nisan 2019.
"Commission Decision of 23 January 2002 amending its Rules of Procedure":	**OJ**, L 21/23, 23.01.2002, (Çevrimiçi) https :// eur-lex. europa. eu/ legal-content/ GA/ TXT/ ?uri= CELEX: 32002D0047, 25 Nisan 2019.
"Commission Decision of 7 July 2004 amending its Rules of Procedure":	**OJ**, L 251/9**,** 07.07.2004, (Çevrimiçi) https :// publications. europa. eu/ s/ lhdF, 25 Nisan 2019.
"Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi":	Kararname Numarası: 1, **R.G.**, S 30474, tar. 10.07.2018 (Çevrimiçi), https:// www. resmigazete. gov. tr/ eskiler/ 2018/ 07/20180710-1.pdf, 6 Kasım 2020.
"Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi":	Kararname Numarası: 15, **R.G.**, S 30499, tar. 04.08.2018 (Çevrimiçi), https:// www. resmigazete. gov. tr/ eskiler/ 2018/ 08/ 20180804-1.pdf, 6 Kasım 2020.
"Damga Vergisi Kanunu":	Kanun No: 488, **R.G.**, S 11751, tar. 11.07.1964, (Çevrimiçi) http:// www. mevzuat. gov. tr/ MevzuatMetin/ 1. 5. 488. pdf, 2 Mayıs 2018.

“Décret n° 2017-719 du 2 mai 2017 relatif aux services publics d'archives, aux conditions de mutualisation des archives numériques et aux conventions de dépôt d'archives communales”:	**JORF**, 4 Mayıs 2017, (Çevrimiçi) https :// www. legifrance. gouv. fr/ affichTexte. do; jsessionid= 0B75F6F567F3B039148A0DF7317AEDCB.tplgfr29s_2?cidTexte=JORFTEXT000034567704&dateTexte=20170504, 14 Ekim 2018.
“Devlet Arşiv Hizmetleri Hakkında Yönetmelik”:	**R.G.**, S 30922, tar. 18.10.2019, (Çevrimiçi) https :// www. resmigazete. gov. tr/ eskiler/ 2019/ 10/ 20191018-9. pdf, 22 Mayıs 2020.
“Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repailing Directive”:	**OJ**, L 257/73, tar. 28.08.2014, (Çevrimiçi) https: //eur-lex. europa. eu/ legal-content/ EN/ TXT/ PDF/ ?uri= CELEX: 3201 4R0910&from=EN, 15 Mart 2020.
“Elektronik Haberleşme Kanunu”:	Kanun No: 5809, **R.G.**, S 27050 Mükerrer, tar. 10.11.2008, (Çevrimiçi) https :// www. mevzuat. gov. tr/ MevzuatMetin/ 1. 5. 5809.pdf, 22 Şubat 2020.
“Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği”:	**R.G.**, S 29059, tar. 13.07.2014, (Çevrimiçi) https :// www. resmigazete. gov. tr/ eskiler/ 2014/ 07/ 20140713-4.htm, 22 Şubat 2020.
“Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliğ”:	**R.G.**, S 25692, tar. 06.01.2005, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2005/ 01/ 20050106-19.htm, 5 Nisan 2020.
“Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliğ”:	**R.G.**, S 30123, tar. 13.07.2017, (Çevrimiçi) https:// www.resmigazete.gov.tr/eskiler/2017/07/20170713-9.htm, 5 Nisan 2020.
“Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliğ”:	**R.G.**, S 31078, tar. 24.03.2020, (Çevrimiçi) https:// www.resmigazete.gov.tr/eskiler/2020/03/20200324-7.htm, 5 Nisan 2020.
“Elektronik İmza Kanunu”:	Kanun No: 5070, **R.G.**, S 25355, tar. 23.01.2004, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2004/ 01/ 20040123.htm, 4 Aralık 2020.

"Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik":	**R.G.**, S 25692, tar. 06.01.2005, (Çevrimiçi) www. resmigazete. gov. tr/ eskiler/ 2005/ 01/ 20050106. htm, 22 Mayıs 2018.
"Elektronik Tebligat Yönetmeliği":	**R.G.**, 30617, tar. 06.12.2018, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2018/ 12/ 20181206-2.htm, 10 Mart 2019.
"Emeklilik Fayda Planlarında Muhasebeleştirme ve Raporlama":	**R.G.**, S 26095, tar. 01.03.2006, (Çevrimiçi) http :// www. resmigazete. gov. tr/ eskiler/ 2006/ 03/ 20060301-20.htm, 11 Mart 2019.
"Federal Rules of Evidence":	**GPO** (Çevrimiçi) https:// www. uscourts. gov/ sites/ default/ files/ evidence-rules-procedure-dec2017_0.pdf, 23 Mayıs 2019.
"Finansal Raporlamaya İlişkin Kavramsal Çerçeve":	**R.G.**, S 30578, tar. 27.10.2018, (Çevrimiçi) http :// www. resmigazete. gov. tr/ eskiler/ 2018/ 10/ 20181027-16. pdf, 11 Mart 2019.
"Finansal Tabloların Sunuluşu":	**R.G.**, S 30430, tar. 24.05.2018, (Çevrimiçi) http:// www.resmigazete.gov.tr/eskiler/2018/05/20180524-14.pdf, 11 Mart 2019.
Gelir İdaresi Başkanlığı [GİB]:	**E-Bilet Raporu Teknik Kılavuzu (Etkinlik)**, Ankara, 2020, (Çevrimiçi) https:// ebelge. gib. gov. tr/ dosyalar/ ebilet/ e-Bilet_ Raporu_ Teknik_ Kilavuzu(Etkinlik).pdf, 7 Ocak 2021.
GİB:	**E-Bilet Raporu Teknik Kılavuzu (Havayolu)**, Ankara, 2020, (Çevrimiçi) https :// ebelge . gib. gov. tr/ dosyalar/ ebilet/ e-Bilet_ Raporu_ Teknik_ Kilavuzu (Havayolu). pdf, 7 Ocak 2021.
GİB:	**E-Defter Uygulama Kılavuzu V. 1.8**, Ankara, 2021, (Çevrimiçi) http :// www. edefter. gov. tr/ dosyalar/ kilavuzlar/ e-DefterUygulamaKilavuzu_ (V_ 1.8)_ 21. 05.2021.pdf, 7 Ocak 2021.
GİB:	**E-Defter Uygulaması Yazılım Uyumluluk Onayı Versiyon 1.8**, Ankara, 2021, (Çevrimiçi) http :// edefter. gov. tr/ dosyalar/ kilavuzlar/ e-Defter Uygulama Kilavuzu_ (V_1.8)_ 21.05.2021.pdf, 15 Temmuz 2021.

GİB: **E-Fatura Portalı Kullanım Kılavuzu**, Ankara, 2013, (Çevrimiçi) http :// ebelge. gib. gov. tr/ dosyalar/ kilavuzlar/ e-Fatura Portali Kullanim Kilavuzu-v 1. 5. pdf, 10 Mart 2019.

GİB: **E-Fatura Uygulaması Entegrasyon Kılavuzu**, Ankara, 2018, (Çevrimiçi) http :// ebelge. gib. gov. tr/ dosyalar/ kilavuzlar/ e-FaturaUygulamasi EntegrasyonKilavuzu-v1.10.pdf, 10.03.2018.

GİB: **E-Fatura Uygulaması Sistem Yanıtı Şema Yapısı**, Ankara, 2017, (Çevrimiçi) http :// ebelge. gib. gov. tr/ dosyalar/ kilavuzlar/ Ek-2 e- Fatura Uygulamasi SistemYanitiSemaYapisi-v1.5.pdf, 10 Mart 2019.

GİB: **E-Fatura Uygulaması Test Planı**, Ankara, 2017, (Çevrimiçi) http:/ ebelge. gib. gov. tr/dosyalar/kilavuzlar/e-FaturaTestPlani.pdf, 10 Mart 2019.

GİB: **Elektronik Arşiv Kılavuzu**, Ankara, 2021, (Çevrimiçi) https :// ebelge. gib. gov. tr/ dosyalar/ kilavuzlar/ e-Arsiv_Teknik_Kilavuzu_V.1.12.pdf, 3 Ağustos 2021.

GİB: **Elektronik Arşiv Başvuru Kılavuzu**, Ankara, 2021, (Çevrimiçi) https :// ebelge. gib. gov. tr/ dosyalar/ kilavuzlar/ e-ArsivBasvuruKilavuzu. 1. 5. Versiyon. pdf, 3 Ağustos 2021.

GİB: **Elektronik Yolcu Listesi Raporu**, Ankara, 2020, (Çevrimiçi) https :// ebelge. gib. gov. tr/ dosyalar/ ebilet/ e-Yolcu_ Listesi_ Raporu_ Teknik_ Kilavuzu. pdf, 7 Ocak 2021.

"Hukuk Muhakemeleri Kanunu [HMK]": Kanun No: 6100, **R.G.**, S 28736, tar. 04.02.2011, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2011/ 02/ 20110204-2.htm, 27 Nisan 2018.

İstanbul Üniversitesi Sosyal Bilimler Enstitüsü: **Tez Hazırlama Yönergesi**, İstanbul, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, tarih yok, (Çevrimiçi) https:// cdn. istanbul. edu. tr/ FileHandler2.ashx?f=tez.hazirlama.yonergesi.pdf, 4 Ekim 2020.

“Kamu Malî Yönetimi ve Kontrol Kanunu [KMYKK]”:	Kanun No: 5018, **R.G.**, S 25326, tar. 24.12.2003, (Çevrimiçi) https :// www. resmigazete. gov. tr/ eskiler/ 2003/12/20031224.htm#1, 19 Mayıs 2020.
“Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ”:	**R.G.**, S 28036, tar. 25.08.2011, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2011/ 08/ 20110825-21.htm, 10 Mart 2019.
“Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik”:	**R.G.**, S 28036, tar. 25.08.2011, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2011/ 08/ 20110825-7.htm, 10 Mart 2019.
“Model Law on Electronic Commerce”:	**United Nations Commission on International Trade Law [UNCITRAL]**, 1996, (Çevrimiçi) https:// www. uncitral. org/ pdf/ english/ texts/ electcom/05-89450_Ebook.pdf, 24 Mayıs 2018.
“Model Law on Electronic Signatures”:	**UNCITRAL**, 2001, (Çevrimiçi) https :// www. uncitral. org/ pdf/ english/ texts/ electcom/ ml-elecsig-e.pdf, 24 Mayıs 2018.
“Muhasebe Politikaları, Muhasebe Tahminlerinde Değişiklikler ve Hatalar”:	**R.G.**, S 30450, tar. 13.06.2018, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2018/ 06/ 20180613-14.pdf, 11 Mart 2019.
“National Conference of Commissioners on Uniform State Laws”:	**Uniform Electronic Legal Material Act**, 2011, (Çevrimiçi) http:// www. uniformlaws. org/ shared/ docs/ electronic %20 legal %20 material/ uelma_final_2011.pdf, 14 Ekim 2018.
North Carolina State Crime Laboratory:	“Procedure for Record and Data Management”, North Carolina[ABD], 2013, (Çevrimiçi) http:// www. ncids. com/ forensic/ labs/ Lab/ Policy/ Record-and-Data-Management-10-31-2013.pdf, 6 Aralık 2019.
“Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik”:	**R.G.**, S 29413, tar. 11.07.2015, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2015/ 07/ 20150711-19.htm, 10 Mart 2019.
“Noterlik Kanunu”:	Kanun No: 15152, **R.G.**, S. 14090, tar. 05.02.1972, (Çevrimiçi) http:// www. mevzuat. gov. tr/ MevzuatMetin/1.5.1512.pdf, 10 Mart 2019.

"Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmelik":	**R.G.**, S 29043, tar. 27.06.2014, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2014/ 06/ 20140627.htm, 18 Şubat 2019.
"Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun":	**R.G.**, S 28690, tar. 27.06.2013, (Çevrimiçi) http:// www. mevzuat. gov. tr/ MevzuatMetin/ 1. 5. 6493. pdf, 18 Şubat 2019.
"Ödeme ve Menkul Kıymet Mutabakat Sistemlerinde Kullanılan Bilgi Sistemleri Hakkında Tebliğ":	**R.G.**, S 29588, tar. 09.01.2016, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2016/ 01/ 20160109.htm, 18 Şubat 2019.
"Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik":	**R.G.**, S 31151, tar. 10.06.2020, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2020/ 06/ 20200610-8.pdf, 5 Aralık 2020.
"Sigortacılık Bağımsız Denetim İlkelerine İlişkin Yönetmelik":	**R.G.**, S 26934, tar. 12.07.2008, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2008/ 07/ 20080712-7.htm, 23 Şubat 2020.
"Sigortacılık Kanunu":	Kanun No: 5684, **R.G.**, S 26552, tar. 14.06.2007, (Çevrimiçi) https:// www. mevzuat. gov. tr/ MevzuatMetin/ 1.5.5684.pdf, 23 Şubat 2020.
"Türk Borçlar Kanunu":	Kanun No: 6098, **R.G.**, S 27836, tar. 04.02.2011, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2011/ 02/ 20110204-1.htm, 23 Mayıs 2019.
"Türk Ceza Kanunu":	Kanun No: 5237, **R.G.**, S 25611, tar. 12.10.2004, (Çevrimiçi) http:// www. mevzuat. gov. tr/ MevzuatMetin/ 1.5.5237.pdf, 1 Mayıs 2018.
Türk Medeni Kanunu":	Kanun No: 4721, **R.G.**, S 24607, tar. 08.12.2001, (Çevrimiçi) https:// www. mevzuat. gov. tr/ MevzuatMetin/ 1.5.4721.pdf, 23 Mayıs 2019.
"Türk Ticaret Kanunu":	Kanun No: 6102, **R.G.**, S 27846, tar. 14.02.2011, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2011/ 02/ 20110214.htm, 11 Aralık 2018.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu [TÜBİTAK] Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi [BİLGEM] Kamu Sertifikasyon Merkezi [KAMU SM]: **Elektronik Belgeleri Açık Anahtar Altyapısı Kullanarak Güvenli İşleme Rehberi**, Sürüm 1.4, 2015, (Çevrimiçi) http:// kamusm. bilgem. tubitak. gov. tr/ dosyalar/ rehberler/ REHB-001. 001_ 1.4.pdf, 23 Eylül 2020.

KAMU SM: **Zaman Damgası Uygulama Esasları**, 2020, (Çevrimiçi) https:// kam usm. bilgem. tubitak. gov. tr/BilgiDeposu/KSM_ZDUE/YON.01.02_02_KAMU_SM_ZAMAN_DAMGASI_UYGULAMA_ESASLARI.pdf, 11 Mayıs 2020.

Türkiye Büyük Millet Meclisi [TBMM]: **HMK Gerekçesi**, 2008, (Çevrimiçi) https:// www. tbmm. gov. tr/ sirasayi/ donem23/ yil01/ ss393.pdf, 1 Mayıs 2018.

TBMM: **Türk Ceza Kanunu Gerekçesi**, 2003, (Çevrimiçi) http:// www2. tbmm. gov. tr/ d22/1/1-0593.pdf, 1 Mayıs 2018.

Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO): **E-Yazışma Projesi**, (Çevrimiçi) https :// cbddo. gov. tr/ projeler/ e-yazisma, 30 Ağustos 2020.

CBDDO: **e-Yazışma Teknik Rehberi**, Ankara, Sürüm 2.0., 2020, (Çevrimiçi) https :// cbddo. gov. tr/ SharedFolderServer/ Projeler/ File/ EYP_2.0/ EYP2.0_teknik-rehberi.pdf, 30 Ağustos 2020.

Türkiye Cumhuriyeti Cumhurbaşkanlığı İdari İşler Başkanlığı Destek ve Mali Hizmetler Genel Müdürlüğü Bilgi ve Belge Yönetimi Daire Başkanlığı: **Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik Kılavuzu**, 2020, (Çevrimiçi) https:// www. tccb. gov. tr/ assets/ dosya/ resmiyazisma/ dosyalar/ kilavuz.pdf, 20 Mayıs 2021.

Türkiye Cumhuriyeti Kalkınma Bakanlığı Bilgi Toplumu Dairesi: **e-Dönüşüm Türkiye Projesi: Birlikte Çalışabilirlik Esasları Rehberi**, Sürüm 2.1., 2012, (Çevrimiçi) http :// www. bilgitoplumu. gov. tr/ wp-content/ uploads/ 2014/ 04/ Birlikte_Calisabilirlik_Esaslari_Rehberi_2.1.pdf, 26 Temmuz 2019.

"Vergi Usul Kanunu [VUK]":	Kanun No: 213, **R.G.**, S 10703-10705, tar. 10.01.1961-12.01.1961, (Çevrimiçi) http: // www. mevzuat. gov. tr / Mevzuat Metin / 1. 4. 213.pdf, 11 Aralık 2018.
"Yargıtay Ceza Genel Kurulu Kararı":	Esas No: 1993/10, Karar No: 1993/6-79.
"Yargıtay Ceza Genel Kurulu Kararı":	Esas No: 2016/1065, Karar No: 2017/27.
"Yargıtay 9. Ceza Dairesi Kararı":	Esas No: 2013/9110, Karar No: 2013/12351.
"1 Sıra No'lu Elektronik Defter Tebliği":	**R.G.**, S 28141, tar. 13.12.2011, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2011/ 12/ 20111213.htm, 10 Mart 2019.
"3 Sıra No'lu Elektronik Defter Tebliği":	**R.G.**, S 30923, tar. 19.10.2019, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2019/ 10/ 20191019-4.htm, 7 Ocak 2021.
"2004/21 sayılı Başbakanlık Genelgesi":	"2004/21 sayılı Başbakanlık Genelgesi", **R.G.**, S. 25575, tar. 06.09.2004, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2004/ 09/ 20040906. htm#8, 15 Mart 2020.
"2006/13 sayılı Başbakanlık Genelgesi":	**R.G.**, S. 26144, tar. 19.04.2006, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2006/ 04/ 20060419-5.htm, 15 Mart 2020.
"2008/16 sayılı Başbakanlık Genelgesi":	**R.G.**, S. 26938, tar. 16.07.2008, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2008/ 07/ 20080716-7.htm, 8 Haziran 2020.
"2017/21 sayılı Başbakanlık Genelgesi":	**R.G.**, S 30210, tar. 14.10.2017, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2017/ 10/ 20171014-11.pdf, 20 Ağustos 2020.
"446 Sıra No'lu VUK Genel Tebliği":	**R.G.**, S 29316, tar. 04.04.2015, (Çevrimiçi) http:// www. resmigazete. gov. tr/ eskiler/ 2015/ 04/ 20150404.htm, 10 Mart 2019.
"509 Sıra No'lu VUK Genel Tebliği":	**R.G.**, S 30923, tar. 19.10.2019, (Çevrimiçi) https:// www. resmigazete. gov. tr/ eskiler/ 2019/ 10/ 20191019-5.pdf, 5 Nisan 2020.

Standartlar:

British Standart Institute [BSI]: **10008: Evidential Weight and Legal Admissibility of Electronic Information**, Londra[Birleşik Krallık], BSI, 2020.

Canadian General Standards Board [CGSB]: **National Standart of Canada: Electronic Records as Documentary Evidence**, Gatineau[Kanada], CGSB, 2017.

European Telecommunications Standard Institute [ETSI]: **Technical Specification [TS] 119 312: Electronic Signatures and Infrastructures: Cryptographic Suites**, 2017, (Çevrimiçi), https:// www. etsi. org/ deliver/ etsi_ts/ 119300_ 119399/ 119312/ 01.02.01_60/ ts_119312v010201p.pdf, 29 Şubat 2020.

International Organization of Standardization [ISO]: **Assessment of Machine Learning Classification Performance**, Cenevre[İsviçre], ISO. y.y.

ISO: **Blockchain and Distributed Ledger Technologies**, Cenevre[İsviçre], ISO, 2016.

ISO: **10244 Business Process Baseling and Analysis**, Cenevre[İsviçre], ISO, 2010.

ISO: **10789 Information and Documentation Management**, Cenevre[İsviçre], ISO, 2011.

ISO: **11506 Archiving of Electronic Data: Computer Output Microform (COM)/Computer Output Laser Disc (COLD)**, Cenevre[İsviçre], ISO, 2017.

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

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

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

ISO: **14721 Open Archival Information System (OAIS)**, Cenevre[İsviçre], ISO, 2012.

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

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

ISO: **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, 2020.

ISO: **16175-2 Processes and Functional equirements for Software for Managing Records Part 2: Guidance for Selecting, Designing, Implementing and Maintaining Software for Managing Records**, Cenevre[İsviçre], ISO, 2020.

ISO: **17068 Trusted Third Party Repository for Digital Records**, Cenevre[İsviçre], ISO, 2017.

ISO: **18128 Risk Assessment for Records Processes and Systems**, Cenevre[İsviçre], ISO, 2014.

ISO: **18492 Long-term Preservation of Electronic Document-based Information**, Cenevre[İsviçre], ISO, 2005.

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

ISO: **21043-2 Recognition, Recording, Collecting, Transport and Storage of Items**, Cenevre [İsviçre], ISO, 2018.

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

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

ISO: **23081-2 Managing Metadata for Records Part 2: Conceptual and Implemantation Issues**, Cenevre[İsviçre], ISO, 2009.

ISO: **24028 Overview of Trustworthiness in Artificial Intelligence**, Cenevre[İsviçre], ISO, 2020.

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

ISO: **27001 Information Security Management Systems: Requirements**, Cenevre[İsviçre], ISO, 2013.

ISO: **27003 Information Security Management Systems: Guidance**, Cenevre[İsviçre], ISO, 2017.

ISO: **27035-2 Information Security Incident Management Part 2: Guidelines to Plan and Prepare for Incident Response**, Cenevre[İsviçre], ISO, 2016.

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

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

ISO: **27042 Guidelines for the Analysis and Interpretation of Digital Evidence**, Cenevre [İsviçre], ISO, 2016.

ISO: **27043 Incident Investigation Principles and Process**, Cenevre[İsviçre], ISO, 2015.

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

ISO: **27050-2**: **Electronic Discovery, Part 2: Guidance for Governance and Management of Electronic Discovery**, Cenevre[İsviçre], ISO, 2018.

ISO: **30121 Governance of Digital Forensic Risk Framework**, Cenevre[İsviçre], ISO, 2015.

ISO: **30301 Management Systems for Records: Requirements**, Cenevre[İsviçre], ISO, 2019.

Türk Standartları Enstitüsü [TSE]: **13298 Elektronik Belge Yönetim Sistemi Standardı**, Ankara, TSE, 2015.

TSE: **9001 Kalite Yönetim Sistemi Standardı - Şartlar**, Ankara, TSE, 2015.

Sözlükler:

Arşivcilik Terimleri Sözlüğü: Almanca, İngilizce, Fransızca, İtalyanca, Hollandaca, Rusça ve İspanyolca Karşılıklarıyla: Türkçe hazırlayan ve genişleten: Bekir Kemal Ataman, İstanbul, Librairie de Pera Yayınları, 1995.

Türkiye Bilimler Akademisi [TÜBA]: **Türkçe Bilim Terimleri Sözlüğü**, (Çevrimiçi) www.tubaterim.gov.tr, 6 Haziran 2020.

Kitaplar:

Acar, Ayşe Ece: **Medeni Muhakeme Hukukunda Elektronik İmzalı Belgelerin Delil Niteliği**, İstanbul, On İki Levha Yayıncılık, 2012.

Alpaydın, Ethem: **Yapay Öğrenme**, 4. bs., İstanbul, Boğaziçi Üniversitesi Yayınevi, 2018.

Atalı, Murat, Ermenek, İbrahim ve Üçüncü, Hilal: **Tebligat Hukuku**, 3. bs., Ankara, Seçkin Yayınları, 2020.

Ber, Ahmet Said: **Elektronik Konişmento**, Ankara, Seçkin Yayınları, 2018.

Berryhill, Jamie, Bourgery, Theo ve Hanson, Angela: **Blockchains Unchained: Blockchain Technology and its Use in the Public Sector**, (Çevrimiçi) https :// www. oecd- ilibrary. org/ governance/ blockchains-unchained_3c32c429-en, 30 Mart 2020.

Birleşmiş Milletler: **The Future is Decentralised**, (Çevrimiçi) https :// www. undp. org/ content/ undp/ en/ home/ librarypage/ corporate/ the-future-is-decentralised. html, 30 Mart 2020.

Boudrez, Filip vd.: **Digital Archiving: The New Challenge?**, IRIS, Belçika, 2005.

Cansel, Erol ve Özel, Çağlar: **Borçlar Hukuku Genel Hükümler Cilt: 1**, 2. bs., Ankara, Seçkin Yayıncılık, 2017.

Centel, Nur: **Ceza Muhakemesi Hukuku**, 9. bs., İstanbul, Beta Basım Yayınları, 2012.

Christian, Brian ve Griffiths, Tom: **Hayatımızdaki Algoritmalar: Günlük Kararların Bilgisayar Bilimi**, çev.: Ali Atav, 3. bs., Ankara, Buzdağı Yayınevi, 2018.

Çetin, Süleyman ve Ateş, Derya: **Avukatlık ve Noterlik Hukuku**, 2. bs., Ankara, Seçkin Yayıncılık, 2019.

Çiçek, Niyazi: **Kurumsal Bilgi ve Belge Yönetimi**, İstanbul, Marmara Belediyeler Birliği, 2018.

Çiçek, Niyazi: **Modern Belgelerin Diplomatiği**, İstanbul, Derlem Yayınları, 2009.

Creswell, John W.: **Araştırma Deseni: Nitel, Nicel ve Karma Yöntem Yaklaşımları**, çev.: Selçuk Beşir Demir vd., 3. bs., Ankara, Eğiten Kitap, 2017.

Creswell, John W.: **Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research**, 4. bs., Boston[ABD], Pearson, 2012.

Creswell, John W.: **Karma Yöntem Araştırmalarına Giriş**, çev.: Mustafa Sözbilir vd., Ankara, Pegem Akademi Yayınları, 2017.

Creswell, John W.: **Nitel Araştırma Yöntemleri: Beş Yaklaşıma göre Nitel Araştırma ve Araştırma Deseni**, çev.: Mesut Bütün vd., 3. bs., Ankara, Siyasal Kitabevi, 2016.

Creswell, John W. ve Clark, Vicki L. Piano: **Karma Yöntemler Araştırmaları: Tasarımı ve Yürütülmesi**, çev.: Yüksel Dede vd., 3. bs., Ankara, Anı Yayıncılık, 2018.

Doğan, Murat, Şahan, Gökhan ve Atamulu, İsmail: **Borçlar Hukuku Genel Hükümler Ders Kitabı**, Ankara, Seçkin Yayıncılık, 2019.

Doğrusöz, Bumin, Onat, Öznur ve Toralp, Funda Tunçel: **Gerekçe, Karşılaştırmalı Maddeler, Komisyon Raporları, Önergeler ve Karşılaştırmalı Tabloları ile Türk Ticaret Kanunu (Ticari İşletme, Ticaret Şirketleri Kıymetli Evrak Hükümleri): Cilt: I (Madde 1-849)**, Ankara, Türkiye Odalar ve Borsalar Birliği, 2011.

Domingos, Pedro: **Master Algoritma: Yapay Öğrenme Hayatımızı Nasıl Değiştirecek?**, çev.: Tufan Göbekçin, 3. bs., İstanbul, Paloma Yayınları, 2019.

Ergün, Ömer ve Çaldağ, Coşkun: **Borçlar Hukuku Genel Hükümler Ders Notları**, Ankara, Seçkin Yayınları, 2019.

Exterro: **The State of E-Discovery 2018**, yayım yeri yok, yayımcı yok, 2018.

Fukuyama, Francis: **Güven: Sosyal Erdemler ve Refahın Yaratılması**, çev.: Ahmet Buğdaycı, 3. bs., İstanbul, İş Bankası Yayınları, 2005.

Goodfellow, Ian vd.: **Derin Öğrenme**, çev.: Fatoş Yarman Vural vd., Ankara, Buzdağı Yayınevi, 2018.

Gökcen, Ahmet: **Belgede Sahtecilik Suçları (m. 204-212)**, 5. bs., Ankara, Adalet Yayınevi, 2018.

Göksoy, Resul: **Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması**, Ankara, Seçkin Yayınevi, 2019.

Güler, Ceyhan: **Elektronik Belgelerin İmhası: Teori ve Uygulama,** İstanbul, Hiperlink Yayınları, 2020.

Günay, Barış: **Sigorta Hukuku**, Ankara, Seçkin Yayıncılık, 2019.

Gündoğdu, Aysel: **Bankacılık Hukuku**, 6. bs., Ankara, Seçkin Yayıncılık, 2019.

Harvey, Ross ve Weatherburn, Jaye: **Preserving Digital Materials**, 3. bs., Londra[Birleşik Krallık], Rowman & Littlefield, 2018.

Henkoğlu, Türkay: **Adli Bilişim: Dijital Delillerin Elde Edilmesi ve Analizi**, İstanbul, Pusula Yayınları, 2014.

Jenkinson, Hilary: **A Manual of Archive Administration**, Londra[Birleşik Krallık], Percy Lund, Humphries & Co Ltd., 1937.

John, Jeremy Leighton: **Digital Forensics and Preservation**, Birleşik Krallık, Digital Preservation Coalition [DPC], 2012.

Kayar, İsmail: **6102 Sayılı Türk Ticaret Kanunu'na göre Ticaret Hukuku**, 5. bs., Ankara, Seçkin Yayıncılık, 2018.

Kelleher, John D. **Deep Learning**, yayım yeri yok, MIT Press, 2019.

Kirschenbaum, Matthew G. vd.: **Digital Forensics and Born-Digital Content in Cultural Heritage Collections**, Washington[Amerika Birleşik Devletleri - ABD], Council on Library and Information Resources, 2010.

Lee, Christopher vd.: **From Bitstreams to Heritage: Putting Digital Forensics into Practice in Collecting Institutions**, yayım yeri yok, BitCurator, 2013.

MacNeil, Heather: **Trusting Records: Legal, Historical and Diplomatic Perspectives**, yayım yeri yok, Springer, 2000.

Millar, Laura: **Archives, Principles and Practices**, 2. bs., Londra [Birleşik Krallık], Facet Publishing, 2017.

Millar, Laura: **A Matter of Facts: The Value of Evidence in an Information Age**, Chicago[ABD], American Library Association, 2019.

National Archives and Records Administration [NARA]: **Blockchain White Paper**, Washington[ABD], NARA, 2019.

Ngoepe, Mpho ve Mukwevho, Jonathan: **Ensuring Authenticity and Reliability of Digital Records to Support the Audit Process**, yayım yeri yok, yayımcı yok, 2018.

Nilsson, Nils J.: **Yapay Zekâ**, çev.: Mehmet Doğan, 2. bs., İstanbul, Boğaziçi Üniversitesi Yayınevi, 2019.

Organisation for Economic Co-operation and Development [OECD]: **Government at a Glance**, Paris[Fransa], OECD, 2013, (Çevrimiçi) https :// doi. org/ 10. 1787/ gov_glance-2013-en, 20 Mayıs 2020.

OECD: **Blockchain and Beyond: Encoding 21st Century Transport**, OECD, International Transport Forum, 2018.

Öner, Erdoğan: **Vergi Hukuku**, 11. bs., Ankara, Seçkin Yayıncılık, 2019.

Pekcanıtez, Hakan vd.: **Hukuk Muhakemeleri Kanunu Hükümlerine Göre Medeni Usul Hukuku**, 11. bs., Ankara, Yetkin Yayınları, 2011.

Policies for Recordkeeping and Digital Preservation: Recommendations for Analysis and Assesment Services: ed.: Stefano Allegrezza vd., yayım yeri yok, yayımcı yok, 2016.

Schellenberg, T. R.: **Arşiv İdaresi**, çev.: Necla İlemin, T.C. Başbakanlık Devlet Arşivleri Genel Müdürlüğü, Cumhuriyet Arşivi Daire Başkanlığı, Ankara, 1993.

Türk Sanayicileri ve İşadamları Derneği [TÜSİAD]: **Kamu Hizmetinde Etik: Güncel Konular ve Uygulamalar**, İstanbul, Lebib Yalkım Yayınları, 2003.

Usta, Ahmet ve Doğantekin, Serkan: **Blockchain 101**, 2. bs., İstanbul, Bankalararası Kart Merkezi, 2018.

Upward, Frank vd.: **Recordkeeping Informatics for a Networked Age**, Victoria[Avustralya], Monash University Publishing, 2018.

Weinberger, David: **Everything is Miscellaneous: The Power of the New Digital Disorder**, New York[ABD], Holt Paperbacks, 2008.

Yavaş, Murat: **Senetle İspat ve Senede Karşı İspat Kuralları ile Bu Kuralların İstisnaları**, Ankara, Seçkin Yayıncılık, 2009.

Yeo, Geoffrey: **Records, Information and Data: Exploring the Role of Record-keeping in an Information Culture**, Londra [Birleşik Krallık], Facet Publishing, 2018.

Yıldırım, Ali ve Şimşek, Hasan: **Sosyal Bilimlerde Nitel Araştırma Yöntemleri**, 10. bs., Ankara, Seçkin Yayınları, 2018.

Yin, Robert K.: **Case Study Research: Design and Methods**, 4. bs., California[ABD], SAGE Publications, 2009.

Zafer, Hamide ve Centel, Nur: **Ceza Muhakemesi Hukuku**, 9. bs., İstanbul, Beta Basım Yayım, 2012.

Makaleler:

Abichandani, Payal ve Prakash, Rishi: "Digital Preservation of Court's Disposed Case Records - A Case Study from Indian Judicial System's Perspective", **APA/C-DAC International Conference on Digital Preservation and Development Trusted Digital Repositories**, 5-6 Şubat 2014, ed.: Dinesh Katre ve David Giaretta, Yeni Delhi[Hindistan], yayımcı yok, 2014, s. 220-227.

Adams, Regan: "Information Privacy in the USA", **Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra [Birleşik Krallık], Facet Publishing, 2011, s. 77-87.

Adu, Kofi Koranteng ve Ngulube, Patrick: "Key Threats and Challenges to the Preservation of Digital Records of Public Institutions in Ghana", **Information, Communication&Society**, C. 20, No: 8, 2016, s. 1-19.

Agata, Teru, Miyata, Yosuke ve Ikeuchi, Atsushi: "Long-term Preservation of PDF Files in Institutional Repositories in Japan", **16. International Conference on Digital Preservation**, 16-20 Eylül 2019, ed.: Marcel Ras, Sierman, Barbara ve Puggioni, Angela, Amsterdam [Hollanda], yayımcı yok, 2019, s. 423-425, (Çevrimiçi) https:// ipres2019. org/ static/ proceedings/ iPRES2019. pdf, 5 Mart 2020.

Akgün, Birol: "Türkiye'de Siyasal Güven: Nedenleri ve Sonuçları", **Ankara Üniversitesi SBF Dergisi**, C. 56, No: 4, 2001, s. 1-23.

Aksoy, Mehmet Ali: "Türk Ticaret Kanunu Bağlamında Defter Tutma Yükümlülüğü", **Hacettepe Hukuk Fakültesi Dergisi**, C. 6, No: 2, 2016, s. 154-156.

Aydın, Cengiz ve Özdemirci, Fahrettin: "Elektronik Belgelerin Arşivlenmesinde Gerçekliğin ve Bütünlüğün Korunması", **Bilgi Dünyası**, C. 12, No: 1, 2011, s. 105-127.

Ayvaz, Sema Taşpınar: "Türk Borçlar Kanunu ve Hukuk Muhakemeleri Kanunu'nun İmza Atamayanlarla İlgili Yeni Düzenlemesine Eleştirel Bir Bakış", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C. 61, No: 1, 2012, s. 321-349.

Bak, Greg: "Trusted by Whom"? TDRs, Standards Culture and Nature of Trust", **Archival Science**, No: 16, 2016, s. 373-402.

Bearman, David: "Moments of Risk: Identifying Threats to Electronic Records", **Archivaria**, No: 62, 2006, s. 15-46.

Bearman, David ve Trant, Jennifer: "Authenticity of Digital Resources: Towards a Statement of Requirements in the Research Process", **D-Lib Magazine**, 1998, (Çevrimiçi) http :// www. dlib. org/ dlib/ june98/ 06bearman.html, 31 Mayıs 2020.

Bell, AR: "Standards and Standards Culture: Understanding the Nature and Criticisms of Standardisation", **Comma**, No: 2, 2011, s. 25-38.

Berkin, Necmettin: "İspat Hukukunda Senet Delili ve Yazılı Şekil", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. 12, No: 4, 1946, s. 1175-1192.

Binici, Kasım: "Makine Öğrenmesi Yaklaşımıyla e-Belgelere Standart Dosya Plan Numaralarının Otomatik Olarak Atanması Üzerine Bir Çalışma", **Bilgi Yönetimi**, C. 2, No: 2, 2019, s. 116-126.

Boudrez, Philip: "Digital Signatures and Electronic Records", **Archival Science**, C. 7, No: 2, 2007, s. 180-191.

Boztepe, Hatun: "Halkla İlişkiler Perspektifinden Güven Kavramı: Katılımcılık, Şeffaflık ve Hesap Verebilirlik İlkelerinin Kamu Kurumlarına Yönelik Güveninin Oluşmasındaki Rolü", **İstanbul Üniversitesi İletişim Fakültesi Dergisi**, No: 45, 2013, s. 53-74.

Bralic, Vladamir, Kules, Magdalena ve Stancic, Hrvoje: "A Model for Long-term Preservation of Digital Signature Validity: TrustChain", **InFuture 2017**, 8-10 Kasım 2017, ed.: Iana Atassova v.d., Zagrep, yayımcı yok, 2017, s. 89-103.

Bralic, Vladamir, Stancic, Hrvoje ve Stengard, Mats: "A Blockchain Approach to Digital Archiving: Digital Signature Certification Chain Preservation", **Records Management Journal**, C. 30, No: 3, 2020, s. 345-362.

Breen, Mike: "Nothing to Hide: "Why Metadata Should Be Presumed Relevant", U**niversity of Kansas Law Review**, C. 56, 2008, s. 439-471.

Breir, Jakub ve Branisova, Jana: "A Dynamic Rule Creation Based Anomaly Detection Method for Identifying Security Breaches in Log Records", **Wireless Personal Communications**, No: 94, 2017, s. 497-511.

Bryne, Terrance K.: "Time for an Upgrade- Amending the Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation", **Journal of Law and Health**, C. 28, No: 379, 2015, s. 379-405.

Buchmann, Nicholas vd.: "Enhancing Breeder Document Long-Term Security Using Blockchain Technology", **41. International Computer Software and Applications Conference**, yayım yeri yok, The Institute of Electrical and Electronics Engineers [IEEE], 2017, s. 744–748.

Bui, Tu vd.: "ARCHANGEL: Tamper-proofing Video Archives Using Temporal Content Hashes on the Blockchain", **CVPR Blockchain Workshop**, 17 Haziran 2019, Long Beach[ABD], yayımcı yok, 2019, (Çevrimiçi) https:// arxiv. org/ abs/ 1904.12059, 1 Nisan 2020.

Bunawan, Ap-azli, Nordin, Sharifalillah ve Haron, Haryani: "Model for Preserving the Electronic Records Event History Metadata in Malaysia Government Agencies", **Seventh International Conference on Computational Intelligence, Modelling and Simulation (CIMSim)**, 27-29 Temmuz 2015, ed.: David Al-Dabass, Zuwairie Ibrahim ve Mohd Ibrahim Shapiai, yayım yeri yok, yayımcı yok, 2015, s. 29-34.

Casemento, Greg ve Hatfield, Patrick: "The Essential Elements of An Effective Electronic Signature Process", **Digital Evidence and Electronic Signature Law Review**, No: 6, 2009, s. 83-97.

Chasse, Ken: "Electronic Records for Evidence and Disclosure and Discovery", **Criminal Law Quarterly**, No: 57, 2011, s. 284-326.

Chasse, Ken: **Electronic Records as Evidence**, (Çevrimiçi) http:// ssrn. com/ abstract=2438350, 28 Kasım 2019.

Chema, G. Shabbir: "Building Trust in Government: An Introduction", **Building Trust in Government: Innovations in Governance Reform in Asia**, ed.: G. Shabbir Chema ve Vesselin Popovski, New York[ABD], United Nations University Press, 2010, s. 1-21.

Cibaroğlu, Mehmet Oytun: "Elektronik Belge Yönetim Sistemi'nde Belgelerin Uzun Süreli Korunmasına Dair Bir Yaklaşım Değerlendirmesi: Açık Arşiv Bilgi Sistemi Referans Modeli (OAIS)", ed.: Fahrettin Özdemirci ve Zeynep Akdoğan, **Bilgi Sistemleri ve Bilişim Yönetimi: Beklentiler ve Yeni Yaklaşımlar**, Ankara, Ankara Üniversitesi, 2017, s. 309-331.

Cohen, Frederick B.: "Digital Diplomatics and Forensics: Going Forward on a Global Basis" **Records Management Journal**, C. 25, No: 1, 2015, s. 21-44.

Collomosse, John vd.: "ARCHANGEL: Trusted Archives of Digital Public Documents", **Proceedings of the Association of Computing Machinery [ACM] Symposium on Document Engineering**, yayım yeri yok, ACM, 2018, (Çevrimiçi) https:// arxiv. org/ pdf/ 1804.08342.pdf, 1 Nisan 2020.

Cook, Terry: "Evidence, Memory, Identity and Community: Four Shifting Archival Paradigms", **Archival Science**, C. 13, No: 2-3, 2013, s. 95-120.

Cunningham-Day, Julian ve Didizian, Marly: "Data Exchange and Confidentiality: An Asia Pacific Perspective", **Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra[Birleşik Krallık], Facet Publishing, 2011, s. 61-76.

Çatalkaya, Hayrettin, Karaman, Muhammer ve Koca, Erdal: "Elektronik Kopyanın (Adli İmaj) Alınmasında Açık Kaynak Uygulamalarının Güvenirliği", **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi**, C. 1, No: 2, 2015, s. 15-19.

Çelik, Vural vd.: "Elektronik Yazışma Projesi Güvenlik Katmanları ve Uygulama Geliştirme Esnasında Dikkat Edilmesi Gereken Hususlar", **Bilgi Sistemleri ve Bilişim Yönetimi: Beklentiler ve Yeni Yaklaşımlar**, ed.: Fahrettin Özdemirci ve Zeynep Akdoğan, Ankara, Ankara Üniversitesi, 2017, s. 103-120.

Çiçek, Niyazi: "Belediyelerdeki Elektronik Belge Yönetim Sistemlerinde Dijital Devamlılığı Tehdit Eden Yazılıma Dayalı Sorunlar", **Belediyelerin Kütüphane ve Arşiv Hizmetleri Uluslararası Sempozyumu**, 12-14 Mayıs 2016, ed.: Bülent Yılmaz vd., Nilüfer Belediyesi, Bursa, 2016, s. 409-428.

Çiçek, Niyazi: "Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme", **Bilgi Dünyası**, C. 12, No: 1, 2011, s. 87-104.

Çiçek, Niyazi: "Elektronik Belge Yönetimi Uygulamalarında Bir Alt Sistem Olarak Dosya Yönetimi", **Türk Kütüphaneciliği**, C. 30, No: 3, 2016, s. 434-448.

Çiçek, Niyazi: "Elektronik Belge Yönetimi Uygulamalarında Dosya Bütünlüğü Problemi", **e-Beyas 2015 Sempozyumu Kurumsal Belleklerin Geleceği: Dijitalleştirme-Elektronik Arşiv-Elektronik Belge Yönetimi**, 21-22 Ekim 2015, ed.: Fahrettin Özdemirci vd., Ankara, Ankara Üniversitesi, 2016, s. 163-172.

Çiçek, Niyazi: "E-Devlet Stratejisi Bağlamında Elektronik Belge Yönetimi için "Yazılı Politika" Gereksinimi: Türkiye'deki Uygulamalar Üzerine Bir İnceleme", **Türk Kütüphaneciliği**, C. 34, No: 3, 2020, s. 377-405.

Çiçek, Niyazi: "Özel Diplomatik Analiz Metodu: Sağlık Bakanlığında Üretilen İki Yazışma Üzerinde Uygulama", **Bilgi Dünyası**, C. 7, No: 2, 2006, s. 267-292.

Çiçek, Niyazi ve Sağlık, Özhan: "Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı", **Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ**, ed.: Bahattin Yalçınkaya vd., Ankara, Ankara Üniversitesi, 2019, s. 141-170.

Çiçek, Niyazi ve Sağlık, Özhan: e-Belgelerin Arşivsel Bağının lektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme, **Bilgi Sistemleri ve Bilişim Yöntemi: Beklentiler ve Yeni Yaklaşımlar**, ed.: Fahrettin Özdemirci ve Zeynep Akdoğan, Ankara, Ankara Üniversitesi, 2017, s. 257-276.

Çilingir, Lokman: "Locke'un Toplum Sözleşmesi Kuramı", **Temâşâ Felsefe Dergisi**, No: 11, 2019, s. 31-43.

Di Cosmo, Roberto ve Zacchiroli, Stefano: "Software Heritage: Why and How to Preserve Software Source Code", **14. International Conference on Digital Preservation**, 25-29 Eylül 2017, Kyoto[Japonya], yayımcı yok, 2017, (Çevrimiçi) https:// ipres2017. jp/ wp-content/ uploads/ 19Roberto-Di-Cosmo. pdf, 31 Aralık 2019.

Dore, Michael H.: "Forced Preservation Electronic Evidence and the Business Records Hearsay Exception", **Columbia Science and Technology Law Review**, No: 76, 2010, s. 76-92.

Duranti, Luciana: "Concepts and Principles for the Management of Electronic Records, or Records Management Theory is Archival Diplomatics", **Records Management Journal**, C. 20, No: 1, 2010, s. 78-95.

Duranti, Luciana: "Diplomatics: New Uses for an Old Science", **Archivaria**, No: 28, 1989, s. 7-27.

Duranti, Luciana: "Preservation in the Cloud: Towards an International Framework for a Balance of Trust and Trustworthiness", **APA/C-DAC International Conference on Digital Preservation and Development Trusted Digital Repositories**, Yeni Delhi[Hindistan], 5-6 Şubat 2014, ed.: Dinesh Katre ve David Giaretta, yayım yeri yok, yayımcı yok, 2014, s. 23-38.

Duranti, Luciana: "Structural and Formal Analysis: The Contribution of Diplomatics to Archival Appraisal in the Digital Environment", **The Future of Archives and Recordkeeping: A Reader**, ed.: Jennie Hill, Londra [Birleşik Krallık], Facet Publishing, 2011, s. 65-88.

Duranti, Luciana: "The Concept of Electronic Record", **Preservation of the Integrity of Electronic Records**, ed.: Luciana Duranti, Terry Eastwood ve Heather MacNeil, yayım yeri yok, Springer, 2002, s. 9-22.

Duranti, Luciana: "The INTERPARES2 Project (2002-2007): An Overview", **Archivaria**, No: 64, 2007, s. 113-121.

Duranti, Luciana ve Rogers, Corinne: "Educating for Trust", **Archival Science**, C. 11, No: 3-4, 2011, s. 373-390.

Duranti, Luciana ve Rogers, Corinne: "Memory Forensics: Integrating Digital Forensics with Archival Science for Trusting Records and Data", **eForensics Magazine**, C. 2, No: 15, 2013, (Çevrimiçi) https:// www. academia. edu/ 11328085/ Memory_ Forensics_ Integrating_ Digital_ Forensics_ with_ Archival_ Science_ for_ Trusting_ Records_and_Data, 29 Mart 2020.

Duranti, Luciana ve Rogers, Corinne: "Trust in Digital Records: An Increasingly Cloudy Legal Area, **Computer Law & Security Review**, No: 28, 2012, s. 522-531.

Duranti, Luciana, Rogers, Corinne ve Sheppard, Anthony: "Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later", **Archivaria**, No: 70, 2011, s. 101-120.

Duranti, Luciana ve Stanfield, Allison: "Authenticating Electronic Evidence", **Electronic Evidence and Electronic Signatures**, 5. bs., ed.: Stephen Mason ve Daniel Seng, Londra[Birleşik Krallık], University of London Press, 2021, s. 236-278.

Duranti, Luciana ve Thibodeau, Kenneth: "The Concept of Record in Interactive, Experiential and Dynamic Environments: The View of Interpares", **Archival Science**, No: 6, 2006, s. 13-68.

Eastwood, Terry: "Introduction", **Preservation of the Integrity of Electronic Records**, ed.: Luciana Duranti, Terry Eastwood ve Heather MacNeil, yayım yeri yok, Springer, 2002, s. 1-8.

Elitaş, Cemal, Aydemir, Oğuzhan ve Elitaş, Leyli Bilge: "Muhasebe Açısından Kamu Güveni: Türk Ceza Kanunu'nun İncelenmesi", **Mali Çözüm Dergisi**, No: 93, 2009, s. 29-44.

Ellis, Judith: "Embedding Records Management in the Business", **Managing Records Risks in Global Financial Institutions, Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra[Birleşik Krallık], Facet Publishing, 2011, s. 199-216.

Ergun, Tamer ve Çelik, Vural: "E-Arşiv ve Uzun Süreli Doğrulama", **e-Beyas 2015 Sempozyumu Kurumsal Belleklerin Geleceği: Dijitalleştirme-Elektronik Arşiv-Elektronik Belge Yönetimi**, 21-22 Ekim 2015, ed.: Fahrettin Özdemirci vd., Ankara, Ankara Üniversitesi, 2016, s. 199-203.

Erickson, Chris L. ve. Lunt, Barry M.: "Alternatives for Long-Term Storage of Digital Information", **12. International Conference on Digital Preservation**, 2-6 Kasım 2015, ed.: Christopher Lee, North Carolina[ABD], School of Information and Library Science University of North Carolina at Chapel Hill, 2015, s. 231-232, (Çevrimiçi) https:// phaidra. univie. ac. at/ view/ o: 429524, 4 Mart 2020.

Eroğlu, Şahika ve Külcü, Özgür: "TS 13298 Çerçevesinde Kurumsal Bilgi Yönetim Sistemleri ve Elektronik Belge Yönetimi Standartlarının Değerlendirilmesi: İçişleri Bakanlığı Örneği", **Bilgi Dünyası**, C. 15, No: 2, 2014, s. 327-352.

Galiev, Albert vd.: "Archain: A Novel Blockchain Based Archival System", **Proceedings of the 2nd World Conference on Smart Trends in Systems, Security and Sustainability**, Londra[Birleşik Krallık], yayımcı yok, 2019, s. 84-89.

Garfinkel, Simon: "Digital Forensics XML and the DFXML Toolset", **Digital Investigation**, No: 8, 2012, s. 161-174.

Garfinkel, Simon: "Providing Cryptographic Security and Evidentiary Chain-of Custody with the Advanced Forensic Format, Library, and Tools", **International Journal of Digital Crime and Forensics**, C. 1, No: 1, 2009, s. 1-28.

Garnett, Alex, Winter, Mike ve Simpson, Justin: "Checksums on Modern Filesystems, or: On the Virtuous Consumption of CPU Cycles", **15. International Conference on Digital Preservation**, 24-27 Eylül 2018, ed.: Megan Potterbusch vd., Boston[ABD], yayımcı yok, 2018, (Çevrimiçi) https:// osf. io/ cxahf, 1 Ocak 2020.

Glassford, Sarah: "Black Hole or Brave New World? Archivists, Historians and the Challenges of the Digital Age", **Emerging Library & Information Perspectives**, C. 1, No: 1, Spring 2018, s. 91-110.

Guercio, Maria: "Digital Preservation in Europe: Strategic Plans, Research Outputs and Future Implementation. The Weak Role of the Archival Institutions", **The Memory of the World in the Digital Age: Digitization and Preservation. An International Conference on Permanent Access to Digital Documentary Heritage**, 26-28 Eylül 2012, ed.: Luciana Duranti ve Elizabeth Shaffer, Vancouver[Kanada], UNESCO, 2013, s. 467-481.

Guercio, Maria: "The Italian Case: Legal Framework and Good Practices for Digital Preservation", **Policies for Recordkeeping and Digital Preservation: Recommendations for Analysis and Assesment Services**, ed.: Stefano Allegrezza vd., yayım yeri yok, yayımcı yok, 2016, s. 28-37.

Gübeş, Neşe Öztürk: "An Investigation into Weighting Problem in Norm-Referenced Grading System", **Eurasian Journal of Educational Research**, No: 93, 2021, s. 337-356.

Gümüş, Hatice: "Kurumlarda EBYS ve Arşiv Çalışmaları, Yaşanan Sorunlara Genel Bir Bakış", **e-Beyas 2015 Sempozyumu Kurumsal Belleklerin Geleceği: Dijitalleştirme Elektronik Arşiv-Elektronik Belge Yönetimi**, 21-22 Ekim 2015, ed.: Fahrettin Özdemirci vd., Ankara, Ankara Üniversitesi, 2016, s. 97-108.

Gunnlaugsdottir, Johanna: "Information and Records Management: A Precondition for a Well Functioning Quality Management System", **Records Managament Journal**, C. 22, No: 3, 2012, s. 170-185.

Guo, Wei vd.: "Archives as a Trusted Third Party in Maintaining and Preserving Digital Records in The Cloud Environment, **Records Management Journal**, C. 26, No: 2, 2016, s. 170-184.

Han, Yan ve Chan, Chi Pak: "The Modeling System Reliability For Digital Preservation: Model Modification and Four-Copy Model Study", **5. International Conference on Preservation of Digital Objects: Joined Up and Working: Tools and Methods for Digital Preservation**, 29-30 Eylül 2008, Londra[Birleşik Krallık], The British Library, 2008, s. 281-286, (Çevrimiçi) https:// phaidra. univie. ac. at/ detail_object/o:294190, 4 Mart 2020.

Hasan, Ragib vd.: "Trustworthy Records Retention", **Handbook of Database Security**, ed.: Michael Gertz ve Sushil Jajodia, New York[ABD], Springer, 2008, s. 357-381.

Hasırcıoğlu, Işıl: "Elektronik İmza Oluşturma ve Doğrulama Standartları", **Ulusal Elektronik İmza Sempozyumu**, Ankara, Gazi Üniversitesi, 2006, (Çevrimiçi) http :// www. kamusm. gov. tr/ dosyalar/ makaleler/ Elektronik % 20 Imza % 20 Olusturma % 20 ve % 20Dogrulama.pdf, 29 Şubat 2020.

Herbest, Jonathan ve Lovegrove, Simon: "Moves towards a Common Regulatory Framework for Financial Services in the European Union", **Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra[Birleşik Krallık], Facet Publishing, 2011, s. 41-60.

Hernandez-Ardieta, Jorge L. vd.: "A Taxonomy and Survey of Attacks on Digital Signatures", **Computers&Security**, No: 34, 2013, s. 67-112.

Hofman, Darra vd.: "Building Trust Protecting Privacy Analyzing Evidentiary Quality in a Blockchain Proof-of Concept for Health Research Data Consent Management", **IEEE 2018 International Congress on Cybermatics**, 30 Temmuz-3 Ağustos 2018, ed.: Juan E. Guerrero, Halifax[Kanada], IEEE, s. 1650-1656.

Hofman, Darra vd.: "The Margin Between the Edge of the World and Infinite Possibility: Blockchain, GDPR and Information Governance", **Records Management Journal**, C. 29, No: 1-2, 2019, s. 240-257.

Hosmer, Chet: "Providing the Integrity of Digital Evidence with Time", **International Journal of Digital Evidence**, C. 1, No: 1, Spring 2002, s. 1-7.

Hutchinson, Tim: "Natural Language Processing and Machine Learning as Practical Toolsets for Archival Processing", **Records Management Journal**, C. 30, No: 2, 2020, s. 155-174.

Irons, Alastair: "Computer Forensics and Records Management: Compatible Disciplines", **Records Management Journal**, C. 16, No: 2, 2006, s. 102-112.

John, Jeremy Leighton: "Adapting Existing Technologies for Digitally Archiving Personal Lives: Digital Forensics, Ancestral Computing, and Evolutionary Perspectives and Tools", **5. International Conference on Preservation of Digital Objects**, 29-30 Eylül 2008, Londra[Birleşik Krallık], The British Library, 2008, s. 48-55, (Çevrimiçi) https :// ipres-conference. org/ ipres08/ ipres2008-proceedings.pdf, 28 Mart 2020.

Johnson, Duff: "Achieving Canonical PDF Validation", **11. International Conference on Digital Preservation**, 6-10 Ekim 2014, ed.: Serena Coates vd., Melbourne[Avustralya], State Library of Victoria, 2014, s. 39-43, (Çevrimiçi) https:// phaidra. univie. ac. at/ detail_object/ o:378066, 5 Mart 2020.

Kandur, Hamza: "Elektronik Belgelerin Özniteliklerinin Elektronik Belge Yönetimi Açısından İncelenmesi", **Aysel Yontar Armağanı**, ed.: Bekir Kemal Ataman ve Mesut Yalvaç, İstanbul, Türk Kütüphaneciler Derneği İstanbul Şubesi, 2004, s. 121-131.

Kelton, Kari, Fleischmann, Kenneth R. ve Wallace, William A.: "Trust in Digital Information", **Journal of the American Society for Information Science and Technology**, C. 59, No: 3, 2008, s. 363-374.

Klindt, Marco: "PDF/A Considered Harmful for Digital Preservation", **14. International Conference on Digital Preservation**, 25-29 Eylül 2017, Kyoto[Japonya], yayımcı yok, 2017, (Çevrimiçi) https :// ipres2017. jp/ wp-content/ uploads/ 15. pdf, 31 Aralık 2019.

Kocaoğlu, Belgin Uçar: "Kamu Kurumlarında Yönetsel Kapasitenin Güçlendirilmesi", **Sayıştay Dergisi**, No: 114, 2019, s. 117-133.

Külcü, Özgür ve Külcü, Hande: "The Records Management Capacity Assessment System (RMCAS) as a Tool for Program Development at the Turkish Red Crescent Society", **International Journal of Information Management**, C. 29, No: 6, 2009, s. 483-487.

Külcü, Özgür ve Turan, Metin: "Kamu Hukukunda Geleneksel ve Elektronik İletişim, Bilgi ve Belge Yönetimi Uygulamaları", **Türk Kütüphaneciliği**, C. 27, No: 2, 2013, s. 266-300.

Lax, Gianluca, Buccafurri, Francesco ve Caminiti, Gianluca: "Digital Document Signing: Vulnerabilities and Solutions, **Information Security Journal: A Global Perspective**, No: 24, 2015, s. 1–14.

Lee, Christopher: "Archival Application of Digital Forensics Methods for Authenticity, Description and Access Provision, **Comma**, No: 2, 2012, s. 133-139.

Lee, Christopher ve Woods, Kam: "Diverse Digital Collections Meet Diverse Uses: Applying Natural Language Processing to Born-Digital Primary Sources", **14. International Conference on Digital Preservation**, 25-27 Eylül 2017, Kyoto[Japonya], yayımcı yok, 2017, (Çevrimiçi) https:// ipres2017. jp/ wp-content/ uploads/ 50. pdf, 31 Aralık 2019.

Lehtonen, Juha vd.: "PDF Mayhem: Is Broken Really Broken?", **15. International Conference on Digital Preservation**, 24-27 Eylül 2018, ed.: Megan Potterbusch vd., Boston [ABD], yayımcı yok, 2018, (Çevrimiçi) https :// osf. io/ n85b9/, 5 Ocak 2020.

Lekkas, Dimitrios ve Gritzalis, Dimitris: "Long-term Verifiability of Electronic Healthcare Records' Authenticity", **International Journal of Medical Informatics**, No: 76, 2007, s. 442-448.

Lemieux, Victoria L.: "A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation", **2017 IEEE International Conference on Big Data**, ed.: Nie Jian-Yun vd., Boston [ABD], IEEE, 2017, s. 2271-2278.

Lemieux, Victoria L.: "Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework", **Future Technologies Conference**, 29-30 Aralık 2017, Vancouver[Kanada], The Science and Information Organization, 2017, s. 41-48.

Lemieux, Victoria L.: "Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective", **European Property Law Journal**, C. 6, No: 3, 2017, s. 392-440.

Lemieux, Victoria L.: "Trusting Records: Is Blockchain Technology the Answer?", **Records Management Journal,** C. 26, No: 2, 2016, s. 110-139.

Lemieux, Victoria L. ve Krumwied, Ember D.: "Managing Records Risks in Global Financial Institutions", **Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra[Birleşik Krallık], Facet Publishing, 2011, s. 91-105.

Lemieux, Victoria L. vd.: "Caught in the middle? Strategic Information Governance Disruptions in the Era of Blockchain and Distributed Trust", **Records Management Journal**, C. 30, No: 3, 2020, s. 301-324.

Leroux, Oliver: "Legal Admissibility of Electronic Evidence", **International Review of Law, Computers & Technology**, C. 18, No: 2, 2004, s. 193-220.

Loehrlein, Aaron J., Lemieux, Victoria L. ve Bennett, Michael: "The Classification of Financial Products", **Journal of the Association for Information Science and Technology**, C. 65, No: 2, 2014, s. 263-280.

Luu, Loi vd.: "Making Smart Contracts Smarter", **23. ACM Conference on Computer and Communications Security Hofburg Palace**, 24-28 Ekim 2016, Viyana[Avusturya], ACM, 2016, (Çevrimiçi) https:// eprint. iacr. org/ 2016/ 633. pdf, 1 Nisan 2020.

Lynch, Clifford "Stewardship in the Age of Algorithms", **First Monday**, C. 22, No: 14, 2017, s. 1-21.

MacNeil, Heather: "Methods for Creating and Maintaning Reliable and Authentic Electronic Records", **Preservation of the Integrity of Electronic Records**, ed.: Luciana Duranti, Terry Eastwood ve Heather MacNeil, yayım yeri yok, Springer, 2002, s. 39-56.

Majore, Sekie Amanuel, Yoo, Hyunguk ve Shon, Taeshik: "Next Generation Electronic Record Management Systems Based on Digital Forensics", **International Journal of Security and its Applications**, C. 7, No: 1, 2013, s. 189-193.

Majore, Sekie Amanuel, Yoo, Hyunguk ve Shon, Taeshik: "Secure and Reliable Electronic Record Management System Using Digital Forensic Technologies", **The Journal of Supercomputing**, No: 70, 2014, s. 149-165.

Manap, Cevat ve Apohan, A. Murat: "Özet Fonksiyonlarındaki Zayıflıklar ve Elektronik İmzalara Etkisi", **Ulusal Elektronik İmza Sempozyumu**, Ankara, Gazi Üniversitesi, 2006, (Çevrimiçi) http:// www. kamusm. gov. tr/ dosyalar/ makaleler/ Ozet %20Fonksiyonlarindaki %20Zayifliklar %20Ve %20Elektronik %20Imzalara %20Etkisi.pdf, 29 Şubat 2020.

Manor, James: "The potential -Constructive and Destructive- of Information Technology for Records Management: Case Studies from India", **A Matter of Trust: Building Integrity into Data, Statistics and Records to Support the Sustainable Development Goals**, ed.: Anne Thurston, Londra[Birleşik Krallık], University of London Press, 2020, s. 67-82.

Mason, Stephen: "Electronic Signature", **Electronic Evidence and Electronic Signatures**, 5. bs., ed.: Stephen Mason ve Daniel Seng, Londra[Birleşik Krallık], University of London Press, 2021, s. 279-396.

McLeod, Julie, Childs, Sue ve Heaford, Susan: "Records Management Capacity and Compliance Toolkits: A Critical Assessment", **Records Managament Journal**, C. 17, No: 3, 2007, s. 216-232.

McLeod, Julie: "On Being Part of the Solution, not the Problem", **Records Management Journal**, C. 22, No: 3, 2012, s. 186-197.

Meehan, Jennifer: "Towards an Archival Concept of Evidence", **Archivaria**, No: 61, 2006, s. 127-146.

Meissonnier, Antoine ve Banat-Berger, Françoise: "French Legal Framework of Digital Evidence", **Records Management Journal**, C. 25, No: 1, 2015, s. 96-106.

Michetti, Giovanni vd.: "Intellectual Control", **Trusting Records in the Cloud**, ed.: Luciana Duranti ve Corinne Rogers, Londra[Birleşik Krallık], Facet Publishing, 2019, s. 155-178.

Millar, Laura: "An Obligation of Trust: Speculations on Accountability and Description", **American Archivist**, C. 69, No: 1, 2006, s. 60-78.

Mosweu, Olefhile ve Ngoepe, Mpho: "Trustworthiness of Digital Records in Government Accounting System to Support the Audit Process in Botswana", **Records Management Journal**, C. 31, No: 1, 2021, s. 89-108.

Niu, Jinfang: "Original Order in the Digital World", **Archives and Manuscripts**, C. 43, No: 1, 2015, s. 61-72.

Oliver, Gillian: "International Records Management Standards: The Challenges of Achieving Consensus", **Records Management Journal**, C. 24, No: 1, 2014, s. 22-31.

Örselli, Erhan ve Sipahi, Esra Banu: "Türkiye'de Vatandaşların Kamu urumlarına Güveni", **Uluslararası Sosyal Araştırmalar Dergisi**, C. 9, No: 45, 2016, s. 843-850.

Özbek, Murat: "Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları", **1. International Symposium on Digital Forensics and Security**, 20-21 Mayıs 2013, ed.: Asaf Varol vd., Elazığ, yayımcı yok, 2013, s. 255-262.

Özbek, Mustafa Serdar: "Elektronik Ortamda Düzenlenen Noter Senetleri", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 22, No: 3, Cevdet Yavuz'a Armağan Özel Sayısı, 2016, s. 2247-2248.

Özdemir, Lale ve Cengiz, Emine: "Türk Kamu Sektöründe Dijital Süreklilik Ne Kadar Mevcut: Teorik Bir Çerçeve", **Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ**, ed.: Bahattin Yalçınkaya vd., Ankara, Ankara Üniversitesi, 2019, s. 273-294.

Pan, Weimei ve Duranti, Luciana: "Sitting in Limbo or Being the Flaming Phoenix: The Relevance of the Archival Discipline to the Admissibility of Digital Evidence in China", **Archives and Manuscripts**, C. 48, No: 3, 2020, s. 300-327.

Pember, Margaret: "Sorting out the Standards: What Every Records and Information Professional Should Know", **Records Managament Journal**, C. 16, No:1, 2006, s. 21-33.

Rechert, Klaus, Valizada, Isgandar ve Suchodoletz, Dirk von: "Future-Proof Preservation of Complex Software Environments", **9. International Conference on the Preservation of Digital Objects**, 1-5 Ekim 2012, ed.: Reagan Moore, Kevin Ashley ve Seamus Ross, Toronto [Kanada], University of Toronto, 2012, s. 180-183.

Rimkus, Kyle R. vd.: "Preservation and Access for Born-digital Electronic Records: The Case for an Institutional Digital Content Format Registry", **American Archivist**, C. 83, No: 2, 2020, s. 397-428.

Rogers, Corinne: "Authenticity of Digital Records in Practice", **2015 Digital Heritage Conference**, 28 Eylül-2 Ekim 2015, ed.: Gabriele Guidi vd., Granada[İspanya], IEEE, 2015, s. 395-398.

Rogers, Corinne: "Diplomatics of Born-digital Documents: Considering Documentary Form in a Digital Environment", **Records Management Journal**, C. 25, No: 1, 2015, s. 6-20.

Rolan, Gregory vd.: "More Human than Human? Artificial Intelligence in the Archive", **Archives and Manuscripts**, C. 47, No: 2, 2019, s. 179-203.

Rosenthal, David S.: "Bit Preservation: A Solved Problem?", **5. International Conference on Preservation of Digital Objects: Joined Up and Working: Tools and Methods for Digital Preservation**, 29-30 Eylül 2008, Londra[Birleşik Krallık], The British Library, 2008, s. 274-280, (Çevrimiçi) https:// phaidra. univie. ac. at/ detail_ object/ o:294190, 4 Mart 2020.

Rosenthal, David S. vd.: "Requirements for Digital Preservation Systems: A Bottom-Up Approach", **D-Lib Magazine**, C. 11, No: 11, 2005 (Çevrimiçi) http:// www. dlib. org/ dlib/ november05/rosenthal/11rosenthal.html, 2 Şubat 2020.

Rupasinghe, P. L., Weerasena H.H., ve Murray, I: "Trustworthy Provenance Framework for Document Workflow Provenance", **International Conference on Computational Techniques in Information and Communication Technologies**, 11-13 Mart 2016, New York[ABD], Curran Associates, s. 168-175.

Sa'di, Mursilalaili Mustapa vd.: "Authentication of Electronic Evidence in Cybercrime Cases Based on Malaysian Laws", **Pertanika Journal of Social Sciences & Humanities**, C. 23, s. 153-167.

Sağlık, Özhan ve Çiçek, Niyazi: "Elektronik İmzalı Belgelerin Delil Değerinin Korunmasında Mevzuatta Öngörülen Delil Özelliklerinin İncelenmesi", **Bilgi Yönetimi**, C. 3, No: 2, 2020, s. 120-142.

Salza, Silvio ve Guercio, Maria: "Authenticity Management in Long Term Digital Preservation of Medical Records", **9. International Conference on the Preservation of Digital Objects**, 1-5 Ekim 2012, ed.: Reagan Moore, Kevin Ashley ve Seamus Ross, Toronto[Kanada], University of Toronto, 2012, s. 172-179.

Sataaslaatten, Olav Hagen: "The Norweigan Noark Model Requirements for EDRMS in the Context of Open Government and Access to Governmantal Information", **Records Management Journal**, C. 34, No: 3, 2014, s. 189-204.

Sautter, Ed: "Conflicts of Laws in Multiple Jurisdictions", **Managing Records in Global Financial Markets: Ensuring Compliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra[Birleşik Krallık], Facet Publishing, 2011, s. 17-32.

Schneider, Josh vd.: "Appraising, Processing, and Providing Access to Email in Contemporary Literary Archives", **Archives and Manuscripts**, C. 47, No: 3, 2019, s. 305-326.

Schüll, Natasha Dow: "Digital Containment and its Discontents", **History and Anthropology**, C. 29, No: 1, 2018, s. 42-48.

Seltzer, Margo ve Murphy, Nicholas: "Hierarchical File Systems Are Dead", **Proceedings of the 12th Conference on Hot Topics in Operating Systems**, ABD, USENIX Association, 2009.

Sethia, Aradya: "Rethinking Admissibility of Electronic Evidence", **International Journal of Law and Information Technology**, C. 24, No: 3, 2016, s. 229-250.

Shabou, Basma Makhlouf: "Digital Diplomatics and Measurement of Electronic Public Data Qualities What Lessons Should be Learned?", **Records Management Journal**, C. 25, No: 1, 2015, s. 56-77.

Sodring, Thomas, Reinholdtsen, Petter ve Olnes, Svein: "Publishing and Using Record-keeping Structural Information in a Blockchain", **Records Management Journal**, C. 30, No: 3, 2020, s. 325-343.

Solhan, Selman: "Fizikselden Elektroniğe; Belge Yönetim ve Arşivleme Sürecinin Sürdürülebilirliği", **e-Beyas 2015 Sempozyumu Kurumsal Belleklerin Geleceği: Dijitalleştirme-Elektronik Arşiv-Elektronik Belge Yönetimi**, 21-22 Ekim 2015, ed.: Fahrettin Özdemirci vd., Ankara, Ankara Üniversitesi, 2016, s. 49-64.

Spencer, Ross: "Binary Trees? Automatically Identifying the Links between Born-digital Records", **Archives and Manuscripts**, C. 45, No: 2, 2017, s. 77-99.

Stancic, Hrvoje, Rajh, Arian ve Brzica, Hrvoje: "Archival Cloud Services: Portability, Continuity and Sustainability Aspects of Long-term Preservation of Electronically Signed Records", **The Canadian Journal of Information and Library Science**, C. 39, No: 2, 2015, s. 210-227.

Stephens, David: "Legal Issues", **Managing Electronic Records**, ed.: Julie McLeod ve Catherine Hare, Londra[Birleşik Krallık], Facet Publishing, 2005, s. 101-114.

Suderman, Jim: "Defining Electronic Series: A Study", **Archivaria**, No: 53, 2002, s. 31-46.

Sultan, Kashif, Hazrat Ali ve Zhongshan Zhang: "Call Detail Records Driven Anomaly Detection and Traffic Prediction in Mobile Cellular Networks", **IEEE Access**, 2018, s. 41728-41737.

Şahin, Ali ve Söylemez, Adnan: "Yerel Yönetimlerde Kurumsal Kapasitenin Ölçülmesi (Konya Örneği)", **ASSAM Uluslararası Hakemli Dergi 13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı**, 2019, s. 471-493.

Şengül, Gökhan, Atsan, F. K. ve Bostan, Atila: "Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörüleri", **7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı**, 17-18 Ekim 2014, İstanbul, yayımcı yok, 2014, s. 95-101.

Takayama, Noriyuki: "On Fifty Million Floating Pension Records in Japan", **The Geneva Papers on Risk and Insurance - Issues and Practice**, C. 34, No: 4, 2009, s. 631-638.

Tarkhani, Zahra, Brown, Geoffrey ve Myers, Steven: "Trustworthy and Portable Emulation Platform for Digital Preservation", **14. International Conference on Digital Preservation**, 25-29 Eylül 2017, Kyoto [Japonya], yayımcı yok, 2017, (Çevrimiçi) https:// ipres2017. jp/ wp-content/ uploads/ 30.pdf, 1 Ocak 2020.

Tennis, Joseph T.: "Data, Documents and Memory: A Taxonomy of Sources in Relation to Digital Preservation and Authenticity Metadata", **The Memory of the World in the Digital Age: Digitization and Preservation**, 26-28 Eylül 2012, ed.: Luciana Duranti ve Elizabeth Shaffer, Vancouver[Kanada], UNESCO, 2013, s. 933-940.

Thibodeau, Kenneth: "The Perfect Archival Storm: The Transfer of Electronic Records from the G. W. Bush White House to the National Archives of United States", **The Memory of the World in the Digital Age: Digitization and Preservation**, 26-28 Eylül 2012, ed.: Luciana Duranti ve Elizabeth Shaffer, Vancouver[Kanada], UNESCO, 2013, s. 724-733.

Thibodeau, Kenneth: "Wrestling with Shape-Shifters: Perspectives on Preserving Memory in the Digital Age", **The Memory of the World in the Digital Age: Digitization and Preservation. An International Conference on Permanent Access to Digital Documentary Heritage**, 26-28 Eylül 2012, ed.: Luciana Duranti ve Elizabeth Shaffer, Vancouver[Kanada], UNESCO, 2013, s. 15-23.

Thirifays, Alex, Nielsen, Anders Bo ve Dokkedal, Barbara: "Evaluation of a Large Migration Project", **8. International Conference on Preservation of Digital Objects**, 1-4 Kasım 2011, ed.: Jose Borbinha vd., Singapur, yayımcı yok, 2011, s. 24-33, (Çevrimiçi) https :// services. phaidra. univie. ac. at/ api/ object/ o: 294293/diss/Content/get, 28 Mart 2020.

Thurston, Anne: "Digitization and Preservation: Global Opportunities and Cultural Challenges", **The Memory of the World in the Digital Age: Digitization and Preservation**, 26-28 Eylül 2012, ed.: Luciana Duranti ve Elizabeth Shaffer, Vancouver[Kanada], UNESCO, 2013, s. 31-37.

Thurston, Anne: "Records as Evidence for Measuring Sustainable Development in Africa", **A Matter of Trust: Building Integrity into Data, Statistics and Records to Support the Sustainable Development Goals**, ed.: Anne Thurston, Londra[Birleşik Krallık], University of London Press, 2020, s. 7-18.

Torunlar, Mehmet: "Arşiv - Hafıza - Kamusal Ensefalizasyon", **Arşiv Dünyası**, C. 6, No: 2, 2019, s. 100-133.

Tumuhairwe, Ronald ve Ahimbisibwe, Arthur: "Procurement Records Compliance, Effective Risk Management and Records Management Performance: Evidence from Ugandan Public Procuring and Disposing Entities", **Records Management Journal**, C. 26, No: 1, 2016, s. 83-101.

Turan, Metin: "Adli Bilişim ve Dijitalleştirme: Roller, Etkileşim ve Sorunlar", **e-Beyas 2015 Sempozyumu Kurumsal Belleklerin Geleceği: Dijitalleştirme-Elektronik Arşiv-Elektronik Belge Yönetimi**, 21-22 Ekim 2015, ed.: Fahrettin Özdemirci vd., Ankara, Ankara Üniversitesi, 2016, s. 121-134.

Vigil, Martin A. Gagliotti v.d.: "Assessing Trust in the Long-term Protection of Documents", **2013 IEEE Symposium on Computers and Communications**, 7-10 Temmuz 2013, Split[Hırvatistan], IEEE, tarih yok, s. 185-191.

Ward, Burke vd.: "Electronic Discovery Rules for a Digital Age", **Boston University Journal of Science and Technology aw**, C. 18, No: 150, 2012, (Çevrimiçi) https:// papers. ssrn. com/ sol3/ papers. cfm? abstract_ id =2229408, 5 Mart 2020.

Wilsey, Laura vd.: "Capturing and Processing Born-Digital Files in the STOP AIDS Project Records: A Case Study", **Journal of Western Archives**, C. 4, No: 1, 2013, s. 1-22.

Woods, Kam ve Lee, Christopher: "Acquisition and Processing of Disk Images to Further Archival Goals", **Archiving 2012**, Springfield[ABD], Society for Imaging Science and Technology, 2012, s. 147-152.

Woods, Kam, Lee, Christopher ve Garfinkel, Simon: "Extending Digital Repository Architectures to Support Disk Image Preservation and Access", **Proceedings of the 11th Annual International ACM/IEEE Joint Conference on Digital Libraries**, 13-17 Haziran 2011, Ontario[Kanada], ACM, 2011, s. 57-66.

Woods, Kam, Lee, Christopher ve Misra, Sunitha: "Automated Analysis and Visualization of Disk Images and File Systems for Preservation", **Archiving 2013**, Washington[ABD], Society for Imaging Science and Technology, 2013, s. 239-244.

Yalçınkaya, Bahattin: "Belge Yönetim Sistemlerinde ve Süreçlerinde Risk Tanımları", **Arşiv Dünyası**, No: 16-17, 2014, s. 16-24.

Yalçınkaya, Bahattin: "E-Arşiv Uygulamalarına Teknolojik ve Altyapı Kapsamında Yaklaşımlar: Güvenilir E-Arşivleme Koşulları Yol Haritası", ed.: Fahrettin Özdemirci vd., **e-BEYAS 2015 Sempozyumu: Kurumsal Belleklerin Geleceği, Dijitalleştirme-Elektronik Arşiv-Elektronik Belge Yönetimi**, 21-22 Ekim Ankara, Ankara, Ankara Üniversitesi, 2012, s. 221-234.

Yalçınkaya, Bahattin, Gedikli, Muhammet Emin ve Cibaroğlu, Mehmet Oytun: "Elektronik Belge Yönetim Sisteminde Log Analizi: İstatistiksel Bir Değerlendirme", **Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ**, ed.: Bahattin Yalçınkaya vd., Ankara, Ankara Üniversitesi, 2019, s. 61-77.

Yardım, Ertan: "Medeni Usul Hukuku Çerçevesinde Güvenli Elektronik İmzalı Belgelerin Delil Niteliği ve Unsurları", **Prof.Dr. Mustafa Dural'a Armağan**, ed.: Tufan Öğüz, İstanbul, Seçkin Yayıncılık, 2013, s. 1290-1315.

Yaşa, Ayşe Atılgan ve Tüğen, Kamil: "İlişkisel Sözleşmeler Bağlamında Vatandaş Güveni ve Devlet Bütçesi", **Yönetim ve Ekonomi**, C. 26, No: 3, 2019, s. 745-762.

Yeo, Geoffrey: "Bringing Things Together: Aggregate Records in a Digital Age", **Archivaria**, No: 74, 2012, s. 43-91.

Yeo, Geoffrey: "Introduction", **Managing Records in Global Financial Markets: Ensuring ompliance and Mitigating Risk**, ed.: Lynn Colemann vd., Londra[Birleşik Krallık], Facet Publishing, 2011, s. xix-xxix.

Yeo, Geoffrey: "Trust and Context in Cyberpsace", **Archives and Records**, C. 34, No: 2, 2013, s. 214-234.

Yılmaz, Mustafa: "Elektronik İmzalı Belgelerin Karşılaştırmalı Hukukta ve İdari Yargılama Hukukunda Delil Niteliği", **Marmara Üniversitesi Hukuk Fakültesi Araştırmaları Dergisi**, C. 22, No: 3, 2016, s. 3413-3464.

Zhang, Guigang vd.: "A New Electronic Records Security Model for Long-term Preservation**", 10th Web Information System and Application Conference**, 10-15 Kasım 2013, ed.: Bin Li, Ruixuan Li ve Derong Shen, Yangzhou[Çin], yayımcı yok, 2013, s. 191-194.

Zhang, Jane: "Original Order in Digital Archives", **Archivaria**, No: 74, 2012, s. 167-193.

Zierau, Eld: "The Rescue of Danish Bits: A Case Study of the Rescue of Bits and How the Digital Preservation Community Supported it", **15. International Conference on Digital Preservation**, 24-27 Eylül 2018, ed.: Megan Potterbusch vd., Boston[ABD], yayımcı yok, 2018, (Çevrimiçi) https:// osf. io/ 2eazn, 1 Ocak 2020.

Zikratov, Igor vd.: "Ensuring Data Integrity Using Blockchain Technology", **20. Conference of Open Innovation Association**, ed.: Sergey Palandin, Saint Petersburg [Rusya], IEEE, 2017, s. 534–539.

Proje Raporları:

Duranti, Luciana: "Introduction", **The Long-term Preservation of Authentic Electronic Records: Findings of the International Research on Permanent Authentic Electronic Records [INTERPARES] Project**, (Çevrimiçi) http:// www. interpares. org/ book/ interpares_ book_c_intro.pdf, 28 Aralık 2020.

Flores, Daniel, Lacombe, Claudia ve Lemieux, Victoria L.: **Real Estate Transaction Recording in the Blockchain in Brazil**, (Çevrimiçi) http:// blogs. ubc. ca/ recordsinthechain/ files/ 2018/ 01/ RCPLM- 01- Case-Study- 1_ v14 _ English_ Final. pdf, 1 Nisan 2020.

Lynch, Clifford: **Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust**, Alexandria[ABD], CLIR, 2000, (Çevrimiçi) https :// www. clir. org/ pubs/ reports/ pub92/ lynch/, 31 Mayıs 2020.

MacNeil, Heather vd.: "Authenticity Task Force Report", **The Long-term Preservation of Authentic Electronic Records: Findings of the INTERPARES Project**, (Çevrimiçi) http:// www. interpares. org/ book/ interpares_book_d_part1.pdf, 28 Aralık 2020.

MacNeil, Heather vd.: "Requirements for Assessing and Maintaining the Authenticity of Electronic Records", **The Long-term Preservation of Authentic Electronic Records: Findings of the INTERPARES Project**, (Çevrimiçi) http:// www. interpares. org/ book/ interpares_book_k_app02.pdf, 28 Aralık 2020.

MacNeil, Heather vd.: "Template for Analysis", **The Long-term Preservation of Authentic Electronic Records: Findings of the INTERPARES Project**, (Çevrimiçi) http:// www. interpares. org/ book/ interpares_book_j_app01.pdf, 28 Aralık 2020.

INTERPARES: **INTERPARES 2: Experiential, Interactive and Dynamic Records**, ed.: Luciana Duranti ve Randy Preston, 2008, (Çevrimiçi) http:// www. interpares. org/ ip2/ display_ file. cfm ?doc =ip2 _ book_ complete. pdf, 28 Aralık 2020.

Külcü, Özgür: **INTERPARES 3 Kurumsal Bilgi Sistemleri İçerisinde Belge Yönetimi: Türkiye'deki Kamu Üniversitelerinde Gerçekleştirilen Uygulamalara Yönelik Bir Durum Analizi**, 1011 TÜBİTAK Projesi, Proje No: 109K518, 2014, Ankara.

Lemieux, Victoria L.: **One Step Forward, Two Steps Backward? Does EGovernment make Governments in Developing Countries more Transparent and Accountable?**, Washington[ABD], 2016, (Çevrimiçi) https :// openknowledge. worldbank. org/handle/10986/23647, 10 Ağustos 2020.

Lemieux, Victoria L.: **Blockchain Technology for Recordkeeping Help or Hype ? Blockchain Technology for Recordkeeping**, Montreal[Kanada], Social Sciences and Humanities Research Council of Canada, 2016.

Pew Research Center: **Public Trust in Government: 1958-2021**, (Çevrimiçi) https: // www. pewresearch. org/ politics/ 2021/ 05/ 17/ public-trust-in-government-1958-2021/, 20 Mayıs 2020.

Stancic, Hrvoje: **Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records**, 2018, (Çevrimiçi) https:// interparestrust. org / assets / public / dissemination / TRUSTER Preservation Model(EU31)-Finalreportv_1_3.pdf, 12 Nisan 2020.

Tezler:

Alır, Gülten: "E-Türkiye Uygulamaları: Elektronik Belge Yönetimi ve Üst Veri", Yayınlanmamış Doktora Tezi, Ankara, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı, 2008.

Arısoy, Yunus Emre: "Türkiye'de Elektronik Belge Yönetiminde Milli Arşiv Politikalarının Geliştirilmesi", Yayınlanmamış Doktora Tezi, Ankara, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı, 2018.

Aydoğan, Hakan: "Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri", Yayınlanmamış Yüksek Lisans Tezi, Ankara, Polis Akademisi, 2009.

Biricikoğlu, Hale: "Yerel Yönetimlerde Hesap Verebilirlik (Marmara Bölgesi Örneği)", Yayınlanmamış Doktora Tezi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı, 2011.

Bushey, Jessica: "The Archival Trustworthiness of Digital Photographs in Social Media Platforms", Yayınlanmamış Doktora Tezi, British Columbia Üniversitesi[Kanada], 2016.

Çakmak, Tolga: "Türkiye'de Kültürel Bellek Kurumlarında Dijitalleştirme ve Dijital Koruma Politikaları: Bir Model Önerisi", Yayınlanmamış Doktora Tezi, Ankara, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı, 2016.

Dündar, Meltem: "İngiliz ve Türk Ceza Muhakemesi Hukuklarında Hukuka Aykırı Deliller", Yayınlanmamış Doktora Tezi, İstanbul, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, 2014.

Erek, Mustafa Salim: "Merkez Bankası Bağımsızlığı ve Mali Güvenilirlik İlişkisi: Gelişmekte Olan Ülkeler Örneği", Yayınlanmamış Doktora Tezi, İstanbul, Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü Bankacılık Anabilim Dalı, 2019.

Ergün, Tamer: "Security Analysis of Electronic Signature Applications and Test Suite Study", Yayınlanmamış Doktora Tezi, Ankara, Ortadoğu Teknik Üniversitesi, 2013.

Erturgut, Mine: "Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi", Yayınlanmamış Doktora Tezi, İzmir, Dokuz Eylül Üniversitesi Özel Hukuk Anabilim Dalı, 2004.

Gümüşkaya, Gamze: "Vergi Hukukunda İspat", Yayınlanmamış Doktora Tezi, İstanbul, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Mali Hukuk Anabilim Dalı, 2015.

Güralp, Ayşe Gülin: "Anglo-Amerikan ve Kıta Avrupası Medeni Yargılama Sistemlerindeki Yeni Gelişmeler ve Türk Hukuku ile Karşılaştırılması", Yayınlanmamış Doktora Tezi, İzmir, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, 2010.

Hay-Gibson, Naomi: "Risk and Records Management: Investigating Risk and Risk Management in the Context of Records and Information Management in the Electronic Environment", Yayınlanmamış Doktora Tezi, Northumbria University, Newcastle[Birleşik Krallık], 2011.

Kasap, Şenol: "F-16 Uçaklarında Uçuş Güvenliğinin Güvenilirlik Mühendisliği ile Araştırılması", Yayınlanmamış Doktora Tezi, Eskişehir, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü İşletme Sayısal Yöntemler Anabilim Dalı, 2020.

Kavak, Yalçın: "Borçlar Hukukunda Yazılı Şekil", Yayınlanmamış Doktora Tezi, İstanbul, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, 2015.

Köküsarı, İsmail: "Anayasa Hukukunda Hukuki Güvenlik İlkesi", Yayınlanmamış Doktora Tezi, Ankara, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, 2020.

Pamuk, Sevil: "Türkiye'de Noter Belgelerinin Form Özellikleri", Yayınlanmamış Doktora Tezi, İstanbul, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı, 2014.

Rogers, Corinne: "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice", Yayınlanmamış Doktora Tezi, University of British Columbia[Kanada], 2015.

Yalçınkaya, Bahattin: "E-devlet Üstveri Standardının Oluşturulması ve Türkiye için Modellenmesi", Yayınlanmamış Doktora Tezi, İstanbul, Marmara Üniversitesi Türkiyat Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı, 2014.

Yalçınkaya, Mazlum: "Rekabet Hukuku Uygulamaları apsamında Elektronik Delil", Yayınlanmamış Uzmanlık Tezi, Rekabet Kurumu, Ankara, 2015, (Çevrimiçi) https:// www. rekabet. gov. tr/ Dosya/ uzmanlik-tezleri/ 143-pdf, 5 Mart 2020.

Yılmaz, Elif: "Hukuki Güvenlik İlkesinin Bir Gereği Olarak Vergi Hukukunda Geriye Yürümezlik İlkesi", Yayınlanmamış Doktora Tezi, Ankara, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, 2014.

Web Sayfaları:

Alliance Permanent Access to the Records of Science in Europe Network [APARSEN]: **APARSEN Web Sitesi**, (Çevrimiçi) http :// www. alliancepermanentaccess. org, 26 Temmuz 2020.

Archivematica: **Archivematica Web Sitesi**, (Çevrimiçi) https:// www. archivematica. org, 1 Ağustos 2020.

BitCurator: **BitCurator Web Sitesi**, (Çevrimiçi) https://bitcurator.net/, 1 Ağustos 2020.

Başçi, Gülen Çelebi: **Sertifika Geçerlilik Kontrolündeki Sorunların Giderilmesi**, (Çevrimiçi) https:// kamusm. bilgem. tubitak. gov. tr/ dosyalar/ makaleler/ Sertifika %20 Gecerlilik %20 Kontrolundeki %20 Sorunlarin %20Giderilmesi.pdf, 30 Nisan 2020.

BDO Consulting: **Inside E-Discovery: The State of E-Discovery According to Corporate Counsel,** 2015, (Çevrimiçi) https:// www. bdo. com/ getattachment/ Insights/ Consulting/ Inside-E-Discovery/ 2015BDOC-E-Discovery-report-WEB.pdf.aspx, 5 Mart 2020.

Blake: **Blake Web Sitesi**, (Çevrimiçi) https:// www. blake2. net/, 5 Haziran 2020.

CBDDO: **Hizmet Envanteri Yönetim Sistemi Web Sayfası**, (Çevrimiçi) https :// envanter. kaysis. gov. tr/, 30 Nisan 2020.

Cerf, Vint: **ASCII Format for Network Interchange,** yayım yeri yok, 1969, (Çevrimiçi) https :// www. rfc-editor. org/rfc/rfc20.pdf, 29 Mart 2020.

Connecting Europe Facility [CEF]: **eSignature Documentation**, (Çevrimiçi) https:// ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Introduction+to+e-signature, 12 Mayıs 2020.

Crane, Tom: **Baffled by Archives: Part One**, (Çevrimiçi) https :// blog. nationalarchives. gov. uk/ baffled-by-archives-part-one/, 24 Mart 2020.

Cultural, Artistic and Scientific Knowledge for Preservation, Access and Retrieval [CASPAR]: **CASPAR Web Sitesi**, (Çevrimiçi) http :// casparpreserves. digitalpreserve. info, 26 Temmuz 2020.

Çakır, Nurullah: **SQL Server ACID Kuralları**, (Çevrimiçi) http :// www. veritabani. gen. tr/ 2017/ 10/ 18/sql-server-acid-kurallari/, 8 Nisan 2020.

Deloitte: **Blokzincir Potansiyelinin Keşfi: 2018 Yılı Türkiye Blokzincir Araştırması**, (Çevrimiçi) https:// www2. deloitte. com/ content/ dam/ Deloitte/ tr/Documents/consulting/blokzincir-potansiyelinin-kesfi.pdf, 15 Nisan 2020.

E-ARK: **Common Specification for Information Packages**, (Çevrimiçi) https:// earkcsip.dilcis.eu/, 24 Mart 2020.

Electronic Resource Preservation and Access Network[ERPANET]: **ERPANET Web Sitesi**, (Çevrimiçi) https:// www. erpanet. org, 26 Temmuz 2020.

GitHub: **GitHub Web Sitesi**, (Çevrimiçi) https:// github. com/, 5 Haziran 2020.

Gollins, Tim: **Twitter**, 3 Temmuz 2018, (Çevrimiçi) https:// twitter. com/ timgollins/ status/ 1014084416526802944?s=21, 6 Mart 2020.

Google: **Google Code Web Sitesi**, (Çevrimiçi) https:// code. google.com/archive/, 5 Haziran 2020.

Green, Alex: **Trustworthy Technology: The Future of Digital Archives?**, 2018, (Çevrimiçi) https:// blog. nationalarchives. gov. uk/ trustworthy-technology-future-digital-archives, 1 Nisan 2020.

Illinous Üniversitesi: **Metadata Offer New Knowledge (MONK) Projesi Web Sayfası**, (Çevrimiçi) http:// monk. library. illinois. edu/, 31 Aralık 2019.

INTERPARES: **Terminology Web Sayfası**, (Çevrimiçi) https :// interparestrust. org/ terminology/ term/ trustworthiness, 27 Nisan 2020.

International Records Management Trust [IRMT]: **Records Management Capacity Assesment System: User Guide**, Version 1.4., 2005, (Çevrimiçi) https:// www. nationalarchives. gov. uk/ rmcas/ documentation/ rmcas_user_guide.pdf, 26 Mayıs 2020.

J. Young, Lauren: **Data Reawakening: The "File Not Found" Series: Part 3 of 3**, (Çevrimiçi) https:// apps. sciencefriday. com/ data/ reawakening. html, 4 Mart 2020.

KAMU SM: **E-İmza Teknolojileri Test SuitWeb Sayfası**, (Çevrimiçi), https :// yazilim. kamusm. gov. tr/eit-wiki/ doku.php?id=ana_sayfa, 23 Eylül 2020.

KAMU SM: **Nitelikli Elektronik Sertifika İlkeleri**, 2020, (Çevrimiçi) http:// www. kamusm. gov. tr/ BilgiDeposu/ KSM_NES_SI/KSM_NES_SI.pdf, 15 Mart 2020.

KAMU SM: **Temel Kavramlar**, (Çevrimiçi) https:// kamusm. bilgem. tubitak. gov. tr/ dokumanlar/ belgeler/ kitaplar/temel_kavramlar.jsp, 24 Şubat 2020.

Kortun, Vasıf: **Bu Bize Ne Anlatıyor**, (Çevrimiçi) https:// www. unlimitedrag. com/ post/ bu-bize-ne-anlat%C4%B1yor, 26 Şubat 2020.

Kussmann, Carol: "Checksum Verification Tools", **Practical E-Records: Software and Tools for Archivists**, (Çevrimiçi) https:// e-records. chrisprom. com/ checksum-verification-tools, 16 Ekim 2019.

Long Term Records Management Project: **Recommended Practices**, (Çevrimiçi) http:// research. dnv. com/ LongRec/ ResearchResults/ Pages/ RecommendedPractices.html, 28 Ocak 2020.

Metz, Cade: An Infusion of AI Makes Google Translate More Powerful Than Ever, **Wired**, (Çevrimiçi) https:// www. wired. com/ 2016/ 09/ google-claims-ai-breakthrough-machine-translation, 29 Eylül 2020.

Minnesota State Archives: **Center for Archival Resources on Legislatures**, (Çevrimiçi) http:// www. mnhs. org/ preserve/ records/ legislativerecords/ carol/ preservation. php, 16 Ekim 2019.

Nakamoto, Satoshi: **Bitcoin: A Peer-to-Peer Electronic Cash System**, 2008, (Çevrimiçi) https:// bitcoin. org/ bitcoin.pdf, 16 Haziran 2019.

National Archives of Australia: **Legislation, Policies, Standards and Advice**, (Çevrimiçi) http:// www. naa. gov. au/ information-management/ information-governance/ legislation-standards/ index.aspx, 14 Ekim 2020.

National Digital Stewardship Alliance [NDSA]: **2014 National Agenda for Digital Stewardship**, (Çevrimiçi) https:// www. digitalpreservation. gov/ documents/ 2014NationalAgenda.pdf, 5 Mart 2020.

Northwestern Üniversitesi: **Wordhoard Projesi Web Sayfası**, (Çevrimiçi) http :// wordhoard. northwestern. edu/ userman/ index.html, 31 Aralık 2019.

OECD: **Trust in Government Web Sayfası**, (Çevrimiçi) https :// www. oecd. org/ gov/ trust-in-government. htm, 20 Mayıs 2020.

Oxford Common File Layout (OCFL): **OCFL Web Sitesi**, (Çevrimiçi) https://ocfl.io/, 1 Mayıs 2020.

Qian, Jiahe, Jiang, Yanming ve von Davier, Alina A.: **Weighting Test Samples in IRT Linking and Equating: Toward an Improved Sampling Design for Complex Equating**, Educational Testing Service, Princeton[ABD], 2013, (Çevrimiçi) https :// origin-www. ets. org/ Media/ Research/ pdf/RR-13-39.pdf, 24 Haziran 2020.

Queensland Government Contract Services Department of Public Works: **Guidance on Evaluating Tenders Using Price Quality Method**, (Çevrimiçi) https:// www. hpw. qld. gov. au/ __data/ assets/ pdf_ file/ 0013/ 3334/ pricequalitymethod.pdf, 24 Haziran 2020.

Perez, Eduardo del Valle: A Story of Unexpected Data Loss and How to Do Digital Preservation", Preservation and Archiving Special Interest Group [PASIG], 11-13 Eylül 2017, Oxford, Birleşik Krallık, (Çevrimiçi) https:// pasig. figshare. com/ articles/ presentation/ Sharing_ my_loss_to_protect_your_data_A_story_of_unexpected _data_loss_and_how_to_do_real_preservation/5415046/ 1, 15 Aralık 2020.

Perseus Digital Library: **Perseus Digital Library Web Sayfası**, (Çevrimiçi) https :// www. perseus. tufts. edu/ hopper/, 31 Aralık 2019.

Phillips, Larry ve Stock, Adrian: **Use of Multi-Criteria Analysis in Air Quality Policy**, Department for Environment, Food and Rural Affairs, 2003, (Çevrimiçi) https: // uk-air. defra. gov. uk/ assets/ documents/ reports/ cat09/ 0711231556_MCDA_Final.pdf, 24 Haziran 2020.

Preservation and Long-Term Access Through Networked Services [PLANETS]: **PLANETS Web Sitesi**, (Çevrimiçi) https:// www. planets-project. eu, 26 Temmuz 2020.

Rosenthal, David: **Do You Need a Blockchain,** 2018, (Çevrimiçi) https :// blog. dshr. org/ 2018/ 02/ do-you-need-blockchain.htm, 1 Nisan 2020.

Sayarlıoğlu, Ahmet: **Herkes için Blok-zincir**, (Çevrimiçi) https :// medium. com/ @ahmet.sayarlioglu/herkes-i%C3%A7in-blok-zincir-blokchain-1c85eb3a0bee, 30 Mart 2020.

Selçuk, Gonca Hülya: **E-Devlet Uygulamaları için Elektronik İmza Formatları**, (Çevrimiçi) http :// www. kamusm. gov. tr/ dosyalar/makaleler/EDevletUygulamalariIcinElektronikImzaFormatlari.pdf, 29 Şubat 2020.

Shattered: **Shattered Web Sitesi**, (Çevrimiçi) https:// shattered. io/, 29 Şubat 2020.

Software Preservation Network: **Emulation-as-a Service Infrastructure**, (Çevrimiçi) https:// www. softwarepreservationnetwork. org/ eaasi/, 29 Mart 2020.

Stabilize: **Stabilize Web Sitesi**, (Çevrimiçi) https:// www. stabilize. app/, 5 Haziran 2020.

SourceForge: **SourceForge Web Sitesi**, (Çevrimiçi) https:// sourceforge. net/, 5 Haziran 2020.

Tapu ve Kadastro Genel Müdürlüğü: **Tapu Sicili Uygulamaları**, 2014, (Çevrimiçi) https:// www. tkgm. gov. tr/ sites/ default/ files/ icerik/ekleri/tapu_sicili_uygulamari_2014_0_0.pdf, 9 Nisan 2020.

The BagIt File Packaging Format: **The BagIt File Packaging Format Web Sitesi**, (Çevrimiçi) https :// tools. ietf. org/ html/ draft-kunze-bagit-17, 1 Mayıs 2020.

The National Archives [TNA]: **Managing Digital Contuinity**, 2017, (Çevrimiçi) https :// nationalarchives. gov. uk/ documents/ information-management/managing-digital-continuity.pdf, 8 Aralık 2020.

TNA: **Managing Digital Contunity Loss**, 2017, (Çevrimiçi) https: // www. nationalarchives. gov. uk/documents/information-management/ managing-digital-continuity-los.pdf, 4 Mart 2020.

TNA: **Mapping the Technical Dependencies of Information Assets**, 2017, (Çevrimiçi) https :// www. nationalarchives. gov. uk/ documents/ information-management/mapping-technical-dependencies.pdf, 8 Aralık 2020.

TNA: **Migrating Information between Records Management Systems**, 2017, (Çevrimiçi) https :// nationalarchives. gov. uk/ documents/ information-management/ edrms.pdf, 5 Mart 2020.

TNA: **Risk Assessment Handbook**, 2017, (Çevrimiçi) https:// www. nationalarchives. gov. uk/ documents/ information-management/ risk-assessment-handbook. pdf, 6 Mart 2020.

TNA: **Technical Discovery: Project Alpha**, (Çevrimiçi) https:// blog. nationalarchives. gov. uk/ technical-discovery-project-alpha/, 24 Mart 2020.

TNA: **Understanding Digital Contunity**, 2017, (Çevrimiçi) https:// www. nationalarchives. gov. uk/ documents/ information-management/understanding-digital-continuity.pdf, 5 Mart 2020.

TNA: **Understanding Digital Contunity Loss**, 2017, (Çevrimiçi) https :// www. nationalarchives. gov. uk/ documents/information-management/understanding digital-continuity. pdf, 4 Mart 2020.

The National Electronic Commerce Coordinating Council: **Creating and Maintaining Proper Systems for Electronic Record Keeping**, 2002, (Çevrimiçi) https :// www. ctg. albany. edu/ publications/ reports/ proper_systems/ proper_systems.pdf, 4 Mart 2020.

Thomson**,** Lucy L: **Admissibility of Electronic Documentation as Evidence in U.S. Courts**, 2011, (Çevrimiçi) http:// www. crl. edu/ sites/ default/ files/ d6/ attachments/ pages/Thomson-E-evidence-report.pdf, 14 Ekim 2018.

Türkiye Radyo Televizyon Kurumu (TRT) 2: **Levent Erden: Anjelika Akbar ile Sesler**, (Çevrimiçi) https :// www. facebook. com/ watch/ ?v = 556779264910717, 18 Şubat 2020.

TÜBİTAK Ulusal Akademik Ağ ve Bilgi Merkezi: **Araştırma Verileri Yönetimi Eğitim Portalı**, (Çevrimiçi) https:// acikveri. ulakbim. gov. tr/ acik-veri-acik-bilim/bolum-3-veri-isleme/3-4-verinin-anonimlestirilmesi, 24 Haziran 2020.

UNESCO: **Software Heritage Web Sitesi**, (Çevrimiçi) https :// www. softwareheritage. org/, 23 Mayıs 2020.

UNESCO: **Software Heritage Web Sitesi**, (Çevrimiçi) https :// www. softwareheritage. org/ 2016/ 07/ 21/ gitorious-retrieved/, 5 Haziran 2020.

VeraPDF: **VeraPDF Web Sitesi**, (Çevrimiçi) https://verapdf.org, 20 Şubat 2020.

Williams, Kim: **Twitter**, 26 Temmuz 2018, (Çevrimiçi) https :// twitter. com/ thelibrarykim/ status/ 1022280871259168768, 6 Mart 2020.

Görüşmeler:

Antwerp Üniversitesi öğretim üyesi Dr. Thorsten Ries ile 13 Şubat 2020 tarihinde yapılan görüşme.

Bursa Uludağ Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyesi Prof. Dr. Ahmet Emir Dirik ile 5 Aralık 2017 tarihinde yapılan görüşme.

INTERPARES Direktörü Luciana Duranti ile 3 Eylül 2018 tarihinde yapılan görüşme.

Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümü Araştırma Görevlisi Emin Gedikli ile 18 Nisan 2019 tarihinde yapılan görüşme.

Yale Üniversitesi Kütüphanesi Sayısal Koruma Müdürü Euan Cochrane ile 30 Ağustos 2018 tarihinde yapılan görüşme.

EKLER

EK 1. ETİK KURUL İZİNLERİ

Tarih ve Sayı: 03/03/2020-43404

T.C.
İSTANBUL ÜNİVERSİTESİ REKTÖRLÜĞÜ
Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu Başkanlığı

Sayı :35980450-663.05-
Konu :Özhan SAĞLIK

Sayın Özhan SAĞLIK

İlgi :17/01/2020 tarihli, 3829 sayılı yazı

Sorumlu araştırıcılığını üstlendiğiniz 2020/16 dosya numaralı "Arşivlenen Elektronik Belgelerin Delil Değerinin Güvenilirlik Açısından İncelenmesi" başlıklı çalışma Kurulumuzun 03.02.2020 tarih 02 sayılı toplantısında görüşülerek etik yönden uygun bulunmuş olup, karar ekte sunulmuştur.

Bilgilerinizi rica ederim.

e-İmzalı
Prof. Dr. N. Tolga SARUÇ
Başkan

EK :
Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu Kararı

Doğrulamak İçin:http://194.27.128.66/envision.Sorgula/belgedogrulama.aspx?V=BE6EHHNZP
Ayrıntılı bilgi için irtibat : Süleyman ARIK Dahili : 10689
İstanbul Üniversitesi Merkez Kampüsü
34452 Beyazıt/Fatih-İstanbul
Tel : 0212 440 20 89 Faks : 0212 440 20 88
e-posta : sosyalbilimleretikkurul@istanbul.edu.tr Elektronik Ağ : www.istanbul.edu.tr

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL VE BEŞERİ BİLİMLER
ARAŞTIRMALARI ETİK KURULU BAŞKANLIĞI

İlgili makama,

İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Bilgi ve Belge Yönetimi Ana Bilim Dalı Doktora Öğrencisi **Özhan SAĞLIK** "Arşivlenen Elektronik Belgelerin Delil Değerinin Güvenilirlik Açısından İncelenmesi" başlıklı, **2020/16** dosya numaralı 17.01.2020 tarih ve **3839** sayılı başvurusu ile İ.Ü. Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu'na başvurmuştur. 03.02.2020 tarihinde gerçekleşen inceleme sonucunda, adı geçen çalışmada etik açıdan bir sorun olmadığına oybirliği ile karar verilmiştir. Gereğini bilgilerinize saygılarımızla sunarız.

Unvanı / Adı / Soyadı	Kurumu	Araştırma ile ilişki	Karar	İmza
Prof. Dr. Naci Tolga SARUÇ (Başkan)	İktisat Fakültesi	E ☐ H ☑	☑ Onay ☐ Katılmadı ☐ Ret ☐ M.Katılmadı	
Doç. Dr. Çiğdem Börke TUNALI (Başkan Yardımcısı)	İktisat Fakültesi	E ☐ H ☑	☑ Onay ☐ Katılmadı ☐ Ret ☐ M.Katılmadı	
Prof. Dr. Eray YURTSEVEN (Başkan Yardımcısı)	İstanbul Tıp Fakültesi	E ☐ H ☑	☑ Onay ☐ Katılmadı ☐ Ret ☐ M.Katılmadı	
Prof. Dr. Aydın TOPALOĞLU	İlahiyat Fakültesi	E ☐ H ☑	☑ Onay ☐ Katılmadı ☐ Ret ☐ M.Katılmadı	
Prof. Dr. Yasemin IŞIKTAÇ	Hukuk Fakültesi	E ☐ H ☐	☐ Onay ☐ Katılmadı ☐ Ret ☑ M.Katılmadı	
Prof. Dr. Selahattin KARABINAR	İktisat Fakültesi	E ☐ H ☑	☑ Onay ☐ Katılmadı ☐ Ret ☐ M.Katılmadı	
Prof. Dr. Seyhan NİŞEL	İşletme Fakültesi	E ☐ H ☐	☐ Onay ☐ Katılmadı ☐ Ret ☑ M.Katılmadı	
Prof. Dr. Mustafa Hamdi SAYAR	Edebiyat Fakültesi	E ☐ H ☑	☑ Onay ☐ Katılmadı ☐ Ret ☐ M.Katılmadı	
Prof. Dr. Selim YAZICI	Siyasal Bilgiler Fakültesi	E ☐ H ☑	☑ Onay ☐ Katılmadı ☐ Ret ☐ M.Katılmadı	
Prof. Dr. Rasim İlker GÖKBULUT	Ulaştırma ve Lojistik Fakültesi	E ☐ H ☑	☑ Onay ☐ Katılmadı ☐ Ret ☐ M.Katılmadı	
Prof. Dr. Enes KABAKCI	Edebiyat Fakültesi	E ☐ H ☑	☑ Onay ☐ Katılmadı ☐ Ret ☐ M.Katılmadı	
Doç. Dr. Hanife Özlem SERTEL BERK	Edebiyat Fakültesi	E ☐ H ☐	☐ Onay ☐ Katılmadı ☐ Ret ☑ M.Katılmadı	
Doç. Dr. Haluk ZÜLFİKAR	İktisat Fakültesi	E ☐ H ☑	☑ Onay ☐ Katılmadı ☐ Ret ☐ M.Katılmadı	
Doç. Dr. Şerife Sema KARAKELLE	Edebiyat Fakültesi	E ☐ H ☐	☐ Onay ☐ Katılmadı ☐ Ret ☑ M.Katılmadı	
Dr. Öğr. Üyesi Göklem TEKDEMİR YURTDAŞ	Edebiyat Fakültesi	E ☐ H ☐	☐ Onay ☐ Katılmadı ☐ Ret ☑ M.Katılmadı	
Dr. Öğr. Üyesi Bengi PİRİM DÜŞGÖR	Edebiyat Fakültesi	E ☐ H ☑	☑ Onay ☐ Katılmadı ☐ Ret ☐ M.Katılmadı	
Dr. Öğr. Üyesi Ayşe Elif YAVUZ SEVER	Edebiyat Fakültesi	E ☐ H ☐	☐ Onay ☐ Katılmadı ☐ Ret ☑ M.Katılmadı	

Tarih ve Sayı: 26/06/2020-71477

BECFR61PN

T.C.
İSTANBUL ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü

Sayı :44850192-302.14.01-
Konu :Tez Başlığı Değişikliği

Özhan SAĞLIK

Enstitümüz Yönetim Kurulunun 25.06.2020 tarihli ve 20 sayılı toplantısının 45. maddesi aşağıya çıkartılmıştır.

Bilgilerinizi ve gereğini rica ederim.

e-İmzalı
Dr. Öğr. Üyesi Şerif Emre GÖKÇAY
Enstitü Müdür Yardımcısı

Madde **Adı Soyadı**	**45** **Özhan SAĞLIK**
Öğrenci No	**2502150019**
Anabilim Dalı	**Bilgi ve Belge Yönetimi**
Programı	**Doktora**
Gelen Evrak; Tarih/Sayı	**23/06/2020-28206**
Talep	Eski tez başlığı: "Arşivlenen Elektronik Belgelerin Delil Değerinin Güvenilirlik Açısından İncelenmesi" Yeni tez başlığı: "Elektronik Belge Yönetimi Uygulamalarındaki Koşullar Işığında E-İmzalı Belgelerin Delil Değerinin Arşivsel Güvenilirlik Açısından İncelenmesi" şeklinde değiştirilmesi teklifi.
Enstitü Yönetim Kurulu Kararı	Tez başlığının "Elektronik Belge Yönetimi Uygulamalarındaki Koşullar Işığında E-İmzalı Belgelerin Delil Değerinin Arşivsel Güvenilirlik Açısından İncelenmesi" şeklinde değiştirilmesi teklifinin kabulüne oybirliği ile karar verildi.

DAĞITIM

Gereği:
Özhan SAĞLIK
Sayın Prof. Dr. Niyazi ÇİÇEK

Bilgi:
Edebiyat Fakültesi Dekanlığı
Sayın Prof. Dr. Ümit KONYA

Doğrulamak İçin:http://194.27.128.66/envision.Sorgula/belgedogrulama.aspx?V=BECFR61PN
Ayrıntılı bilgi için irtibat : Zübeyde ŞAHİN Dahili : 14243
Besim Ömerpaşa Cad. Devlet Arşivleri Binası.A blok No:39 34119
Fatih/Vezneciler/İstanbul
Tel : (212) 440 00 00 Faks : (212) 440 03 04
e-posta : sbe@istanbul.edu.tr Elektronik Ağ : www.istanbul.edu.tr

Tarih ve Sayı: 23/07/2020-83396

BEL9RC2FS

T.C.
İSTANBUL ÜNİVERSİTESİ REKTÖRLÜĞÜ
Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu Başkanlığı

Sayı :35980450-663.05-
Konu :Özhan SAĞLIK

Sayın Özhan SAĞLIK

İlgi :29.06.2020 tarihli, 29078 sayılı yazı.

Sorumlu araştırıcılığını üstlendiğiniz 2020/16 dosya numaralı "Elektronik Belge Yönetimi Uygulamalarındaki Koşullar Işığında E-imzalı Belgelerin Delil Değerinin Arşivsel Güvenilirlik Açısından İncelenmesi" başlıklı çalışma Kurulumuzun 10.07.2020 tarih 08 sayılı toplantısında görüşülerek etik yönden uygun bulunmuş olup, karar ekte sunulmuştur.

Bilgilerinizi rica ederim.

e-İmzalı
Prof. Dr. N. Tolga SARUÇ
Başkan

EK :
Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu Kararı

Doğrulamak İçin:http://194.27.128.66/envision.Sorgula/belgedogrulama.aspx?V=BEL9RC2FS
Ayrıntılı bilgi için irtibat : Gülcan ÇAKIR (Süleyman ARIK Vekaletiyle) Dahili : 11818
İstanbul Üniversitesi Merkez Kampüsü
34452 Beyazıt/Fatih-İstanbul
Tel : 0212 440 20 89 Faks : 0212 440 20 88
e-posta : sosyalbilimleretikkurul@istanbul.edu.tr Elektronik Ağ : www.istanbul.edu.tr

Tarih ve Sayı: 10/07/2020-116422

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL VE BEŞERİ BİLİMLER
ARAŞTIRMALARI ETİK KURULU BAŞKANLIĞI

İlgili makama,

İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Bilgi ve Belge Yönetimi Ana Bilim Dalı Doktora Öğrencisi **Özhan SAĞLIK** "Elektronik Belge Yönetimi Uygulamalarındaki Koşullar Işığında E-İmzalı Belgelerin Delil Değerinin Arşivsel Güvenilirlik Açısından İncelenmesi" başlıklı, **2020/16** dosya numaralı 29.06.2020 tarih ve **29078** sayılı başvurusu ile İ.Ü. Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu'na başvurmuştur. 10.07.2020 tarihinde gerçekleşen inceleme sonucunda, adı geçen çalışmada etik açıdan bir sorun olmadığına oybirliği ile karar verilmiştir. Gereğini bilgilerinize saygılarımızla sunarız.

Unvanı / Adı / Soyadı	Kurumu	Araştırma ile ilişki	Karar	e-İmza
Prof. Dr. Naci Tolga SARUÇ (Başkan)	İktisat Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Doç. Dr. Çiğdem Börke TUNALI (Başkan Yardımcısı)	İktisat Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Prof. Dr. Eray YURTSEVEN (Başkan Yardımcısı)	İstanbul Tıp Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Prof. Dr. Aydın TOPALOĞLU	İlahiyat Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Prof. Dr. Yasemin IŞIKTAÇ	Hukuk Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Prof. Dr. Selahattin KARABINAR	İktisat Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Prof. Dr. Seyhan NİŞEL	İşletme Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Prof. Dr. Mustafa Hamdi SAYAR	Edebiyat Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Prof. Dr. Selim YAZICI	Siyasal Bilgiler Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Prof. Dr. Rasim İlker GÖKBULUT	Ulaştırma ve Lojistik Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Prof. Dr. Enes KABAKCI	Edebiyat Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Doç. Dr. Hanife Özlem SERTEL BERK	Edebiyat Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Doç. Dr. Haluk ZÜLFİKAR	İktisat Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Doç. Dr. Şerife Sema KARAKELLE	Edebiyat Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Dr. Öğr. Üyesi Göklem TEKDEMİR YURTDAŞ	Edebiyat Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Dr. Öğr. Üyesi Bengi PİRİM DÜŞGÖR	Edebiyat Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	
Dr. Öğr. Üyesi Ayşe Elif YAVUZ SEVER	Edebiyat Fakültesi	E ○ H ○	○ Onay ○ Katılmadı ○ Ret ○ M.Katılmadı	

EK 2. NİTEL ARAŞTIRMA SORULARI

1. E-belgelerin delil değerinin korunmasında üstveriler nasıl rol oynar?
2. E-belgelerin delil değerinin korunması noktasında log kayıtlarından nasıl faydalanılabilir?
3. Devlet Arşivleri, e-belgelerin güvenilirliğinin korunmasında ne gibi yaklaşımlar sergileyebilir?
4. Devlet Arşivlerinin, kurumları belge yönetimi politikası oluşturmak yönünde teşvik ederek bu politikayı denetlemek gibi bir konuma getirilmesi, belgelerin delil değerinin korunmasına katkı sunar mı?
5. Kamunun hizmet sağlayıcıların yedekleme ve log kayıtları oluşturma işlemleri için bir genelge/rehber hazırlaması, belgelerin delil değerinin korunmasında kamuyu duyulan güveni artırır mı?
6. Dosyalama pratikleri ile belgenin delil değeri arasında nasıl bir ilişki vardır?
7. Teknolojik göç sonrasında oluşması muhtemel yeni formattaki belgenin delil değerinin korunduğunu nasıl gösterebiliriz? (Şöyle bir senaryo düşünelim: Bugün elimdeki bir e-belge PDF formatında, 10 sene sonra bu formatı CDF adında bir formata dönüştürmüş olayım ve bu belgeye dayanarak SSK'ya bir dava açayım. SSK, elimdeki belgenin geçerliliğini kabul edecek mi, kabul edecekse e-imza, e-mühür gibi mekanizmaların dışında hangi mekanizmalara ihtiyaç duyabilir)
8. Bir kuruma dışarıdan gelen bir belgenin delil değerinin korunduğunu gösteren mekanizmalar, e-imza ve kurumsal mühürdür. Bu mekanizmaların dışında, arşivciliğin yaşam döngüsündeki süreçlerden neler eklenebilir?
9. E-imza ile zaman damgası altyapısının karşılaşabileceği tehditler neler olabilir?
10. EYP, belgenin delil değerinin korunmasında güçlü bir mekanizma olarak kullanılabilir mi? Bu değerin korunmasını zenginleştirir mi?
11. Seri-dosya-belge hiyerarşisi bozulan ve vaka dosyası konu dosyası ayrımı yapılmayan belgelerin delil vasfının şüphe uyandırabileceğini iddia edebilir miyiz?
12. Risk yönetimi ve belirlenen risklere karşı geliştirilen çözüm önerilerinin uygulanıp uygulanmamasıyla belgelerin delil değerinin korunması arasında bir ilişki kurabilir miyiz?
13. Değerlendirme (Appraisal) ile belgenin delil değerinin korunması arasında bir ilişki kurabilir miyiz?
14. EBYS yazılımların kaynak kodunu korumanın (software preservation) belgelerin delil değerinin korunmasına olumlu bir etkisi olabilir mi?
15. Güncel belgelerle arşive gönderilen belgeleri aynı yerlerde saklamak belgenin delil vasfını tehdit edebilir mi?
16. Belgelerin delil değerinin başarılı bir şekilde korunması için hangi donanım (disk vb.) özellikleri kullanılabilir/kullanılmamalıdır?
17. Belge, Dosya ve seri üstverilerine, hangi kullanıcıların müdahale edebileceği bilgisini bir üstveri alanı olarak eklemek belgelerin delil değerinin korunmasına katkı sağlar mı?

EK 3. NİCEL ARAŞTIRMA SORULARI

Kullandığınız Kaçıncı EBYS?
Sistemi kendiniz mi geliştirdiniz?
Kaç yıldır EBYS kullanıyorsunuz?
Yazılımın TSE uygunluk sertifikası var mı?
KEP kullanıyor musunuz?
UETS kullanıyor musunuz?
EYP kullanıyor musunuz?

1. Belge yönetim sistemine geçerken kurum aşağıdaki prosedürlerden hangilerini gerçekleştirmiştir?
1.1. Kurumun e-belge yönetimi politikasını belirleme
1.2. Kurumun e-arşiv yönetimi politikasını belirleme
1.3. Fonksiyonlar ve iş süreçleri tanımlama ve belgelerle ilişkilendirme
1.4. İş süreçlerine dair dokümantasyon oluşturma
1.5. Form ve şablon oluşturma
1.6. Belge türüne göre oluşturulan şablonlar için bir kontrol numarası verme
1.7. Spesifik üstveri şemaları çıkarma
1.8. Belge profilindeki form özelliklerini (belgedeki kişiler, antet, format, teknolojik özellikler, belgeye işlem safhasında yapılan açıklamalar gibi) tanımlama
1.9. Belgeler ve dosyalar için dosya tasnif planı ve saklama planı hazırlama
1.10. Dosya planına uygun dosyalama sistemi geliştirme
1.11. Kontrollü terminoloji oluşturma
1.12. Felaket kurtarma planı ve yedekleme planı oluşturma

2. Belgenin aşağıdaki form özelliklerinden hangilerini üstverilerde kullanıyorsunuz?
2.1. Sorumlu (Belgeyi üreten kurum)
2.2. Düzenleyen (Belgedeki irade beyanının sahibi)
2.3. Muhatap/Alıcı
2.4. Konu
2.5. Format
2.6. Üretim tarihi
2.7. Gönderim/Alma tarihi (KEP)
2.8. Belge tarihi (Son imzalayıcının imza attığı tarih)

3. Belge profilinde aşağıdaki üstverilerden hangileri bulunmaktadır?
3.1. Belgenin dosyasına kaldırıldığı zaman
3.2. Belgedeki işlemden sorumlu kişi ve birim
3.3. Ait olduğu işlem-dosya-seri-birim
3.4. Dosya kodu
3.5. Belge referans numarası
3.6. Belgeye erişmek için asgari gereksinimler
3.7. Belgenin üretildiği EBYS yazılımı ve versiyon numarası
3.8. Belge yönetimi için kullanılacak algoritmalar (kullanılan EBYS yazılımı algoritmaları ve belgeyi tekrardan üretmek ya da şifreli belgeleri açabilmek için gerekli olan algoritmalar gibi)
3.9. Belge bileşenleri (Üstveri, belgenin ekleri, form elemanları, kontekst (bağlam), içerik, belgenin oluşumunu sağlayan veriler, iş akışları gibi)
3.10. E-imza ve zaman damgası
3.11. Saklama süresi
3.12. Belgeye erişim profilleri
3.13. Belgelerin lokasyonu (Directory)
3.14. Belgeye yapılan açıklama notları (İşlem safhasında (ivedilik durumu, iletim zamanı, tarih, yer, ekler gibi), kullanım safhasında (belgenin alındığı tarih, belgeyi kullanan birim, gerçekleştirilen işlem, yapılan muamele gibi) ve yönetim safhasında (belgenin arşive devir tarihi, versiyon numarası, belge referans numarası, dosya kodu, belgeyi düzenleyen ve oluşturan kişi/birim gibi))

3.15. Teknolojik göç ettirme ile ilgili yapılan işlemler
3.16. Konu
3.17. Belgenin sayısı
3.18. Belgenin gizlilik derecesi (Tasnif dışı, hizmete özel, özel, gizli, çok gizli, kişiye özel gibi)
3.19. Dağıtım listesi
3.20. İlgilerin referans numarası
3.21. Belgenin özet değeri
3.22. Şifreleme bilgisi
3.23. Eklerin referans numaraları

4. Belge bileşenleriyle ilgili aşağıdaki üstverilerden hangileri kurumunuzda kullanılmaktadır?
4.1. Referans numarası
4.2. Format
4.3. Bileşeni üreten yazılım ve o yazılımda kullanılan algoritmalar
4.4. Bileşene erişmek için asgari gereksinimler

5. Log kayıtlarında aşağıdaki bilgilerden hangileri bulunmaktadır?
5.1. Dokümanın belgeye dönüşme tarih ve zamanı
5.2. Belgeye erişim istekleri
5.3. Belgenin iletim geçmişi
5.4. Belgeye yapılan açıklamalar
5.5. Belgede yapılan işlemler ve bu işlemleri yapan kullanıcılar
5.6. Üstverilerde yapılan değişiklikler
5.7. Saklama planı ve saklama sürelerinde yapılan değişiklikler
5.8. Belgede yaşanan teknolojik değişimler
5.9. Sistem arıza ve bakımları
5.10. Paraf bilgileri ve paraflayanın yaptığı işlemler

6. Dosyalama pratikleriyle ilgili aşağıdakilerden hangileri kurumunuz için geçerlidir?
6.1. Belgelerin hangi işlem, dosya, seri ve birime ait olduğunu seçme
6.2. Dosya türü ayrımı yapılması (Konu, Vaka, Gölge dosya, Vaka hazırlık dosyası, melez/hibrit dosya gibi)
6.3. Konu dosyalarının periyodik olarak kapanması
6.4. Vaka dosyasına giren bir belgenin aynı zamanda bir konu dosyasıyla da ilişkiliyse çoğaltılmadan çapraz referans yapılması
6.5. Belgeler ve dosyalar için dosya konu kodunun yanı sıra gerektiğinde özel kodların kullanılması
6.6. Belgeye, birim belge yöneticisi tarafından da dosya kodu verilmesi
6.7. Birim belge yöneticisinin belgeyi ait olduğunu düşündüğü dosyaya gönderebilmesi
6.8. Dosyaların üstverilerinde ait olduğu seri ve birimin belirtilmesi
6.9. Dosyaların, ait oldukları seriden farklı bir seriye taşınabilmesi
6.10. Sistemde aynı dosyanın parçası olup kâğıt ortamında saklanan belgelerin yerinin belirtilmesi
6.11. Belgenin ve dosyanın dosya kodu değişmiş ise eski ve yeninin birlikte gösterilmesi

7. Belge yönetimiyle ilgili kurumsal prosedürler aşağıdakilerden hangilerini içermektedir?
7.1. Belgenin üretilme kuralları
7.2. Belgenin iletilme kuralları
7.3. Dışarıdan gelen belgelerin sisteme kaydedilme kuralları
7.4. Belgeyi dosyasına kaldırma kuralları
7.5. Belgenin tanımlanmasına ilişkin kurallar
7.6. Belgeyi arşive devretme kuralları
7.7. Belgelerin teknolojik göçü ve bu göçün geçerliliğine yönelik tasdik prosedürleri
7.8. Log kayıtları
7.9. Denetim günlükleri
7.10. Donanımların çalışma şartları (sıcaklık ve nem gibi)
7.11. Bilgi güvenliği

8. Saklama süreli dosya planınız için aşağıdakilerden hangileri geçerlidir?
8.1. Fonksiyon analizi yapılarak belge hiyerarşisinin oluşturulması

8.2. Dosya ve seri kodlarının oluşturulması
8.3. Saklama süresi sonunda yapılacak tasfiye işlemlerinin kararlaştırılması
8.4. Standart Dosya Planının, herhangi bir kod ekleme/çıkarması yapılarak kullanılması

9. Teknolojik göçle ilgili aşağıdakilerden hangileri geçerlidir?
9.1. Belgelerin taşıyıcı ortamının değiştirilip değiştirilmemesi hususunda düzenli aralıklarla incelemelerin yapılması
9.2. Teknolojik göç sonrası belgelerin erişilebilirliği ve okunabilirliğinin kontrol edilmesi
9.3. Yeni taşıyıcı ortam ve göçün gerçekleştiği tarihin belge profiline eklenmesi
9.4. Risk analizinin yapılması

10. Yedeklemelerle ilgili aşağıdakilerden hangileri geçerlidir?
10.1. Yedeklemelere sadece yetkili personelin erişmesi
10.2. Belgeler, belge profilleri ve üstverilerin düzenli aralıklarla yedeklenmesi
10.3. Son yedeklemeden bu yana belgelere yapılan açıklamalar ve işlemlerin denetim günlüklerine kaydedilmesi
10.4. Sistem yedeklemesinin yapılması
10.5. Son üç yedeklemenin kopyalarının muhafaza edilmesi
10.6. Denetim günlüklerine yedeklemenin başarılı gerçekleşip gerçekleşmediğinin eklenmesi
10.7. Herhangi bir sorun karşısında bir önceki yedeklemenin devreye alınabilmesi

11. Yedekleme ile ilgili aşağıdaki üstverilerden hangileri sisteminizde mevcuttur?
11.1. Yedeklemenin tarihi ve zamanı
11.2. Yedeklemeyi onaylayan
11.3. Yedeklemenin konumu
11.4. Yedekleme referans numarası

12. Arşive devredilecek belgelerle ilgili mevcut üstverilerin dışında onların delil değerini ilgilendirecek aşağıdaki üstverilerden hangilerinin kullanılması düşünülmektedir?
12.1. Devir zamanı
12.2. Belgelerin özgünlüğünü onaylayan teknikler (iz değeri kontrolü, e-imza sertifikalarının kontrolü, belgedeki kişi ile imzanın uyumu vb.)
12.3. Belgelerin özgünlüğünü onaylayan kişiler
12.4. Özgünlük değerlendirme raporu
12.5. Belgenin tanımlama bilgileri

13. Belgelerin özgünlüğünün tasdik edilmesi için aşağıdaki adımlardan hangileri geçerlidir?
13.1. Belgenin, doğduğu fonksiyonun işlemlerinden en az birini gösterecek nitelikte olması
13.2. Türüne göre belgenin, sahip olması gereken kimlik tespiti araçlarını (tasdik yöntemi) barındırması
13.3. Belge arşive devredildiğinde, onun özniteliklerinin korunduğunu gösteren bir elektronik kurumsal mührün kullanılması
13.4. Belgenin tanımlama bilgilerinin incelenmesi
13.5. Dosya sistemindeki (file system) belge ile veri tabanında tutulan kayıtların ilişkilendirilmesi ve bu ilişkinin kopmaması için gerekli tedbirlerin alınması
13.6. Belge üzerindeki imzaların geçerliliği bitmeden EYP'nin zaman damgası ile damgalanması
13.7. Belgedeki imzaların arşiv imzası tipine dönüştürülmesi
13.8. Bütünlük analizinin düzenli kontrol edilmesi
13.9. Bütünlük bozulması riskine karşı risk değerlendirmesi ve riskten kaçınma raporunun hazırlanması

14. Belgelerin tasfiyesine ilişkin aşağıdaki adımlardan hangileri geçerlidir?
14.1. Belgeler oluşmadan önce belgelere bir saklama süresi tayin edilmesi
14.2. Belgelerin saklama süreleri tamamlandıktan sonra ait oldukları dosyalarla birlikte arşive devredilmesi
14.3. Saklama süresi aşımının gerekçesi
14.4. Belgenin, belge profili ve üstverileriyle birlikte arşive devredilmesi
14.5. Belge tasfiye edilirken belge profili ve üstverisinin de tasfiye edilmesi
14.6. Belge, ister arşive devredilsin ister imha edilsin referans numarasının sistemde tutulması ve belgenin akıbeti hakkında bir bilgi notunun bulunması

14.7. Arşive devredilen belgelerin dosyalarıyla birlikte belge yönetim sisteminden kaldırılıp arşiv yönetim sistemine aktarılması

15. Belge yönetimi kapasitesinin geliştirilmesi için aşağıdakilerden hangileri geçerlidir?
15.1. Kurumsal belge yönetimi politikasının oluşturulması
15.2. Bilgi ve belge yönetimi mezunu kişilerin belge yönetimiyle ilgili birimde istihdam edilmesi
15.3. Belge yönetimiyle ilgilenen personelin eğitim programının bulunması (eğitmen eğitimi)
15.4. Kurum çalışanlarının belge yönetimi birimi tarafından eğitilmesi
15.5. TSE 13298 Kurumsal sertifikasyon alınması yönünde girişimler yapılması

16. Arşivlenen belgelerin tanımlanması için bir standardın kullanılması düşünülmekte midir? Lütfen belirtiniz.
16.1. Evet/Hayır

17. Elektronik belge yönetiminde belgenin delil değerini korumak için aşağıdaki teknolojilerden hangilerinin kullanılması düşünülmektedir?
17.1. Blokzincir
17.2. Yapay zekâ
17.3. Derin öğrenme/Makine öğrenmesi
17.4. Elektronik delil elde etme (Digital forensics-Öykünme, teknolojik göç)

18. Yazılım ve donanımla ilgili aşağıdaki ifadelerden hangileri geçerlidir?
18.1. Yazılım algoritması ve kaynak kodlarının kurum tarafından saklanması
18.2. Veri tabanının arşivlenebilir bir formatta yapılandırılması
18.3. Belgelerin bir kez yazılabilir ortamlarda saklanması
18.4. Belge bileşenlerinin de belgeyle birlikte bütüncül olarak korunması
18.5. Yazılım değiştirildiğinde de belgelere erişilebilmesi
18.6. Güncel belgelerle arşivlenen belgelerin saklanma konumları arasında bir ayrım yapılması
18.7. Donanımların üreticilerin tavsiye ettiği kullanım ömrü dolduktan sonra kullanılmaması
18.8. Belgelerin üretildiği araçlardaki donanım ve yazılım özelliklerinin kayıt altına alınması
18.9. 27001 Sertifikası alınması yönünde girişimlerin yapılması
18.10. Yazılımın TSE 13298 Sertifikasına uygun olması yönünde girişimlerin yapılması
18.11. Log kayıtlarının zaman damgası ile damgalanması

19. Üstveriler için aşağıdakilerden hangileri geçerlidir?
19.1. Üstverilerin belgeden ayrı olarak XML ya da JSON olarak saklanması
19.2. Üstveriler, belge ile birlikte hareket etmektedir. (Belgenin konumu değiştirildiğinde üstverilerin de beraberinde taşınması)
19.3. Yöneticilerin yaptığı değişiklikler sonucunda yeni bir üstveri kaydının oluşması ve daha önceki üstveri kaydının muhafaza edilmesi
19.4. Üstveri dosyasının ait olduğu belgenin referans numarasına sahip olması

20. Denetim günlükleri için aşağıdakilerden hangileri geçerlidir?
20.1. Tüm belgeler için denetim günlüklerinin oluşturulması
20.2. Denetim günlükleri oluşturulmasına karar verilen belgeler için, bunların otomatik olarak oluşması
20.3. Denetim günlüklerinin yapılan işlemlerin tarih ve saatini içermesi
20.4. Denetim günlüklerine erişim sırasında bir sorun yaşanıp yaşanmadığının düzenli aralıklarla otomatik olarak kontrol edilmesi
20.5. Denetim günlüklerinin bir kere yazılması ve üzerinde hiç değişiklik yapılmaması

21. Kurumda üretilen ve dışarıdan gelen belgelerin form özellikleri, formatı ve içeriğinin değiştirilmemesine yönelik aşağıdaki hangi yaklaşımları benimsiyorsunuz?
21.1. İz değeri kontrolü
21.2. Dosya tanımlayıcı kullanımı (JHOVE, DROID gibi)
21.3. Adli bilişim (Digital forensics) yöntemleri
21.4. Log kayıtlarının kontrolü
21.5. Döngüsel artıklık denetimi (CRC)

EK 4. BELGE DÜZEYİ TEMASININ KATEGORİ VE KODLARI

Dosyalama

- **Dosyalama pratikleri, belgenin delil vasfı özelliklerinden biridir**
  - **Belgenin provenansını ispatlar**
  - **Belgenin sahihliğini gösterir**
  - **Dosya planı aracılığıyla belgelerin izi sürülür**
- **Arşivcilik açısından yönetilebilir bir yapıyı mümkün kılar**
- **Belgenin kurumsal bir varlık olduğunu gösterir**
- **Türkiye'nin gelecek 20 yılda karşılaşacağı en büyük sorunlardan biridir**
  - **Mevcut elektronik belge yönetim sistemleri gelecekte arşiv yönetim sistemleri olarak kullanılamayabilir**
  - **Bugüne kadar üretilmiş e-belgeler tasnif edilmeli**

Arşivsel bağ

Üstveriler

- Erişim profili üstverisi
- Diplomatik özellikler
- Kurumsal fonksiyonlarla ilgili üstveriler
- İlişkili olduğu mevzuat üstverisi
- Erişim kodları üstverisi
- İdari birim kimlik kodları
- TSE 13298'deki zorunlu üstveriler
- Belgenin yaşam döngüsünü gösteren üstveriler
- Belge ve üstveri arasındaki bağ
- **E-belge yönetiminin temel direklerinden biridir**

Değerlendirme

Elektronik Yazışma Paketi

- EYP'siz belgelerin EYP'ye dönüştürülmesi
- **Zenginleştirilerek arşivleme için kullanılabilir**

Güvenilirlik mekanizmaları

- Üstveriler
- Dosya planı
- Elektronik Yazışma Paketi
- Log kayıtları
- Belgenin özniteliklerinin korunması
- Diplomatik özellikler
- Tanımlama
- Kayıtlı elektronik posta
- Arşiv imzası
- Arşiv mührü
- Kurumsal mühür
- Yazılımsal güvenilirlik testleri

Belgeler, log kayıtlarıyla birlikte arşive devredilmeli

Belge yönetimi bir disiplin işidir

Şekil 45. Belge Düzeyi Temasının Kategori ve Kodları

EK 5. TEKNOLOJİK KOŞULLAR DÜZEYİ TEMASININ KATEGORİ VE KODLARI

Log kayıtları

- Belgedeki kişileri göstermeli
- **Belge ile birlikte delil olarak kullanılmalı**
- İşlemin hangi görev dâhilinde gerçekleştirildiğini göstermeli
- İşlemin ne zaman yapıldığını göstermeli
- Belge bileşenlerine ilişkin log kayıtları tutulmalı
- Anlamlı ve anlaşılabilir olmalı
- Sahih olmalı
- Müdahaleye açık olmamalı
- Süresiz saklanmalı
- Yeni formatlara ve yazılımlara aktarılabilmeli
- 27001'e göre değil belge yönetimine göre saklanmalı
- Kurumsal mühür ile saklanmalı
- Zaman damgası ile saklanmalı
- Belge yönetiminde log standartları oluşturulmalı

Teknolojik göç

- **Devlet Arşivleri Başkanlığı kuralları belirlemeli**
- Göç ettirme onaylanmalı
- İçerik, kontekst ve yapı korunmalı
- Teknolojik dönüşüm süreci üstverisi oluşturulmalı
- Uluslararası tanınırlığı olan formatlar kullanılmalı
- Belge göç ettirilemiyorsa delil değerinden şüphe duyulur

E-imza ve zaman damgası sorunları

- İmzaların kırılma ihtimali
- Kuantum teknolojisi şifreleri çözebilir
- Kullanılan teknolojinin eskimesi
- Sertifika hizmeti veren kuruluşların faaliyetlerini durdurması
- Siber saldırılar
- Doğrulama sorunları
- Sertifika süresi sorunu
- Sertifikaların kontrol edilememesi
- Sunuculara ve felaket kurtarma merkezine erişememe
- Zaman sapması
- E-imza arşivinin yedeklenmesi
- Arşiv mührü
- Daha güçlü algoritmaların kullanılması
- TÜBİTAK'ın kurumlardaki e-imza süreçlerini denetlemesi

Donanım özellikleri

Güncel ve arşivlenen belgelerin ayrı yerlerde saklanması

- Diskler kullanım ömrüne göre yenilenmeli ve dönüştürülebilmeli
- Dışarıdan müdahaleye izin verilmemeli
- Kullanılacak donanımlara ilişkin kriterler belirlenmeli
- Teknoloji yenileme politikası hazırlanmalı
- Yazılımların gerektirdiği özellikte donanımlar kullanılmalı
- Sağlamlığı kanıtlanmış veri yedekleme kasetleri kullanılmalı
- Arşiv belgeleri SSD'de tutulmamalı
- Depolama ortamı güvenilir olmalı
- WORM diskler kullanılmalı

EBYS kaynak kodlarının korunması

- API'ler saklanmalı
- Yazışma paketi kodları ve versiyonları saklanmalı
- Zaman damgası ile saklanmalı
- Hangi imza algoritmasının kullanıldığı belirtilmeli
- Kaynak kodlarını korumak yönünde bir genelge hazırlanmalı
- Kaynak kodlarında yapılan geliştirmeler, ortak bir alanda tutulmalı

Parafinblok gibi bir yazılım kullanılmalı

Devlet Arşivleri Başkanlığı, milli bir format belirlemeli

Belgenin delil değerini ortam değil, oluşma nitelikleri belirler

EBYS'lerin bilgisayar bilimiyle ilintili ilerlemesi, bir veri tabanı gibi düşünülmesi olumsuz sonuçlar doğurur

Şekil 46. Teknolojik Koşullar Düzeyi Temasının Kategori ve Kodları

EK 6. KURUM DÜZEYİ TEMASININ KATEGORİ VE KODLARI

Devlet Arşivleri Başkanlığının katkısı

- Teknik rehberler hazırlanmalı
- Veri koruma politikası hazırlanmalı
- Milli format belirlenmeli
- Teknolojik öngörü politikası hazırlanmalı
- Elektronik belge yönetimi politikası hazırlanmalı
- Dijital Vizyon Belgesi (Yapay Zekâ, Endüstri 4.0 gibi hazırlanmalı)
- Zorunlu üstveriler belirlenmeli
- Denetimler yapılıp yaptırımlar uygulanmalı
- Log kayıtlarının silinip silinmediği denetlenmeli
- API'leri saklamalı
- Yazışma paketi kodları ve versiyonlarını saklamalı
- E-imzaların kök sertifikalarını sertifika deposunda saklamalı
- Kurumların isim değişimlerini ve kimlik kodlarını saklamalı
- Elektronik belgelerin geleceği konusunda çalıştaylar düzenlenmeli
- Uluslararası çalışmalara eklemlenmeli

Yedekleme ve log kayıtları rehberinin hazırlanması

- Devlet Arşivleri Başkanlığı hazırlamalı
- Veri tabanındaki işlemlerin log kayıtları süresiz saklanmalı
- Yedekleme sistematiği geliştirilmeli

Risk yönetimi

- Eylem planı hazırlanmalı
- Risk iştahı belirlenmeli
- Risk denetimi yapıllmalı
- Eylem planı hazırlanmalı
- Risk tatbikatı yapılmalı
- ISO 27001 seviyesinde sunucu odası oluşturulmalı
- Sayısal koruma
  - Üretim ve sunum şekli korunmalı
  - Belge aktarılabilir, erişilebilir ve kullanılabilir olmalı
  - Belgenin saklama ortamı ve içeriği korunmalı
  - Elektronik belgelerin gelecekte erişilememesi bir risk olarak değerlendirilmeli
  - Dosya formatları konusunda teknik bir mevzuat geliştirilmeli
- İhmal ve kasıt arasında bir ayrım yapılmalı

Devlet Arşivleri Başkanlığı, o ülkenin en yüce noter kurumudur

Elektronik belge yönetimi, kurumlarda müstakil bir birim olmalı

Erişemediğin veri senin değildir

Arşivler, yığından ziyade bir değerdir

Politika belirleyiciler, nitelikli belge yöneticileri olmalı

Şekil 47. Kurum Düzeyi Temasının Kategori ve Kodları

EK 7. NİCEL ARAŞTIRMA SORULARININ TEORİK ALTYAPISI

Sorular	Kaynak	Mevzuatta Karşıladığı Düşünülen Delil Özellikleri
1. Belge yönetim sistemine geçerken kurum aşağıdaki prosedürlerden hangilerini gerçekleştirmiştir? (Kurum Düzeyi)		
Kurumun e-belge yönetimi politikasını belirleme	TSE, 13298 (s. 42)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Kurumun e-arşiv yönetimi politikasını belirleme	TSE, 13298 (s. 42)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Fonksiyonlar ve iş süreçleri tanımlama ve belgelerle ilişkilendirme	ISO, 30301 (s. 5)	Tanımlanabilirlik (Finansal Bilgiye İlişkin Kavramsal Çerçeve)
İş süreçlerine dair dokümantasyon oluşturma	ISO, 14641 (s. 30)	Tanımlanabilirlik (Finansal Bilgiye İlişkin Kavramsal Çerçeve)
Form ve şablon oluşturma	TSE, 13298 (s. 41)	Gerçeklik (TTK)
Belge türüne göre oluşturulan şablonlar için bir kontrol numarası verme	TSE, 13298 (s. 7)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK)
Spesifik üstveri şemaları çıkarma	ISO, 15489 (s. 6)	Tanımlanabilirlik (Finansal Bilgiye İlişkin Kavramsal Çerçeve)
Belge profilindeki form özelliklerini (belgedeki kişiler, antet, format, teknolojik özellikler, belgeye işlem safhasında yapılan açıklamalar gibi) tanımlama	ISO 16175-1 (s. 20)	Tanımlanabilirlik (Finansal Bilgiye İlişkin Kavramsal Çerçeve)
Belgeler ve dosyalar için dosya tasnif planı ve saklama planı hazırlama	ISO, 15489 (s. 14)	Belgelerin tasnif edilmesi (TTK)
Dosya planına uygun dosyalama sistemi geliştirme	TSE, 13298 (s. 4)	Belgelerin tasnif edilmesi (TTK)
Kontrollü terminoloji oluşturma	ISO, 26122 (s. V)	Tanımlanabilirlik (Finansal Bilgiye İlişkin Kavramsal Çerçeve)
Felaket kurtarma planı ve yedekleme planı oluşturma	ISO, 27050-1 (s. 20) ve ISO, 14641 (s. 7)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
2. Belgenin aşağıdaki form özelliklerinden hangilerini üstverilerde kullanıyorsunuz? (Belge Düzeyi)		
Sorumlu (Belgeyi üreten kurum)	TSE, 13298 (s. 52)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK)
Düzenleyen (Belgedeki irade beyanının sahibi)	TSE, 13298 (s. 57)	Düzenleyenin belli olması (EİK)
Muhatap/Alıcı	TSE, 13298 (s. 57)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK)

Konu	TSE, 13298 (s. 57)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Format	TSE, 13298 (s. 58)	Okunabilirlik/Anlaşılabilirlik (Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun)
Üretim tarihi	TSE, 13298 (s. 57)	Düzenleyenin belli olması (EİK)
Gönderim/Alma tarihi (KEP)	TSE, 13298 (s. 57)	Düzenleyenin belli olması (Kayıtlı Elektronik Posta Kanunu)
Belge tarihi (Son imzalayıcının imza attığı tarih)	TSE, 13298 (s. 59)	Düzenleyenin belli olması (EİK)
3. Belge profilinde aşağıdaki üstverilerden hangileri bulunmaktadır?		
Belgenin dosyasına kaldırıldığı zaman	INTERPARES, 2002 (s. 28)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Belgedeki işlemden sorumlu kişi ve birim	INTERPARES, 2002 (s. 147)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK
Ait olduğu işlem-dosya-seri-birim	TSE, 13298 (s. 4)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Dosya kodu	TSE, 13298 (s. 57)	Belgelerin tasnif edilmesi (TTK)
Belge referans numarası	TSE, 13298 (s. 56)	Bütünlük (CMK)
Belgeye erişmek için asgari gereksinimler	ISO, 23081 (s. 13)	Okunabilirlik/Anlaşılabilirlik (Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun)
Belgenin üretildiği EBYS yazılımı ve versiyon numarası	TSE, 13298 (s. 58)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK
Belge yönetimi için kullanılacak algoritmalar (kullanılan EBYS yazılımı algoritmaları ve belgeyi tekrardan üretmek ya da şifreli belgeleri açabilmek için gerekli olan algoritmalar gibi)	ISO, 12033 (s. 42) ve ISO, 27040 (s. 49)	Okunabilirlik/Anlaşılabilirlik (Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun)
Belge bileşenleri (Üstveri, belgenin ekleri, form elemanları, kontekst (bağlam), içerik, belgenin oluşumunu sağlayan veriler, iş akışları gibi)	TSE, 13298 (s. 60)	Bütünlük (CMK)
E-imza ve zaman damgası	TSE, 13298 (s. 59)	Düzenleyenin belli olması (EİK)
Saklama süresi	TSE, 13298 (s. 7)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK
Belgeye erişim profilleri	ISO, 16175-1 (s. 12)	Gizlilik (Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik)
Belgelerin lokasyonu (Directory)	ISO, 27037 (s. 10)	Erişilebilirlik (TTK)

Belgeye yapılan açıklama notları (İşlem safhasında (ivedilik durumu, iletim zamanı, tarih, yer, ekler gibi), kullanım safhasında (belgenin alındığı tarih, belgeyi kullanan birim, gerçekleştirilen işlem, yapılan muamele gibi) ve yönetim safhasında (belgenin arşive devir tarihi, versiyon numarası, belge referans numarası, dosya kodu, belgeyi düzenleyen ve oluşturan kişi/birim gibi))	INTERPARES, 2008, (s. 210-211)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Teknolojik göç ettirme ile ilgili yapılan işlemler	ISO, 15801 (s. 25)	Güvenilirlik (Bankacılık Kanunu)
Konu	TSE, 13298 (s. 57)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Belgenin sayısı	TSE, 13298 (s. 56)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK
Belgenin gizlilik derecesi (Tasnif dışı, hizmete özel, özel, gizli, çok gizli, kişiye özel gibi)	TSE, 13298 (s. 58)	Gizlilik (Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik)
Dağıtım listesi	TSE, 13298 (s. 57)	Aidiyet zincirinin muhafaza edilmesi (RYY)
İlgilerin referans numarası	TSE, 13298 (s. 60)	Bütünlük (CMK)
Belgenin özet değeri	ISO, 13008 (s. 22)	Bütünlük (CMK)
Şifreleme bilgisi	TSE, 13298 (s. 59)	Gizlilik (Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik)
Eklerin referans numaraları	TSE, 13298 (s. 60)	Bütünlük (CMK)
4. Belge bileşenleriyle ilgili aşağıdaki üstverilerden hangileri kurumunuzda kullanılmaktadır? (Belge Düzeyi)		
Referans numarası	TSE, 13298 (s. 60)	Bütünlük (CMK)
Format	TSE, 13298 (s. 60)	Okunabilirlik/Anlaşılabilirlik (Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun)
Bileşeni üreten yazılım ve o yazılımda kullanılan algoritmalar	ISO, 27040 (s. 49)	Okunabilirlik/Anlaşılabilirlik (Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun)
Bileşene erişmek için asgari gereksinimler	ISO, 23081 (s. 13)	Okunabilirlik/Anlaşılabilirlik (Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun)
5. Log kayıtlarında aşağıdaki bilgilerden hangileri bulunmaktadır? (Teknolojik Koşullar Düzeyi)		
Dokümanın belgeye dönüşme tarih ve zamanı	TSE, 13298 (s. 23)	Doğrulanabilirlik (CMK)
Belgeye erişim istekleri	TSE, 13298 (s. 24)	Güvenilirlik (Bankacılık Kanunu)

Belgenin iletim geçmişi	TSE, 13298 (s. 24)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Belgeye yapılan açıklamalar	INTERPARES, 2008 (s. 692)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Belgede yapılan işlemler ve bu işlemleri yapan kullanıcılar	TSE, 13298 (s. 23)	Düzenleyenin belli olması (EİK)
Üstverilerde yapılan değişiklikler	TSE, 13298 (s. 24)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Saklama planı ve saklama sürelerinde yapılan değişiklikler	TSE, 13298 (s. 23)	Belgelerin tasnif edilmesi (TTK)
Belgede yaşanan teknolojik değişimler	ISO 23081 (s. 6)	Okunabilirlik/Anlaşılabilirlik (Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun)
Sistem arıza ve bakımları	ISO 15801 (s. 26)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Paraf bilgileri ve paraflayanın yaptığı işlemler	TSE, 13298 (s. 24)	Doğrulanabilirlik (CMK)
6. Dosyalama pratikleriyle ilgili aşağıdakilerden hangileri kurumunuz için geçerlidir? (Belge Düzeyi)		
Belgelerin hangi işlem, dosya, seri ve birime ait olduğunu seçme	ISO 16175-1 (s. 14)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Dosya türü ayrımı yapılması (Konu, Vaka, Gölge dosya, Vaka hazırlık dosyası, melez/hibrit dosya gibi)	ISO 16175-1 (s. 16)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK
Konu dosyalarının periyodik olarak kapanması	TSE, 13298 (s. 7)	Düzenlilik (TTK)
Vaka dosyasına giren bir belgenin aynı zamanda bir konu dosyasıyla da ilişkiliyse çoğaltılmadan çapraz referans yapılması	TSE, 13298 (s. 6)	Belgelerin tasnif edilmesi (TTK)
Belgeler ve dosyalar için dosya konu kodunun yanı sıra gerektiğinde özel kodların kullanılması	TSE, 13298 (s. 4)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Belgeye, birim belge yöneticisi tarafından da dosya kodu verilmesi	TSE, 13298 (s. 6)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Birim belge yöneticisinin belgeyi ait olduğunu düşündüğü dosyaya gönderebilmesi	TSE, 13298 (s. 6)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Dosyaların üstverilerinde ait olduğu seri ve birimin belirtilmesi	TSE, 13298 (s. 4)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Dosyaların, ait oldukları seriden farklı bir seriye taşınabilmesi	TSE, 13298 (s. 6)	Belgelerin tasnif edilmesi (TTK)
Sistemde aynı dosyanın parçası olup kâğıt ortamında saklanan belgelerin yerinin belirtilmesi	TSE, 13298 (s. 50)	Belgelerin tasnif edilmesi (TTK)
Belgenin ve dosyanın dosya kodu değişmiş ise eski ve yeninin birlikte gösterilmesi	ISO, 23081-1 (s. 24)	Düzenlilik (TTK)
7. Belge yönetimiyle ilgili kurumsal prosedürler aşağıdakilerden hangilerini içermektedir? (Kurum Düzeyi)		
Belgenin üretilme kuralları	ISO, 14641 (s. 6)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK)

Belgenin iletilme kuralları	ISO, 10789 (s. 13)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK)
Dışarıdan gelen belgelerin sisteme kaydedilme kuralları	ISO, 14641 (s. 6)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK)
Belgeyi dosyasına kaldırma kuralları	ISO, 10789 (s. 14)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK)
Belgenin tanımlanmasına ilişkin kurallar	ISO, 30301 (s. 2)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK
Belgeyi arşive devretme kuralları	ISO, 14641 (s. 6)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK)
Belgelerin teknolojik göçü ve bu göçün geçerliliğine yönelik tasdik prosedürleri	ISO, 15801 (s. 7)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK)
Log kayıtları	ISO, 30301 (s. 3)	Güvenilirlik (Bankacılık Kanunu)
Denetim günlükleri	ISO, 30301 (s. 3)	Güvenilirlik (Bankacılık Kanunu)
Donanımların çalışma şartları (sıcaklık ve nem gibi)	ISO, 30301 (s. 3)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Bilgi güvenliği	ISO, 27001	Güvenilirlik (Bankacılık Kanunu)
8. Saklama süreli dosya planınız için aşağıdakilerden hangileri geçerlidir? (Belge Düzeyi)		
Fonksiyon analizi yapılarak belge hiyerarşisinin oluşturulması	ISO, 16175-1 (s. 20)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Dosya ve seri kodlarının oluşturulması	TSE, 13298 (s. 53, 55)	Belgelerin tasnif edilmesi (TTK)
Saklama süresi sonunda yapılacak tasfiye işlemlerinin kararlaştırılması	ISO, 15489 (s. 14)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK
Standart Dosya Planının kod ekleme/çıkarma yapılarak kullanılması	TSE, 13298 (s. 4)	Düzenlilik (TTK)
9. Teknolojik göçle ilgili aşağıdakilerden hangileri geçerlidir? (Teknolojik Koşullar Düzeyi)		
Belgelerin taşıyıcı ortamının değiştirilip değiştirilmemesi hususunda düzenli aralıklarla incelemelerin yapılması	ISO, 27040 (s. 48)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Teknolojik göç sonrası belgelerin erişilebilirliği ve okunabilirliğinin kontrol edilmesi	ISO, 13008 (s. 13-14)	Okunabilirlik/Anlaşılabilirlik (Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun)
Yeni taşıyıcı ortam ve göçün gerçekleştiği tarihin belge profiline eklenmesi	ISO, 13008 (s. 8)	Doğrulanabilirlik (CMK)
Risk analizinin yapılması	INTERPARES, 2002 (s. 30)	Risk planı (Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik)
10. Yedeklemelerle ilgili aşağıdakilerden hangileri geçerlidir? (Teknolojik Koşullar Düzeyi)		

Yedeklemelere sadece yetkili personelin erişmesi	ISO, 15801 (s. 25)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Belgeler, belge profilleri ve üstverilerin düzenli aralıklarla yedeklenmesi	ISO, 15801 (s. 26)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Son yedeklemeden bu yana belgelere yapılan açıklamalar ve işlemlerin denetim günlüklerine kaydedilmesi	ISO, 15801 (s. 26)	Bütünlük (CMK)
Sistem yedeklemesinin yapılması	INTERPARES, 2002 (s. 163)	Bütünlük (CMK)
Son üç yedeklemenin kopyalarının muhafaza edilmesi	ISO, 30300 (s. 17-18)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Denetim günlüklerine yedeklemenin başarılı gerçekleşip gerçekleşmediğinin eklenmesi	INTERPARES, 2002 (s. 163)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK)
Herhangi bir sorun karşısında bir önceki yedeklemenin devreye alınabilmesi	INTERPARES, 2002 (s. 163)	Bütünlük (CMK)
11. Yedekleme ile ilgili aşağıdaki üstverilerden hangileri sisteminizde mevcuttur? (Teknolojik Koşullar Düzeyi)		
Yedeklemenin tarihi ve zamanı	INTERPARES, 2008 (s. 214)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK)
Yedeklemeyi onaylayan	INTERPARES, 2008 (s. 214)	Gerçeklik (TTK)
Yedeklemenin konumu	INTERPARES, 2008 (s. 214)	Erişilebilirlik (TTK)
Yedekleme referans numarası	INTERPARES, 2008 (s. 214)	Bütünlük (CMK)
12. Arşive devredilecek belgelerle ilgili mevcut üstverilerin dışında onların delil değerini ilgilendirecek aşağıdaki üstverilerden hangilerinin kullanılması düşünülmektedir? (Belge Düzeyi)		
Devir zamanı	INTERPARES, 2008 (s. 211)	Düzenleyenin belli olması (RYY)
Belgelerin özgünlüğünü onaylayan teknikler (özet değeri kontrolü, e-imza sertifikalarının kontrolü, belgedeki kişi ile imzanın uyumu vb.)	INTERPARES, 2008 (s. 226)	Güvenilirlik (CMK)
Belgelerin özgünlüğünü onaylayan kişiler	INTERPARES, 2008 (s. 226)	İrade beyanı içermek (Türk Borçlar Kanunu)
Özgünlük değerlendirme raporu	INTERPARES, 2008 (s. 226)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Belgenin tanımlama bilgileri	INTERPARES, 2008 (s. 226)	Tanımlanabilirlik (Finansal Bilgiye İlişkin Kavramsal Çerçeve)
13. Belgelerin özgünlüğünün tasdik edilmesi için aşağıdaki adımlardan hangileri geçerlidir? (Belge Düzeyi)		
Belgenin, doğduğu fonksiyonun işlemlerinden en az birini gösterecek nitelikte olması	INTERPARES, 2008 (s. 229)	Doğrulanabilirlik (CMK)
Türüne göre belgenin, sahip olması gereken kimlik tespiti araçlarını (tasdik yöntemi) barındırması	INTERPARES, 2008 (s. 229)	Doğrulanabilirlik (CMK)

Belge arşive devredildiğinde, onun özniteliklerinin korunduğunu gösteren bir elektronik kurumsal mührün kullanılması	TSE, 13298 (s. 28)	Düzenleyenin belli olması (RYY)
Belgenin tanımlama bilgilerinin incelenmesi	INTERPARES, 2008 (s. 229)	Tanımlanabilirlik (Finansal Bilgiye İlişkin Kavramsal Çerçeve)
Dosya sistemindeki (file system) belge ile veri tabanında tutulan kayıtların ilişkilendirilmesi ve bu ilişkinin kopmaması için gerekli tedbirlerin alınması	ISO, 18492 (s. 15)	Gerçeklik (TTK)
Belge üzerindeki imzaların geçerliliği bitmeden EYP'nin zaman damgası ile damgalanması	RYY	Doğrulanabilirlik (CMK)
Belgedeki imzaların arşiv imzası tipine dönüştürülmesi	RYY	Aidiyet zincirinin muhafaza edilmesi (RYY)
Bütünlük analizinin düzenli kontrol edilmesi	ISO, 27040 (s. 17)	Bütünlük (CMK)
Bütünlük bozulması riskine karşı risk değerlendirmesi ve riskten kaçınma raporunun hazırlanması	ISO, 21496 (s. V)	Risk planı (Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik)
14. Belgelerin tasfiyesine ilişkin aşağıdaki adımlardan hangileri geçerlidir? (Belge Düzeyi)		
Belgeler oluşmadan önce belgelere bir saklama süresi tayin edilmesi	ISO, 17068 (s. 12)	Belgelerin tasnif edilmesi (TTK)
Belgelerin saklama süreleri tamamlandıktan sonra ait oldukları dosyalarla birlikte arşive devredilmesi	ISO, 16175-1 (s. 9)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Saklama süresi aşımının gerekçesi	ISO, 16175-1 (s. 9)	Belgenin ait olduğu fonksiyonu gerçekleştirmekle görevli makam tarafından usûlüne uygun olarak üretilmesi (HMK)
Belgenin, belge profili ve üstverileriyle birlikte arşive devredilmesi	TSE, 13298 (s. 42)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Belge tasfiye edilirken belge profili ve üstverisinin de tasfiye edilmesi	TSE, 13298 (s. 42)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Belge, ister arşive devredilsin ister imha edilsin referans numarasının sistemde tutulması ve belgenin akıbeti hakkında bir bilgi notunun bulunması	TSE, 13298 (s. 62)	Doğrulanabilirlik (CMK)
Arşive devredilen belgelerin dosyalarıyla birlikte belge yönetim sisteminden kaldırılıp arşiv yönetim sistemine aktarılması	TSE, 13298 (s. 42)	Düzenlilik (TTK)
15. Belge yönetimi kapasitesinin geliştirilmesi için aşağıdakilerden hangileri geçerlidir? (Kurum Düzeyi)		
Kurumsal belge yönetimi politikasının oluşturulması	TSE, 13298 (s. 42)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Bilgi ve belge yönetimi mezunu kişilerin belge yönetimiyle ilgili birimde istihdam edilmesi	Belge Yöneticisi Meslek Standardı	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Belge yönetimiyle ilgilenen personelin eğitim programının bulunması (eğitmen eğitimi)	ISO, 30301 (s. 7)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)

Kurum çalışanlarının belge yönetimi birimi tarafından eğitilmesi	ISO, 30301 (s. 4)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
TSE 13298 Kurumsal sertifikasyon alınması yönünde girişimler yapılması	TSE, 13298	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
16. Arşivlenen belgelerin tanımlanması için bir standardın kullanılması düşünülmekte midir? (Belge Düzeyi)	ISO, 15489	Tanımlanabilirlik (TTK)
17. Elektronik belge yönetiminde belgenin delil değerini korumak için aşağıdaki teknolojilerden hangilerinin kullanılması düşünülmektedir? (Teknolojik Koşullar Düzeyi)		
Blokzincir	ISO, TC 307	Güvenilirlik (CMK)
Yapay zekâ	ISO, 24028	Güvenilirlik (CMK)
Derin öğrenme/Makine öğrenmesi	ISO, 4213 (Geliştirme aşamasında)	Güvenilirlik (CMK)
Elektronik delil elde etme (Digital forensics-Öykünme, teknolojik göç)	ISO, 21043-2	Güvenilirlik (CMK)
18. Yazılım ve donanımla ilgili aşağıdaki ifadelerden hangileri geçerlidir? (Teknolojik Koşullar Düzeyi)		
Yazılım algoritması ve kaynak kodlarının kurum tarafından saklanması	UNESCO, Software Heritage	Okunabilirlik/Anlaşılabilirlik (Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun)
Veri tabanının arşivlenebilir bir formatta yapılandırılması	ISO, 15801 (s. 20)	Aidiyet zincirinin muhafaza edilmesi (RYY)
Belgelerin bir kez yazılabilir ortamlarda saklanması	ISO, 27040 (s. 52)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Belge bileşenlerinin de belgeyle birlikte bütüncül olarak korunması	TSE, 13298 (s. 60)	Bütünlük (CMK)
Yazılım değiştirildiğinde de belgelere erişilebilmesi	ISO, 16175-1 (s. 10)	Okunabilirlik/Anlaşılabilirlik (Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun)
Güncel belgelerle arşivlenen belgelerin saklanma konumları arasında bir ayrım yapılması	ISO, 27037 (s. 10)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Donanımların üreticilerin tavsiye ettiği kullanım ömrü dolduktan sonra kullanılmaması	TSE, 13298 (s. 30)	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Belgelerin üretildiği araçlardaki donanım ve yazılım özelliklerinin kayıt altına alınması	TSE, 13298 (s. 30)	Okunabilirlik/Anlaşılabilirlik (Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun)
27001 Sertifikası alınması yönünde girişimlerin yapılması	ISO, 27001	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Yazılımın TSE 13298 Sertifikasına uygun olması yönünde girişimlerin yapılması	TSE, 13298	Belgelerin zayi olmaması için gerekli önlemlerin alınması (TTK)
Log kayıtlarının zaman damgası ile damgalanması	ISO, 18829 (s. 6)	Bütünlük (CMK)
19. Üstveriler için aşağıdakilerden hangileri geçerlidir? (Teknolojik Koşullar Düzeyi)		
Üstverilerin belgeden ayrı olarak XML ya da JSON olarak saklanması	INTERPARES, 2008 (s. 277)	Bütünlük (CMK)
Üstveriler, belge ile birlikte hareket etmektedir. (Belgenin konumu değiştirildiğinde üstverilerin de beraberinde taşınması)	ISO, 23081-1 (s. 4)	Bütünlük (CMK)

Yöneticilerin yaptığı değişiklikler sonucunda yeni bir üstveri kaydının oluşması ve daha önceki üstveri kaydının muhafaza edilmesi	ISO, 23081-1 (s. 24)	Doğrulanabilirlik (CMK)
Üstveri dosyasının ait olduğu belgenin referans numarasına sahip olması	ISO, 15489 (s. 5)	Bütünlük (CMK)
20. Denetim günlükleri için aşağıdakilerden hangileri geçerlidir? (Teknolojik Koşullar Düzeyi)		
Tüm belgeler için denetim günlüklerinin oluşturulması	ISO, 15801 (s. 37)	Doğrulanabilirlik (CMK)
Denetim günlükleri oluşturulmasına karar verilen belgeler için, bunların otomatik olarak oluşması	ISO, 15801 (s. 38)	Doğrulanabilirlik (CMK)
Denetim günlüklerinin yapılan işlemlerin tarih ve saatini içermesi	ISO, 27040 (s. 58)	Doğrulanabilirlik (CMK)
Denetim günlüklerine erişim sırasında bir sorun yaşanıp yaşanmadığının düzenli aralıklarla otomatik olarak kontrol edilmesi	ISO, 15801 (s. 39)	Bütünlük (CMK)
Denetim günlüklerinin bir kere yazılması ve üzerinde hiç değişiklik yapılmaması	ISO, 15801 (s. 39)	Bütünlük (CMK)
21. Kurumda üretilen ve dışarıdan gelen belgelerin form özellikleri, formatı ve içeriğinin değiştirilmemesine yönelik aşağıdaki hangi yaklaşımları benimsiyorsunuz? (Belge Düzeyi)		
İz değeri kontrolü	ISO, 27037 (s. 9)	Bütünlük (CMK)
Dosya tanımlayıcı kullanımı (JHOVE, DROID gibi)	The National Archives, Open Preservation Foundation	Tanımlanabilirlik (TTK)
Adli bilişim (Digital forensics) yöntemleri	ISO, 27037	Bütünlük (CMK)
Log kayıtlarının kontrolü	TSE, 13298 (s. 23)	Doğrulanabilirlik (CMK)
Döngüsel artıklık denetimi (CRC)	ISO, 18492 (s. 8)	Bütünlük (CMK)

Tablo 2. Nicel Araştırma Sorularının Teorik Altyapısı

EK 8. NİCEL ARAŞTIRMA ANKET CEVAPLARI

Sorular	**1**	**2**	**3**	**4**	**5**	**6**
Kullandığınız kaçıncı EBYS?	2	2	3	2	2	2
Sistemi kendiniz mi geliştirdiniz?	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Kaç yıldır EBYS kullanıyorsunuz?	4	8	4	7	8	11
Yazılımın TSE uygunluk sertifikası var mı?	Evet	Evet	Evet	Evet	Evet	Evet
KEP kullanıyor musunuz?	Evet	Evet	Evet	Evet	Evet	Evet
UETS kullanıyor musunuz?	Evet	Evet	Evet	Evet	Evet	Evet
EYP kullanıyor musunuz?	Evet	Evet	Evet	Evet	Evet	Evet
1. Belge yönetim sistemine geçerken kurum aşağıdaki prosedürlerden hangilerini gerçekleştirmiştir?						
Kurumun e-belge yönetimi politikasını belirleme	Hayır	Evet	Evet	Hayır	Hayır	Hayır
Kurumun e-arşiv yönetimi politikasını belirleme	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Fonksiyonlar ve iş süreçleri tanımlama ve belgelerle ilişkilendirme	Evet	Hayır	Hayır	Hayır	Hayır	Hayır
İş süreçlerine dair dokümantasyon oluşturma	Evet	Hayır	Hayır	Hayır	Hayır	Hayır
Form ve şablon oluşturma	Evet	Evet	Evet	Evet	Evet	Evet
Belge türüne göre oluşturulan şablonlar için bir kontrol numarası verme	Hayır	Evet	Evet	Hayır	Hayır	Hayır
Spesifik üstveri şemaları çıkarma	Evet	Hayır	Evet	Hayır	Evet	Hayır
Belge profilindeki form özelliklerini (belgedeki kişiler, antet, format, teknolojik özellikler, belgeye işlem safhasında yapılan açıklamalar gibi) tanımlama	Evet	Evet	Evet	Evet	Evet	Hayır
Belgeler ve dosyalar için dosya tasnif planı ve saklama planı hazırlama	Evet	Evet	Evet	Hayır	Evet	Evet
Dosya planına uygun dosyalama sistemi geliştirme	Evet	Hayır	Evet	Evet	Evet	Evet
Kontrollü terminoloji oluşturma	Hayır	Hayır	Evet	Hayır	Hayır	Hayır
Felaket kurtarma planı ve yedekleme planı oluşturma	Evet	Evet	Evet	Hayır	Evet	Evet
2. Belgenin aşağıdaki form özelliklerinden hangilerini üstverilerde kullanıyorsunuz?						
Sorumlu (Belgeyi üreten kurum)	Evet	Evet	Evet	Evet	Evet	Evet
Düzenleyen (Belgedeki irade beyanının sahibi)	Evet	Evet	Evet	Evet	Evet	Evet
Muhatap/Alıcı	Evet	Evet	Evet	Evet	Evet	Evet
Konu	Evet	Evet	Evet	Evet	Evet	Evet
Format	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Üretim tarihi	Evet	Evet	Evet	Evet	Evet	Evet
Gönderim/Alma tarihi (KEP)	Evet	Evet	Evet	Evet	Evet	Evet
Belge tarihi (Son imzalayıcının imza attığı tarih)	Evet	Evet	Evet	Evet	Evet	Evet
3. Belge profilinde aşağıdaki üstverilerden hangileri bulunmaktadır?						
Belgenin dosyasına kaldırıldığı zaman	Evet	Evet	Evet	Evet	Evet	Evet
Belgedeki işlemden sorumlu kişi ve birim	Evet	Evet	Evet	Evet	Evet	Evet
Ait olduğu işlem-dosya-seri-birim	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Dosya kodu	Evet	Evet	Evet	Evet	Evet	Evet
Belge referans numarası	Evet	Evet	Evet	Evet	Evet	Evet
Belgeye erişmek için asgari gereksinimler	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Belgenin üretildiği EBYS yazılımı ve versiyon numarası	Evet	Evet	Evet	Evet	Evet	Evet

Belge yönetimi için kullanılacak algoritmalar (kullanılan EBYS yazılımı algoritmaları ve belgeyi tekrardan üretmek ya da şifreli belgeleri açabilmek için gerekli olan algoritmalar gibi)	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Belge bileşenleri (Üstveri, belgenin ekleri, form elemanları, kontekst (bağlam), içerik, belgenin oluşumunu sağlayan veriler, iş akışları gibi)	Evet	Evet	Evet	Evet	Evet	Evet
E-imza ve zaman damgası	Evet	Evet	Evet	Evet	Evet	Evet
Saklama süresi	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Belgeye erişim profilleri	Evet	Evet	Evet	Evet	Evet	Evet
Belgelerin lokasyonu (Directory)	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Belgeye yapılan açıklama notları (İşlem safhasında (ivedilik durumu, iletim zamanı, tarih, yer, ekler gibi), kullanım safhasında (belgenin alındığı tarih, belgeyi kullanan birim, gerçekleştirilen işlem, yapılan muamele gibi) ve yönetim safhasında (belgenin arşive devir tarihi, versiyon numarası, belge referans numarası, dosya kodu, belgeyi düzenleyen ve oluşturan kişi/birim gibi))	Evet	Evet	Evet	Evet	Evet	Evet
Teknolojik göç ettirme ile ilgili yapılan işlemler	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Konu	Evet	Evet	Evet	Evet	Evet	Evet
Belgenin sayısı	Evet	Evet	Evet	Evet	Evet	Evet
Belgenin gizlilik derecesi (Tasnif dışı, hizmete özel, özel, gizli, çok gizli, kişiye özel gibi)	Evet	Evet	Evet	Evet	Evet	Evet
Dağıtım listesi	Evet	Evet	Evet	Evet	Evet	Evet
İlgilerin referans numarası	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Belgenin özet değeri	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Şifreleme bilgisi	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Eklerin referans numaraları	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
4. Belge bileşenleriyle ilgili aşağıdaki üstverilerden hangileri kurumunuzda kullanılmaktadır?						
Referans numarası	Evet	Evet	Evet	Evet	Evet	Evet
Format	Evet	Evet	Evet	Evet	Evet	Evet
Bileşeni üreten yazılım ve o yazılımda kullanılan algoritmalar	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Bileşene erişmek için asgari gereksinimler	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
5. Log kayıtlarında aşağıdaki bilgilerden hangileri bulunmaktadır?						
Dokümanın belgeye dönüşme tarih ve zamanı	Evet	Evet	Evet	Evet	Evet	Evet
Belgeye erişim istekleri	Evet	Evet	Evet	Evet	Evet	Evet
Belgenin iletim geçmişi	Evet	Evet	Evet	Evet	Evet	Evet
Belgeye yapılan açıklamalar	Evet	Evet	Hayır	Evet	Hayır	Hayır
Belgede yapılan işlemler ve bu işlemleri yapan kullanıcılar	Evet	Evet	Evet	Evet	Evet	Hayır
Üstverilerde yapılan değişiklikler	Evet	Evet	Hayır	Hayır	Hayır	Hayır
Saklama planı ve saklama sürelerinde yapılan değişiklikler	Evet	Evet	Hayır	Hayır	Hayır	Hayır
Belgede yaşanan teknolojik değişimler	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Sistem arıza ve bakımları	Evet	Evet	Evet	Evet	Evet	Evet
Paraf bilgileri ve paraflayanın yaptığı işlemler	Evet	Evet	Evet	Evet	Evet	Evet
6. Dosyalama pratikleriyle ilgili aşağıdakilerden hangileri kurumunuz için geçerlidir?						
Belgelerin hangi işlem, dosya, seri ve birime ait olduğunu seçme	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır

Dosya türü ayrımı yapılması (Konu, Vaka, Gölge dosya, Vaka hazırlık dosyası, melez/hibrit dosya gibi)	Evet	Evet	Evet	Evet	Evet	Evet
Konu dosyalarının periyodik olarak kapanması	Evet	Evet	Evet	Evet	Evet	Evet
Vaka dosyasına giren bir belgenin aynı zamanda bir konu dosyasıyla da ilişkiliyse çoğaltılmadan çapraz referans yapılması	Evet	Evet	Evet	Evet	Evet	Evet
Belgeler ve dosyalar için dosya konu kodunun yanı sıra gerektiğinde özel kodların kullanılması	Evet	Evet	Evet	Evet	Evet	Evet
Belgeye, birim belge yöneticisi tarafından da dosya kodu verilmesi	Evet	Evet	Evet	Evet	Evet	Evet
Birim belge yöneticisinin belgeyi ait olduğunu düşündüğü dosyaya gönderebilmesi	Evet	Evet	Evet	Evet	Evet	Evet
Dosyaların üstverilerinde ait olduğu seri ve birimin belirtilmesi	Evet	Evet	Evet	Evet	Evet	Evet
Dosyaların, ait oldukları seriden farklı bir seriye taşınabilmesi	Evet	Evet	Evet	Evet	Evet	Evet
Sistemde aynı dosyanın parçası olup kâğıt ortamında saklanan belgelerin yerinin belirtilmesi	Evet	Evet	Evet	Evet	Evet	Evet
Belgenin ve dosyanın dosya kodu değişmiş ise eski ve yeninin birlikte gösterilmesi	Evet	Evet	Evet	Evet	Evet	Evet
7. Belge yönetimiyle ilgili kurumsal prosedürler aşağıdakilerden hangilerini içermektedir?						
Belgenin üretilme kuralları	Evet	Evet	Evet	Evet	Evet	Hayır
Belgenin iletilme kuralları	Evet	Evet	Evet	Evet	Evet	Hayır
Dışarıdan gelen belgelerin sisteme kaydedilme kuralları	Evet	Evet	Evet	Evet	Evet	Hayır
Belgeyi dosyasına kaldırma kuralları	Evet	Evet	Hayır	Hayır	Hayır	Hayır
Belgenin tanımlanmasına ilişkin kurallar	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Belgeyi arşive devretme kuralları	Evet	Hayır	Hayır	Hayır	Hayır	Hayır
Belgelerin teknolojik göçü ve bu göçün geçerliliğine yönelik tasdik prosedürleri	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Log kayıtları	Evet	Evet	Hayır	Hayır	Hayır	Hayır
Denetim günlükleri	Evet	Evet	Hayır	Hayır	Hayır	Hayır
Donanımların çalışma şartları (sıcaklık ve nem gibi)	Evet	Hayır	Hayır	Hayır	Hayır	Hayır
Bilgi güvenliği	Evet	Evet	Evet	Hayır	Hayır	Hayır
8. Saklama süreli dosya planınız için aşağıdakilerden hangileri geçerlidir?						
Fonksiyon analizi yapılarak belge hiyerarşisinin oluşturulması	Evet	Hayır	Hayır	Hayır	Hayır	Hayır
Dosya ve seri kodlarının oluşturulması	Evet	Evet	Evet	Evet	Hayır	Hayır
Saklama süresi sonunda yapılacak tasfiye işlemlerinin kararlaştırılması	Evet	Evet	Evet	Hayır	Evet	Evet
Standart Dosya Planının kod ekleme/çıkarmayapılarak kullanılması	Evet	Evet	Evet	Evet	Evet	Evet
9. Teknolojik göçle ilgili aşağıdakilerden hangileri geçerlidir?						
Belgelerin taşıyıcı ortamının değiştirilip değiştirilmemesi hususunda düzenli aralıklarla incelemelerin yapılması	Hayır	Hayır	Hayır	Hayır	Evet	Hayır
Teknolojik göç sonrası belgelerin erişilebilirliği ve okunabilirliğinin kontrol edilmesi	Hayır	Hayır	Evet	Hayır	Hayır	Hayır
Yeni taşıyıcı ortam ve göçün gerçekleştiği tarihin belge profiline eklenmesi	Hayır	Hayır	Evet	Hayır	Hayır	Evet
Risk analizinin yapılması	Hayır	Hayır	Evet	Hayır	Hayır	Hayır
10. Yedeklemelerle ilgili aşağıdakilerden hangileri geçerlidir?						

Yedeklemelere sadece yetkili personelin erişmesi	Evet	Evet	Evet	Evet	Evet	Evet
Belgeler, belge profilleri ve üstverilerin düzenli aralıklarla yedeklenmesi	Evet	Evet	Evet	Evet	Evet	Evet
Son yedeklemeden bu yana belgelere yapılan açıklamalar ve işlemlerin denetim günlüklerine kaydedilmesi	Evet	Evet	Evet	Evet	Evet	Hayır
Sistem yedeklemesinin yapılması	Evet	Evet	Evet	Evet	Evet	Evet
Son üç yedeklemenin kopyalarının muhafaza edilmesi	Evet	Hayır	Evet	Hayır	Evet	Hayır
Denetim günlüklerine yedeklemenin başarılı gerçekleşip gerçekleşmediğinin eklenmesi	Evet	Hayır	Hayır	Evet	Hayır	Hayır
Herhangi bir sorun karşısında bir önceki yedeklemenin devreye alınabilmesi	Evet	Evet	Evet	Hayır	Evet	Evet
11. Yedekleme ile ilgili aşağıdaki üstverilerden hangileri sisteminizde mevcuttur?						
Yedeklemenin tarihi ve zamanı	Evet	Evet	Evet	Evet	Hayır	Evet
Yedeklemeyi onaylayan	Evet	Hayır	Hayır	Evet	Hayır	Hayır
Yedeklemenin konumu	Evet	Evet	Evet	Evet	Hayır	Evet
Yedekleme referans numarası	Evet	Evet	Evet	Evet	Hayır	Hayır
12. Arşive devredilecek belgelerle ilgili mevcut üstverilerin dışında onların delil değerini ilgilendirecek aşağıdaki üstverilerden hangilerinin kullanılması düşünülmektedir?						
Devir zamanı	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Belgelerin özgünlüğünü onaylayan teknikler (özet değeri kontrolü, e-imza sertifikalarının kontrolü, belgedeki kişi ile imzanın uyumu vb.)	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Belgelerin özgünlüğünü onaylayan kişiler	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Özgünlük değerlendirme raporu	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Belgenin tanımlama bilgileri	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
13. Belgelerin özgünlüğünün tasdik edilmesi için aşağıdaki adımlardan hangileri geçerlidir?						
Belgenin, doğduğu fonksiyonun işlemlerinden en az birini gösterecek nitelikte olması	Hayır	Evet	Evet	Hayır	Hayır	Hayır
Türüne göre belgenin, sahip olması gereken kimlik tespiti araçlarını (tasdik yöntemi) barındırması	Hayır	Evet	Evet	Hayır	Hayır	Hayır
Belge arşive devredildiğinde, onun özniteliklerinin korunduğunu gösteren bir elektronik kurumsal mührün kullanılması	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Belgenin tanımlama bilgilerinin incelenmesi	Hayır	Evet	Hayır	Hayır	Hayır	Hayır
Dosya sistemindeki (file system) belge ile veri tabanında tutulan kayıtların ilişkilendirilmesi ve bu ilişkinin kopmaması için gerekli tedbirlerin alınması	Evet	Hayır	Hayır	Hayır	Hayır	Hayır
Belge üzerindeki imzaların geçerliliği bitmeden EYP'nin zaman damgası ile damgalanması	Evet	Hayır	Evet	Hayır	Hayır	Hayır
Belgedeki imzaların arşiv imzası tipine dönüştürülmesi	Evet	Hayır	Evet	Hayır	Hayır	Hayır
Bütünlük analizinin düzenli kontrol edilmesi	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Bütünlük bozulması riskine karşı risk değerlendirmesi ve riskten kaçınma raporunun hazırlanması	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
14. Belgelerin tasfiyesine ilişkin aşağıdaki adımlardan hangileri geçerlidir?						
Belgeler oluşmadan önce belgelere bir saklama süresi tayin edilmesi	Evet	Evet	Evet	Hayır	Evet	Evet
Belgelerin saklama süreleri tamamlandıktan sonra ait oldukları dosyalarla birlikte arşive devredilmesi	Hayır	Hayır	Hayır	Hayır	Hayır	Evet

Saklama süresi aşımının gerekçesi	Evet	Hayır	Evet	Hayır	Evet	Evet
Belgenin, belge profili ve üstverileriyle birlikte arşive devredilmesi	Evet	Evet	Hayır	Hayır	Hayır	Evet
Belge tasfiye edilirken belge profili ve üstverisinin de tasfiye edilmesi	Evet	Evet	Hayır	Hayır	Hayır	Evet
Belge, ister arşive devredilsin ister imha edilsin referans numarasının sistemde tutulması ve belgenin akıbeti hakkında bir bilgi notunun bulunması	Evet	Hayır	Hayır	Hayır	Hayır	Hayır
Arşive devredilen belgelerin dosyalarıyla birlikte belge yönetim sisteminden kaldırılıp arşiv yönetim sistemine aktarılması	Evet	Evet	Hayır	Hayır	Hayır	Hayır
15. Belge yönetimi kapasitesinin geliştirilmesi için aşağıdakilerden hangileri geçerlidir?						
Kurumsal belge yönetimi politikasının oluşturulması	Evet	Evet	Evet	Hayır	Hayır	Hayır
Bilgi ve belge yönetimi mezunu kişilerin belge yönetimiyle ilgili birimde istihdam edilmesi	Evet	Hayır	Hayır	Hayır	Hayır	Hayır
Belge yönetimiyle ilgilenen personelin eğitim programının bulunması (eğitmen eğitimi)	Evet	Evet	Evet	Hayır	Evet	Hayır
Kurum çalışanlarının belge yönetimi birimi tarafından eğitilmesi	Evet	Evet	Evet	Hayır	Evet	Evet
TS 13298 Kurumsal sertifikasyon alınması yönünde girişimler yapılması	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
16. Arşivlenen belgelerin tanımlanması için bir standardın kullanılması düşünülmekte midir?	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
17. Elektronik belge yönetiminde belgenin delil değerini korumak için aşağıdaki teknolojilerden hangilerinin kullanılması düşünülmektedir?						
Blokzincir	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Yapay zekâ	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Derin öğrenme/Yapay öğrenme	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Elektronik delil elde etme (Digital forensics-Öykünme, teknolojik göç)	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
18. Yazılım ve donanımla ilgili aşağıdaki ifadelerden hangileri geçerlidir?						
Yazılım algoritması ve kaynak kodlarının kurum tarafından saklanması	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Veri tabanının arşivlenebilir bir formatta yapılandırılması	Evet	Evet	Evet	Hayır	Hayır	Hayır
Belgelerin bir kez yazılabilir ortamlarda saklanması	Hayır	Hayır	Evet	Hayır	Hayır	Hayır
Belge bileşenlerinin de belgeyle birlikte bütüncül olarak korunması	Evet	Evet	Evet	Hayır	Evet	Evet
Yazılım değiştirildiğinde de belgelere erişilebilmesi	Evet	Evet	Evet	Evet	Evet	Evet
Güncel belgelerle arşivlenen belgelerin saklanma konumları arasında bir ayrım yapılması	Hayır	Hayır	Hayır	Hayır	Evet	Hayır
Donanımların üreticilerin tavsiye ettiği kullanım ömrü dolduktan sonra kullanılmaması	Evet	Hayır	Evet	Evet	Evet	Evet
Belgelerin üretildiği araçlardaki donanım ve yazılım özelliklerinin kayıt altına alınması	Evet	Evet	Hayır	Evet	Hayır	Hayır
27001 Sertifikası alınması yönünde girişimlerin yapılması	Hayır	Evet	Evet	Evet	Evet	Evet
Yazılımın TS 13298 Sertifikasına uygun olması yönünde girişimlerin yapılması	Evet	Evet	Evet	Evet	Evet	Evet

Log kayıtlarının zaman damgası ile damgalanması	Evet	Hayır	Hayır	Evet	Evet	Evet
19. Üstveriler için aşağıdakilerden hangileri geçerlidir?						
Üstverilerin belgeden ayrı olarak XML ya da JSON olarak saklanması	Evet	Evet	Evet	Evet	Evet	Evet
Üstveriler, belge ile birlikte hareket etmektedir. (Belgenin konumu değiştirildiğinde üstverilerin de beraberinde taşınması)	Evet	Evet	Evet	Evet	Evet	Evet
Yöneticilerin yaptığı değişiklikler sonucunda yeni bir üstveri kaydının oluşması ve daha önceki üstveri kaydının muhafaza edilmesi	Evet	Hayır	Evet	Evet	Evet	Evet
Üstveri dosyasının ait olduğu belgenin referans numarasına sahip olması	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
20. Denetim günlükleri için aşağıdakilerden hangileri geçerlidir?						
Tüm belgeler için denetim günlüklerinin oluşturulması	Evet	Hayır	Hayır	Hayır	Hayır	Hayır
Denetim günlükleri oluşturulmasına karar verilen belgeler için, bunların otomatik olarak oluşması	Evet	Evet	Hayır	Hayır	Hayır	Hayır
Denetim günlüklerinin yapılan işlemlerin tarih ve saatini içermesi	Evet	Evet	Hayır	Hayır	Hayır	Hayır
Denetim günlüklerine erişim sırasında bir sorun yaşanıp yaşanmadığının düzenli aralıklarla otomatik olarak kontrol edilmesi	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Denetim günlüklerinin bir kere yazılması ve üzerinde hiç değişiklik yapılmaması	Evet	Evet	Hayır	Hayır	Hayır	Hayır
21. Kurumda üretilen ve dışarıdan gelen belgelerin form özellikleri, formatı ve içeriğinin değiştirilmemesine yönelik aşağıdaki hangi yaklaşımları benimsiyorsunuz?						
İz değeri kontrolü	Evet	Hayır	Evet	Hayır	Evet	Hayır
Dosya tanımlayıcı kullanımı (JHOVE, DROID gibi)	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Adli bilişim (Digital forensics) yöntemleri	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır
Log kayıtlarının kontrolü	Evet	Hayır	Hayır	Evet	Evet	Evet
Döngüsel artıklık denetimi (CRC)	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır

Tablo 3. Nicel Araştırma Anket Cevapları

EK 9. BELGE DÜZEYİNDEKİ SORULARDA ELDE EDİLEN PUANLAR

Sorular	S/Z	1	2	3	4	5	6
2. Belgenin aşağıdaki form özelliklerinden hangilerini üstverilerde kullanıyorsunuz?							
Sorumlu (Belgeyi üreten kurum)	Z	0.339	0.339	0.339	0.339	0.339	0.339
Düzenleyen (Belgedeki irade beyanının sahibi)	Z	0.339	0.339	0.339	0.339	0.339	0.339
Muhatap/Alıcı	Z	0.339	0.339	0.339	0.339	0.339	0.339
Konu	Z	0.339	0.339	0.339	0.339	0.339	0.339
Format	Z	-	-	-	-	-	-
Üretim tarihi	Z	0.339	0.339	0.339	0.339	0.339	0.339
Gönderim/Alma tarihi (KEP)	Z	0.339	0.339	0.339	0.339	0.339	0.339
Belge tarihi (Son imzalayıcının imza attığı tarih)	Z	0.339	0.339	0.339	0.339	0.339	0.339
3. Belge profilinde aşağıdaki üstverilerden hangileri bulunmaktadır?							
Belgenin dosyasına kaldırıldığı zaman	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Belgedeki işlemden sorumlu kişi ve birim	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Ait olduğu işlem-dosya-seri-birim	**KZ**	-	-	-	-	-	-
Dosya kodu	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Belge referans numarası	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Belgeye erişmek için asgari gereksinimler	Z	-	-	-	-	-	-
Belgenin üretildiği EBYS yazılımı ve versiyon numarası	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Belge yönetimi için kullanılacak algoritmalar (kullanılan EBYS yazılımı algoritmaları ve belgeyi tekrardan üretmek ya da şifreli belgeleri açabilmek için gerekli olan algoritmalar gibi)	**KZ**	-	-	-	-	-	-
Belge bileşenleri (Üstveri, belgenin ekleri, form elemanları, kontekst (bağlam), içerik, belgenin oluşumunu sağlayan veriler, iş akışları gibi)	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
E-imza ve zaman damgası	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Saklama süresi	Z	-	-	-	-	-	-
Belgeye erişim profilleri	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Belgelerin lokasyonu (Directory)	S	-	-	-	-	-	-

Belgeye yapılan açıklama notları (İşlem safhasında (ivedilik durumu, iletim zamanı, tarih, yer, ekler gibi), kullanım safhasında (belgenin alındığı tarih, belgeyi kullanan birim, gerçekleştirilen işlem, yapılan muamele gibi) ve yönetim safhasında (belgenin arşive devir tarihi, versiyon numarası, belge referans numarası, dosya kodu, belgeyi düzenleyen ve oluşturan kişi/birim gibi))	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Teknolojik göç ettirme ile ilgili yapılan işlemler	**KZ**	-	-	-	-	-	-
Konu	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Belgenin sayısı	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Belgenin gizlilik derecesi (Tasnif dışı, hizmete özel, özel, gizli, çok gizli, kişiye özel gibi)	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Dağıtım listesi	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
İlgilerin referans numarası	Z	-	-	-	-	-	-
Belgenin özet değeri	Z	-	-	-	-	-	-
Şifreleme bilgisi	Z	-	-	-	-	-	-
Eklerin referans numaraları	Z	-	-	-	-	-	-
4. Belge bileşenleriyle ilgili aşağıdaki üstverilerden hangileri kurumunuzda kullanılmaktadır?							
Referans numarası	Z	0.339	0.339	0.339	0.339	0.339	0.339
Format	Z	0.339	0.339	0.339	0.339	0.339	0.339
Bileşeni üreten yazılım ve o yazılımda kullanılan algoritmalar	S	-	-	-	-	-	-
Bileşene erişmek için asgari gereksinimler	Z	-	-	-	-	-	-
6. Dosyalama pratikleriyle ilgili aşağıdakilerden hangileri kurumunuz için geçerlidir?							
Belgelerin hangi işlem, dosya, seri ve birime ait olduğunu seçme	**KZ**	-	-	-	-	-	-
Dosya türü ayrımı yapılması (Konu, Vaka, Gölge dosya, Vaka hazırlık dosyası, melez/hibrit dosya gibi)	**KZ**	1.1427	1.1427	1.1427	1.1427	1.1427	1.1427
Konu dosyalarının periyodik olarak kapanması	S	0.1108	0.1108	0.1108	0.1108	0.1108	0.1108
Vaka dosyasına giren bir belgenin aynı zamanda bir konu dosyasıyla da ilişkiliyse çoğaltılmadan çapraz referans yapılması	S	0.1108	0.1108	0.1108	0.1108	0.1108	0.1108
Belgeler ve dosyalar için dosya konu kodunun yanı sıra gerektiğinde özel kodların kullanılması	S	0.1108	0.1108	0.1108	0.1108	0.1108	0.1108
Belgeye, birim belge yöneticisi tarafından da dosya kodu verilmesi	S	0.1108	0.1108	0.1108	0.1108	0.1108	0.1108
Birim belge yöneticisinin belgeyi ait olduğunu düşündüğü dosyaya gönderebilmesi	S	0.1108	0.1108	0.1108	0.1108	0.1108	0.1108

Dosyaların üstverilerinde ait olduğu seri ve birimin belirtilmesi	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Dosyaların, ait oldukları seriden farklı bir seriye taşınabilmesi	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Sistemde aynı dosyanın parçası olup kâğıt ortamında saklanan belgelerin yerinin belirtilmesi	Z	0.1356	0.1356	0.1356	0.1356	0.1356	0.1356
Belgenin ve dosyanın dosya kodu değişmiş ise eski ve yeninin birlikte gösterilmesi	S	0.1108	0.1108	0.1108	0.1108	0.1108	0.1108
8. Saklama süreli dosya planınız için aşağıdakilerden hangileri geçerlidir?							
Fonksiyon analizi yapılarak belge hiyerarşisinin oluşturulması	**KZ**	0.8748	-	-	-	-	-
Dosya ve seri kodlarının oluşturulması	Z	0.1356	0.1356	0.1356	0.1356	-	-
Saklama süresi sonunda yapılacak tasfiye işlemlerinin kararlaştırılması	S	0.1108	0.1108	0.1108	-	0.1108	0.1108
Standart Dosya Planının kod ekleme/çıkarma yapılarak kullanılması	S	0.1108	0.1108	0.1108	0.1108	0.1108	0.1108
12. Arşive devredilecek belgelerle ilgili mevcut üstverilerin dışında onların delil değerini ilgilendirecek aşağıdaki üstverilerden hangilerinin kullanılması düşünülmektedir?							
Devir zamanı	Z	-	-	-	-	-	-
Belgelerin özgünlüğünü onaylayan teknikler (özet değeri kontrolü, e-imza sertifikalarının kontrolü, belgedeki kişi ile imzanın uyumu vb.)	**KZ**	-	-	-	-	-	-
Belgelerin özgünlüğünü onaylayan kişiler	**KZ**	-	-	-	-	-	-
Özgünlük değerlendirme raporu	S	-	-	-	-	-	-
Belgenin tanımlama bilgileri	S	-	-	-	-	-	-
13. Belgelerin özgünlüğünün tasdik edilmesi için aşağıdaki adımlardan hangileri geçerlidir?							
Belgenin, doğduğu fonksiyonun işlemlerinden en az birini gösterecek nitelikte olması	Z	-	0.1356	0.1356	-	-	-
Türüne göre belgenin, sahip olması gereken kimlik tespiti araçlarını (tasdik yöntemi) barındırması	Z	-	0.1356	0.1356	-	-	-
Belge arşive devredildiğinde, onun özniteliklerinin korunduğunu gösteren bir elektronik kurumsal mührün kullanılması	S	-	-	-	-	-	-
Belgenin tanımlama bilgilerinin incelenmesi	S	-	0.1356	-	-	-	-
Dosya sistemindeki (file system) belge ile veri tabanında tutulan kayıtların ilişkilendirilmesi ve bu ilişkinin kopmaması için gerekli tedbirlerin alınması	Z	0.1356	-	-	-	-	-
Belge üzerindeki imzaların geçerliliği bitmeden EYP'nin zaman damgası ile damgalanması	Z	0.1356	-	0.1356	-	-	-

Belgedeki imzaların arşiv imzası tipine dönüştürülmesi	**KZ**	0.9951	-	0.9951	-	-	-
Bütünlük analizinin düzenli kontrol edilmesi	**KZ**	-	-	-	-	-	-
Bütünlük bozulması riskine karşı risk değerlendirmesi ve riskten kaçınma raporunun hazırlanması	S	-	-	-	-	-	-
14. Belgelerin tasfiyesine ilişkin aşağıdaki adımlardan hangileri geçerlidir?							
Belgeler oluşmadan önce belgelere bir saklama süresi tayin edilmesi	Z	0.1356	0.1356	0.1356	-	0.1356	0.1356
Belgelerin saklama süreleri tamamlandıktan sonra ait oldukları dosyalarla birlikte arşive devredilmesi	**KZ**	-	-	-	-	-	0.6102
Saklama süresi aşımının gerekçesi	Z	0.1356	-	0.1356	-	0.1356	0.1356
Belgenin, belge profili ve üstverileriyle birlikte arşive devredilmesi	**KZ**	0.6102	0.6102	-	-	-	0.6102
Belge tasfiye edilirken belge profili ve üstverisinin de tasfiye edilmesi	Z	0.1356	0.1356	-	-	-	0.1356
Belge, ister arşive devredilsin ister imha edilsin referans numarasının sistemde tutulması ve belgenin akıbeti hakkında bir bilgi notunun bulunması	**KZ**	0.6102	-	-	-	-	-
Arşive devredilen belgelerin dosyalarıyla birlikte belge yönetim sisteminden kaldırılıp arşiv yönetim sistemine aktarılması	Z	0.1356	0.1356	-	-	-	-
16. Arşivlenen belgelerin tanımlanması için bir standardın kullanılması düşünülmekte midir?	S	-	-	-	-	-	-
21. Kurumda üretilen ve dışarıdan gelen belgelerin form özellikleri, formatı ve içeriğinin değiştirilmemesine yönelik aşağıdaki hangi yaklaşımları benimsiyorsunuz?							
İz değeri kontrolü	Z	0.1356	-	0.1356	-	0.1356	-
Dosya tanımlayıcı kullanımı (JHOVE, DROID gibi)	**KZ**	-	-	-	-	-	-
Adli bilişim (Digital forensics) yöntemleri	S	-	-	-	-	-	-
Log kayıtlarının kontrolü	Z	0.1356	-	-	0.1356	0.1356	0.1356
Döngüsel artıklık denetimi (CRC)	S	-	-	-	-	-	-
Elde Edilen Puan Toplamı		11.5604	8.7843	9.194	7.4101	7.7921	9.0125
Başarı Yüzdesi (%)		46.27	35.16	36.81	29.66	31.18	36.07

Tablo 4. Belge Düzeyindeki Sorulara Verilen Cevaplar

EK 10. TEKNOLOJİK KOŞULLAR DÜZEYİNDEKİ SORULARDA ELDE EDİLEN PUANLAR

Sorular	S/Z	1	2	3	4	5	6
5. Log kayıtlarında aşağıdaki bilgilerden hangileri bulunmaktadır?							
Dokümanın belgeye dönüşme tarih ve zamanı	Z	0.571	0.571	0.571	0.571	0.571	0.571
Belgeye erişim istekleri	Z	0.571	0.571	0.571	0.571	0.571	0.571
Belgenin iletim geçmişi	Z	0.571	0.571	0.571	0.571	0.571	0.571
Belgeye yapılan açıklamalar	Z	0.571	0.571	-	0.571	-	-
Belgede yapılan işlemler ve bu işlemleri yapan kullanıcılar	Z	0.571	0.571	0.571	0.571	0.571	-
Üstverilerde yapılan değişiklikler	Z	0.571	0.571	-	-	-	-
Saklama planı ve saklama sürelerinde yapılan değişiklikler	Z	0.571	0.571	-	-	-	-
Belgede yaşanan teknolojik değişimler	Z	-	-	-	-	-	-
Sistem arıza ve bakımları	Z	0.571	0.571	0.571	0.571	0.571	0.571
Paraf bilgileri ve paraflayanın yaptığı işlemler	Z	0.571	0.571	0.571	0.571	0.571	0.571
9. Teknolojik göçle ilgili aşağıdakilerden hangileri geçerlidir?							
Belgelerin taşıyıcı ortamının değiştirilip değiştirilmemesi hususunda düzenli aralıklarla incelemelerin yapılması	S	-	-	-	-	0.1428	-
Teknolojik göç sonrası belgelerin erişilebilirliği ve okunabilirliğinin kontrol edilmesi	**KZ**	-	-	0.8494	-	-	-
Yeni taşıyıcı ortam ve göçün gerçekleştiği tarihin belge profiline eklenmesi	**KZ**	-	-	0.8494	-	-	0.8494
Risk analizinin yapılması	Z	-	-	0.2284	-	-	-
10. Yedeklemelerle ilgili aşağıdakilerden hangileri geçerlidir?							
Yedeklemelere sadece yetkili personelin erişmesi	S	0.1428	0.1428	0.1428	0.1428	0.1428	0.1428
Belgeler, belge profilleri ve üstverilerin düzenli aralıklarla yedeklenmesi	**KZ**	1.2349	1.2349	1.2349	1.2349	1.2349	1.2349
Son yedeklemeden bu yana belgelere yapılan açıklamalar ve işlemlerin denetim günlüklerine kaydedilmesi	Z	0.2284	0.2284	0.2284	0.2284	0.571	-
Sistem yedeklemesinin yapılması	**KZ**	1.2349	1.2349	1.2349	1.2349	1.2349	1.2349
Son üç yedeklemenin kopyalarının muhafaza edilmesi	S	0.1428	-	0.1428	-	0.1428	-

Denetim günlüklerine yedeklemenin başarılı gerçekleşip gerçekleşmediğinin eklenmesi	S	0.1428	-	-	0.1428	-	-
Herhangi bir sorun karşısında bir önceki yedeklemenin devreye alınabilmesi	Z	0.2284	0.2284	0.2284	-	0.2284	0.2284
11. Yedekleme ile ilgili aşağıdaki üstverilerden hangileri sisteminizde mevcuttur?							
Yedeklemenin tarihi ve zamanı	Z	0.2284	0.2284	0.2284	0.2284	-	0.2284
Yedeklemeyi onaylayan	**KZ**	1.4704	-	-	1.4704	-	-
Yedeklemenin konumu	S	0.1428	0.1428	0.1428	0.1428	-	0.1428
Yedekleme referans numarası	Z	0.2284	0.2284	0.2284	0.2284	-	-
17. Elektronik belge yönetiminde belgenin delil değerini korumak için aşağıdaki teknolojilerden hangilerinin kullanılması düşünülmektedir?							
Blokzincir	S	-	-	-	-	-	-
Yapay zekâ	S	-	-	-	-	-	-
Derin öğrenme/Yapay öğrenme	S	-	-	-	-	-	-
Elektronik delil elde etme (Digital forensics-Öykünme, teknolojik göç)	S	-	-	-	-	-	-
18. Yazılım ve donanımla ilgili aşağıdaki ifadelerden hangileri geçerlidir?							
Yazılım algoritması ve kaynak kodlarının kurum tarafından saklanması	**KZ**	-	-	-	-	-	-
Veri tabanının arşivlenebilir bir formatta yapılandırılması	S	0.1428	0.1428	0.1428	-	-	-
Belgelerin bir kez yazılabilir ortamlarda saklanması	S	-	-	0.1428	-	-	-
Belge bileşenlerinin de belgeyle birlikte bütüncül olarak korunması	Z	0.2284	0.2284	0.2284	-	0.2284	0.571
Yazılım değiştirildiğinde de belgelere erişilebilmesi	**KZ**	1.3134	1.3134	1.3134	1.3134	1.3134	1.3134
Güncel belgelerle arşivlenen belgelerin saklanma konumları arasında bir ayrım yapılması	S	-	-	-	-	0.1428	-
Donanımların üreticilerin tavsiye ettiği kullanım ömrü dolduktan sonra kullanılmaması	S	0.1428	-	0.1428	0.1428	0.1428	0.1428
Belgelerin üretildiği araçlardaki donanım ve yazılım özelliklerinin kayıt altına alınması	Z	0.2284	0.2284	-	0.2284	-	-
27001 Sertifikası alınması yönünde girişimlerin yapılması	Z	-	0.2284	0.2284	0.2284	0.2284	0.2284
Yazılımın TS 13298 Sertifikasına uygun olması yönünde girişimlerin yapılması	Z	0.2284	0.2284	0.2284	0.2284	0.2284	0.2284
Log kayıtlarının zaman damgası ile damgalanması	**KZ**	1.3134	-	-	1.3134	1.3134	1.3134
19. Üstveriler için aşağıdakilerden hangileri geçerlidir?							

Üstverilerin belgeden ayrı olarak XML ya da JSON olarak saklanması	Z	0.2284	0.2284	0.2284	0.2284	0.2284	0.2284
Üstveriler, belge ile birlikte hareket etmektedir. (Belgenin konumu değiştirildiğinde üstverilerin de beraberinde taşınması)	**KZ**	1.5988	1.5988	1.5988	1.5988	1.5988	1.5988
Yöneticilerin yaptığı değişiklikler sonucunda yeni bir üstveri kaydının oluşması ve daha önceki üstveri kaydının muhafaza edilmesi	Z	0.2284	-	0.2284	0.2284	0.2284	0.2284
Üstveri dosyasının ait olduğu belgenin referans numarasına sahip olması	Z	-	-	-	-	-	-
20. Denetim günlükleri için aşağıdakilerden hangileri geçerlidir?							
Tüm belgeler için denetim günlüklerinin oluşturulması	S	0.357	-	-	-	-	-
Denetim günlükleri oluşturulmasına karar verilen belgeler için, bunların otomatik olarak oluşması	Z	0.571	0.571	-	-	-	-
Denetim günlüklerinin yapılan işlemlerin tarih ve saatini içermesi	Z	0.571	0.571	-	-	-	-
Denetim günlüklerine erişim sırasında bir sorun yaşanıp yaşanmadığının düzenli aralıklarla otomatik olarak kontrol edilmesi	Z	-	-	-	-	-	-
Denetim günlüklerinin bir kere yazılması ve üzerinde hiç değişiklik yapılmaması	Z	0.571	0.571	-	-	-	-
Elde Edilen Puan Toplamı		18.2872	14.718	13.6476	14.5612	12.4342	12.427
Başarı Yüzdesi %		73.20	58.91	54.63	58.28	49.77	49.74

Tablo 5. Teknolojik Koşullar Düzeyindeki Sorulara Verilen Cevaplar

EK 11. KURUM DÜZEYİNDEKİ SORULARDA ELDE EDİLEN PUANLAR

Sorular	S/Z	1	2	3	4	5	6
1. Belge yönetimi sistemine geçerken kurum aşağıdaki prosedürlerden hangilerini gerçekleştirmiştir?							
Kurumun e-belge yönetimi politikasını belirleme	**KZ**	-	1.6971	1.6971	-	1.6971	-
Kurumun e-arşiv yönetimi politikasını belirleme	**KZ**	-	-	-	-	-	-
Fonksiyonlar ve iş süreçleri tanımlama ve belgelerle ilişkilendirme	**KZ**	1.6971	-	-	-	-	-
İş süreçlerine dair dokümantasyon oluşturma	S	0.222	-	-	-	-	-
Form ve şablon oluşturma	**KZ**	1.6971	1.6971	1.6971	1.6971	1.6971	1.6971
Belge türüne göre oluşturulan şablonlar için bir kontrol numarası verme	S	-	0.222	0.222	-	-	-
Spesifik üstveri şemaları çıkarma	Z	0.4208	-	0.4208	-	0.4208	-
Belge profilindeki form özelliklerini (belgedeki kişiler, antet, format, teknolojik özellikler, belgeye işlem safhasında yapılan açıklamalar gibi) tanımlama	S	0.222	0.222	0.222	0.222	0.222	-
Belgeler ve dosyalar için dosya tasnif planı ve saklama planı hazırlama	**KZ**	1.6971	1.6971	1.6971	-	1.6971	1.6971
Dosya planına uygun dosyalama sistemi geliştirme	Z	0.4208	-	0.4208	0.4208	0.4208	0.4208
Kontrollü terminoloji oluşturma	S	-	-	0.222	-	-	-
Felaket kurtarma planı ve yedekleme planı oluşturma	Z	0.4208	0.4208	0.4208	-	0.4208	0.4208
7. Belge yönetimiyle ilgili kurumsal prosedürler aşağıdakilerden hangilerini içermektedir?							
Belgenin üretilme kuralları	Z	1.052	1.052	1.052	1.052	1.052	-
Belgenin iletilme kuralları	Z	1.052	1.052	1.052	1.052	1.052	-
Dışarıdan gelen belgelerin sisteme kaydedilme kuralları	Z	1.052	1.052	1.052	1.052	1.052	-
Belgeyi dosyasına kaldırma kuralları	Z	1.052	1.052	-	-	-	-
Belgenin tanımlanmasına ilişkin kurallar	Z	-	-	-	-	-	-
Belgeyi arşive devretme kuralları	Z	1.052	-	-	-	-	-
Belgelerin teknolojik göçü ve bu göçün geçerliliğine yönelik tasdik prosedürleri	Z	-	-	-	-	-	-
Log kayıtları	Z	1.052	1.052	-	-	-	-
Denetim günlükleri	S	0.555	0.555	-	-	-	-
Donanımların çalışma şartları (sıcaklık ve nem gibi)	S	0.555	-	-	-	-	-
Bilgi güvenliği	Z	1.052	1.052	1.052	-	-	-

15. Belge yönetimi kapasitesinin geliştirilmesi için aşağıdakilerden hangileri geçerlidir?							
Kurumsal belge yönetimi politikasının oluşturulması	**KZ**	2.6822	2.6822	2.6822	-	-	-
Bilgi ve belge yönetimi mezunu kişilerin belge yönetimiyle ilgili birimde istihdam edilmesi	S	0.222	-	-	-	-	-
Belge yönetimiyle ilgilenen personelin eğitim programının bulunması (eğitmen eğitimi)	S	0.222	0.222	0.222	-	0.222	-
Kurum çalışanlarının belge yönetimi birimi tarafından eğitilmesi	S	0.222	0.222	0.222	-	0.222	0.222
TS 13298 Kurumsal sertifikasyon alınması yönünde girişimler yapılması	Z	-	-	-	-	-	-
Elde Edilen Puan Toplamı		18.6169	15.9493	14.3539	5.4959	8.4786	4.4578
Başarı Düzeyi %		74.52	63.84	57,45	22.00	33.94	17.84

Tablo 6. Kurum Düzeyindeki Sorulara Verilen Cevaplar

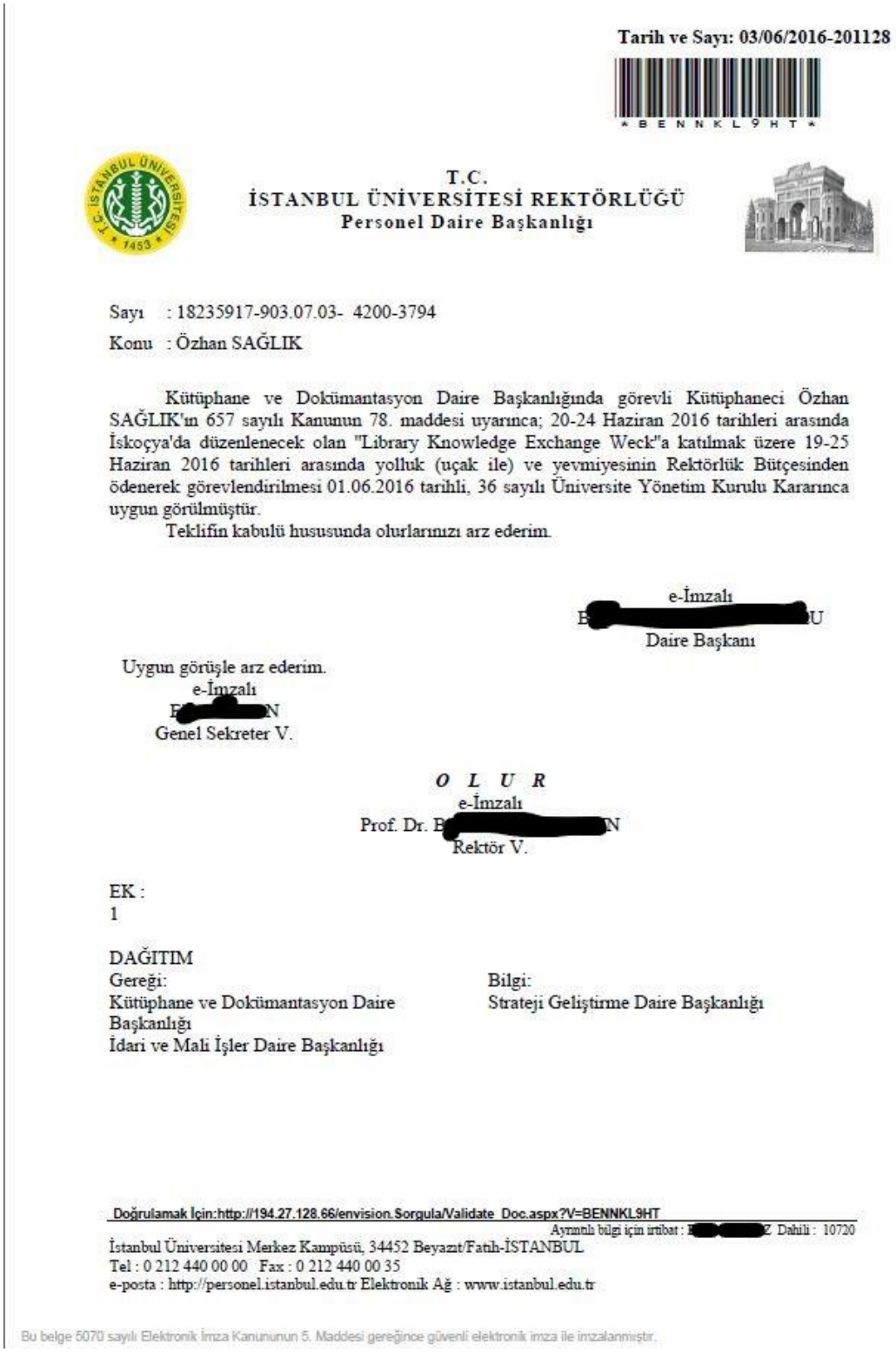
EK 12. ARŞİVSEL GÜVENİLİRLİK ÜSTVERİSİ

Üstveri	Güvenilirlik Düzeyi	Seçmeli/Zorunlu
KURUM		
E-belge yönetimi politika ve prosedürleri		Zorunlu
E-arşiv yönetimi politika ve prosedürleri		Zorunlu
İş süreçlerine dair dokümantasyonlar		Seçmeli
Form ve şablonlar		Zorunlu
Belge türü şablonları kontrol numaraları		Seçmeli
Spesifik üstveri şemaları		Zorunlu
Dosya tasnif ve saklama planları		Zorunlu
Kontrollü terminolojiler		Seçmeli
Felaket kurtarma ve yedekleme planları		Zorunlu
TEKNOLOJİK KOŞULLAR		
Dokümanın belgeye dönüşme tarih ve zamanı (Log kayıtlarında)		Zorunlu
Belgeye erişim istekleri (Log kayıtlarında)		Zorunlu
Belgenin iletim geçmişi (Log kayıtlarında)		Zorunlu
Belgeye yapılan açıklamalar (Log kayıtlarında)		Zorunlu
Belgede yapılan işlemler ve bu işlemleri yapan kullanıcılar (Log kayıtlarında)		Zorunlu
Üstverilerde yapılan değişiklikler (Log kayıtlarında)		Zorunlu
Saklama planı ve saklama sürelerinde yapılan değişiklikler (Log kayıtlarında)		Zorunlu
Belgede yaşanan teknolojik değişimler (Log kayıtlarında)		Zorunlu
Sistem arıza ve bakımları (Log kayıtlarında)		Zorunlu
Paraf bilgileri ve paraflayanın yaptığı işlemler (Log kayıtlarında)		Zorunlu
Belgelerin taşıyıcı ortamının değiştirilip değiştirilmemesi hususunda düzenli aralıklarla yapılan incelemelerin sonuçları		Seçmeli
Teknolojik göç sonrası belgenin erişilebilirliği ve okunabilirliğinin kontrol edilmesi		Zorunlu
Yeni taşıyıcı ortamın oluşturulması ve göçün gerçekleştiği tarih		Zorunlu
Teknolojik göç konusunda risk analiz raporları		Zorunlu
Yedeklemenin tarihi ve zamanı		Zorunlu
Yedeklemeyi onaylayan		Zorunlu
Yedeklemenin konumu		Seçmeli
Yedekleme referans numarası		Zorunlu
Yedeklemenin başarılı olup olmadığı (Log kayıtlarında)		Seçmeli
Yazılım algoritması		Zorunlu
Veri tabanı formatı		Seçmeli
Belgelerin saklama konumu		Seçmeli
Belgelerin üretildiği araçlardaki donanım ve yazılım özellikleri		Zorunlu
Log kayıtlarının zaman damgası ile damgalanması		Zorunlu
Üstveri dosyası formatı		Zorunlu
Yapılan işlemlerin tarih ve zamanı (Log kayıtlarında)		

Denetim günlüklerine erişimde sorun yaşanıp yaşanmadığı hususunda düzenli aralıklarla yapılan otomatik incelemelerin sonuçları		Zorunlu
BELGE		
Sorumlu (Belgeyi üreten kurum)		Zorunlu
Düzenleyen (Belgedeki irade beyanı sahibi)		Zorunlu
Muhatap/Alıcı		Zorunlu
Konu		Zorunlu
Belge formatı		Zorunlu
Belgenin üretim tarihi		Zorunlu
KEP aracılığıyla belgenin gönderim/alma tarihi		Zorunlu
Belge tarihi (Son imzalayıcının imza attığı tarih)		Zorunlu
Belgenin dosyasına kaldırıldığı zaman		Zorunlu
Belgenin ait olduğu işlem-dosya-seri-birim		Zorunlu
Dosya kodu		Zorunlu
Belge referans numarası		Zorunlu
Belgeye erişmek için asgari gereksinimler		Zorunlu
Belgenin üretildiği EBYS yazılımı ve versiyon numarası		Zorunlu
Belge yönetimi için kullanılacak algoritmalar		Zorunlu
Belge bileşenleri		Zorunlu
E-imza ve zaman damgası bilgileri		Zorunlu
Saklama süresi		Zorunlu
Belgeye erişim profilleri		Zorunlu
Belgenin konumu		Seçmeli
Belgeye yapılan açıklama notları		Zorunlu
Sayısal koruma için yapılan işlemler		Zorunlu
Belgenin sayısı		Zorunlu
Belgenin gizlilik derecesi		Zorunlu
Belgedeki ilgilerin referans numarası		Zorunlu
Belgenin özet değeri		Zorunlu
Şifreleme bilgisi		Zorunlu
Belgedeki eklerin referans numaraları		Zorunlu
Belgenin ait olduğu dosya türü		Zorunlu
Fiziksel ortamda saklanan belgelerin yeri		Zorunlu
Saklama süresi sonunda yapılacak tasfiye işlemleri		Seçmeli
Belgenin arşive devir zamanı		Zorunlu
Belgenin özgünlüğünü onaylayan teknikler		Zorunlu
Belgenin özgünlüğünü onaylayan kişiler		Zorunlu
Özgünlük değerlendirme raporu		Seçmeli
Belgenin tanımlama bilgileri		Seçmeli
Kurumsal mühür bilgileri		Seçmeli
EYP bilgileri		Zorunlu
Bütünlük analizinin düzenli kontrolünün sonuçları		Zorunlu
Bütünlük bozulması riskine karşı risk değerlendirmesi ve riskten kaçınma raporları		Seçmeli
Kullanılan dosya tanımlayıcılar		Zorunlu
Log kayıtlarına erişimde sorun yaşanıp yaşanmadığı hususunda düzenli aralıklarla yapılan otomatik incelemelerin sonuçları		Zorunlu

Tablo 7. Arşivsel Güvenilirlik Üstverisi

EK 13. E-İMZALI BELGE DOĞRULAMA ÖRNEKLERİ



Tarih ve Sayı: 03/06/2016-201128

BENNKL9HT

T.C.
İSTANBUL ÜNİVERSİTESİ REKTÖRLÜĞÜ
Personel Daire Başkanlığı

Sayı : 18235917-903.07.03- 4200-3794
Konu : Özhan SAĞLIK

Kütüphane ve Dokümantasyon Daire Başkanlığında görevli Kütüphaneci Özhan SAĞLIK'ın 657 sayılı Kanunun 78. maddesi uyarınca; 20-24 Haziran 2016 tarihleri arasında İskoçya'da düzenlenecek olan "Library Knowledge Exchange Weck"a katılmak üzere 19-25 Haziran 2016 tarihleri arasında yolluk (uçak ile) ve yevmiyesinin Rektörlük Bütçesinden ödenerek görevlendirilmesi 01.06.2016 tarihli, 36 sayılı Üniversite Yönetim Kurulu Kararınca uygun görülmüştür.

Teklifin kabulü hususunda olurlarınızı arz ederim.

e-İmzalı
[redacted]U
Daire Başkanı

Uygun görüşle arz ederim.
e-İmzalı
[redacted]N
Genel Sekreter V.

O L U R
e-İmzalı
Prof. Dr. [redacted]N
Rektör V.

EK :
1

DAĞITIM
Gereği:
Kütüphane ve Dokümantasyon Daire Başkanlığı
İdari ve Mali İşler Daire Başkanlığı

Bilgi:
Strateji Geliştirme Daire Başkanlığı

Doğrulamak İçin:http://194.27.128.66/envision.Sorgula/Validate_Doc.aspx?V=BENNKL9HT

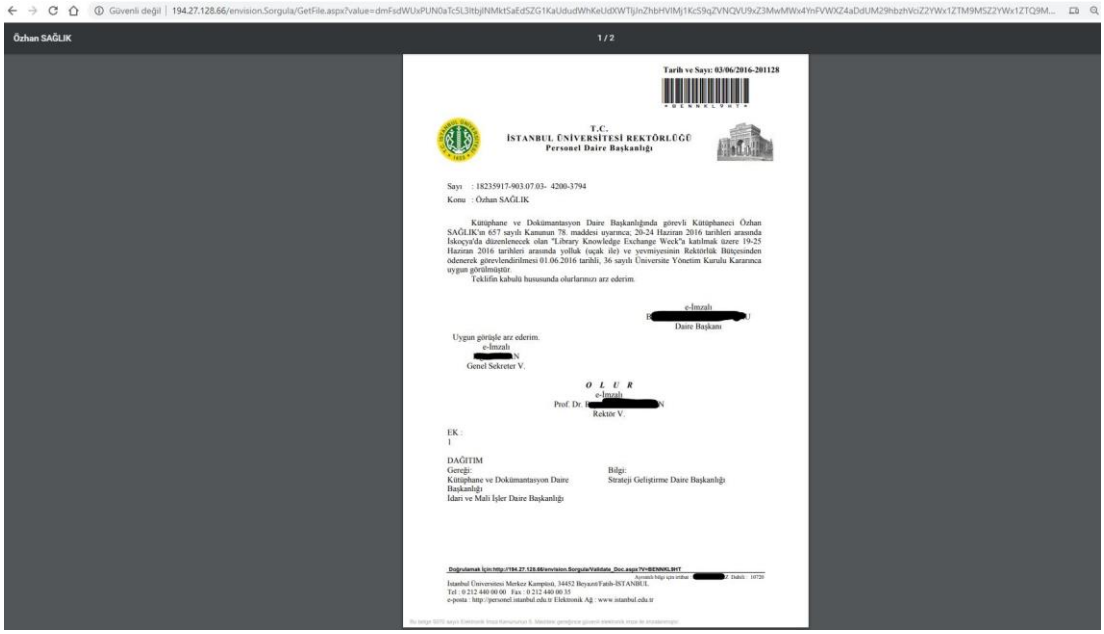
Ayrıntılı bilgi için irtibat : [redacted]Z Dahili : 10720

İstanbul Üniversitesi Merkez Kampüsü, 34452 Beyazıt/Fatih-İSTANBUL
Tel : 0 212 440 00 00 Fax : 0 212 440 00 35
e-posta : http://personel.istanbul.edu.tr Elektronik Ağ : www.istanbul.edu.tr

Bu belge 5070 sayılı Elektronik İmza Kanununun 5. Maddesi gereğince güvenli elektronik imza ile imzalanmıştır.

Şekil 48. İstanbul Üniversitesinde Görevlendirme Oluru

Şekil 49. Görevlendirme Olurunun Doğrulama İşlemleri



Şekil 50. Görevlendirme Olurunu Doğrulama

Şekil 51. Belge Doğrulama Kodu

ÖZGEÇMİŞ

Özhan Sağlık, 2012 yılında İstanbul Üniversitesi Bilgi ve Belge Yönetiminden mezun olmuş, aynı bölümde "İstanbul'daki İlçe Belediyelerinin Stratejik Planları ile Performans Programlarında Bilgi ve Belge Odaklı Hizmetlerin Yeri" adlı teziyle 2015 yılında yüksek lisansını tamamlamıştır. 2013-2017 yılları arasında İstanbul Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığında kütüphaneci olarak çalışmıştır. 2017 yılından itibaren Bursa Uludağ Üniversitesinde öğretim görevlisi olarak görev yapmaktadır. Sağlık, Türk Arşivciler Derneği ve Türk Kütüphaneciler Derneğinin üyesidir. Ayrıca, Open Preservation Foundation ve Digital Preservation Coalition gibi sivil toplum kuruluşlarıyla birlikte çeşitli çalışmalar gerçekleştirmiştir. E-belge yönetimi, arşivcilik ve stratejik planlama üzerine yayınlanmış makaleleri bulunmaktadır. Çeşitli kurumlarda elektronik belge ve arşiv yönetimi programlarının geliştirilmesinde görev almıştır.