

T.C.
MARMARA ÜNİVERSİTESİ
TÜRKİYAT ARAŞTIRMALARI ENSTİTÜSÜ
BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

DİJİTAL ÇAĞDA DOĞUŞTAN DİJİTAL BELGELERİN BİLGİ
YÖNETİM SÜREÇLERİ: KURUMDAN ARŞİVE GİDEN YOL

DOKTORA TEZİ

EMİNE CENGİZ MATER

İSTANBUL, 2022

T.C.
MARMARA ÜNİVERSİTESİ
TÜRKİYAT ARAŞTIRMALARI ENSTİTÜSÜ
BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

**DİJİTAL ÇAĞDA DOĞUŞTAN DİJİTAL BELGELERİN BİLGİ
YÖNETİM SÜREÇLERİ: KURUMDAN ARŞİVE GİDEN YOL**

DOKTORA TEZİ

EMİNE CENGİZ MATER
TEZ DANIŞMANI:
PROF. DR. AHMET OĞUZ İCİMSOY

İSTANBUL, 2022

İÇİNDEKİLER

İÇİNDEKİLER	I
ÖNSÖZ	IV
ÖZET	VI
ABSTRACT	VIII
KISALTMALAR	X
TABLolar LİSTESİ	XI
ŞEKİLLER LİSTESİ	XIII
BİRİNCİ BÖLÜM	1
1. GİRİŞ	1
1.1. Araştırmanın Amacı	5
1.2. Araştırma Problemi ve Araştırma Soruları	6
1.3. Araştırmanın Hipotezleri	6
1.4. Araştırmanın Kapsamı ve Sınırlılıkları	7
1.5. Özgün Değer	8
1.6. Araştırma Yöntemi, Veri Toplama ve Değerlendirme Teknikleri	9
1.7. Araştırma Düzeni	11
1.8. Kaynaklar	12
İKİNCİ BÖLÜM	14
2. LİTERATÜR DEĞERLENDİRMESİ	14
2.1. Doğuştan Dijital Belgelerin Milli Arşive Transferi İlgili Yapılan Uluslararası Çalışmalar	25
2.2. Doğuştan Dijital Belgelerin Bilgi Yönetim Süreçleri ile İlgili Türkiye’de Durum ve Yapılan Çalışmalar	29
ÜÇÜNCÜ BÖLÜM	34
3. KURUMSAL BİLGİ YÖNETİMİ VE SÜREÇLERİ	34
3.1. Kurumsal Bilgi Yönetimi Modelleri	36
3.2. Yasal Düzenlemeler ve Standartlar Işığında Türkiye’deki Kurumsal Bilgi Yönetiminin Mevcut Durumu	38
DÖRDÜNCÜ BÖLÜM	51
4. DOĞUŞTAN DİJİTAL BELGE VE BİLGİ YÖNETİM SÜREÇLERİ	51
4.1. Doğuştan Dijital Belgelerin Milli Arşive Transfer Aşamaları	52
4.1.1. Dijital Değerlendirme (Appraisal)	52

4.1.2.	Dijital Seçim/ Ayıklama (Selection).....	55
4.1.3.	Hassasiyet Değerlendirmesi (Sensitivity Review).....	56
4.1.4.	Uygulamada Dijital Değerlendirme, Dijital Ayıklama ve Hassasiyet Değerlendirmesi	59
4.1.5.	Transferi Planlama	63
4.1.6.	Kontrol Aşaması ve Erişim.....	64
4.2.	Dijital Süreklilik (Digital Continuity).....	64
4.2.1.	Dijital Sürekliliğin Önemi	64
4.2.2.	Dijital Sürekliliğin Sağlanması ve Yönetilmesi.....	65
4.2.3.	Bilgi Varlıkları	68
4.3.	Belge Yönetimi Süreçlerinde Politikalar ve Önemi	71
4.3.1.	Belge Yönetimi Politika Türleri ve Başlıkları	73
4.4.	Dijital Koruma (Digital Preservation).....	78
4.4.1.	Dijital Korumanın Önemi	81
4.4.2.	Dijital Koruma Modelleri	81
4.4.3.	Dijital Korumanın Riskleri ve Zorlukları	85
4.4.4.	Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmeliğin Dijital Süreklilik ve Uzun Vadeli Koruma Açısından İncelenmesi .	88
4.4.5.	Dijital Koruma İçin Faydalı Çalışmalar, Araçlar ve Sistemler.....	89
BEŞİNCİ BÖLÜM.....		94
5. DOĞUŞTAN DİJİTAL BELGELERİN ARŞİVE TRANSFERİ SÜRECİ İLE İLGİLİ YAKLAŞIMLAR, ULUSAL VE ULUSLARARASI ÇALIŞMALAR		94
5.1.	İngiltere – İngiliz Milli Arşivi /TNA (The National Archives)	94
5.2.	Avustralya-Avustralya Milli Arşivi/National Archives of Australia (NAA)...	99
5.3.	Amerika Birleşik Devletleri–ABD Milli Arşivi/The National Archives and Records Administration (NARA)	101
5.4.	Fransa-Fransa Milli Arşivi/France National Archives	103
5.5.	Yeni Zelanda–Yeni Zelanda Milli Arşivi/Archives New Zealand	103
5.6.	Hollanda–Hollanda Milli Arşivi/ Netherlands National Archives.....	107
5.7.	Macaristan-Macaristan Milli Arşivi/Hungarian National Archives.....	107
5.8.	İsviçre–İsviçre Federal Arşivi/Swiss Federal Archives.....	108
5.9.	Estonya–Estonya Milli Arşivi/ The National Archives of Estonia	109
5.10.	İrlanda –İrlanda Milli Arşivi/National Archives of Ireland	112
5.11.	İskoçya–İskoçya Milli Arşivi/ National Records of Scotland (NRS)	112
5.12.	Danimarka–Danimarka Milli Arşivi/The Danish National Archives.....	113
5.13.	Türkiye–Türkiye Cumhuriyeti Cumhurbaşkanlığı Devlet Arşivleri	115

ALTINCI BÖLÜM	117
6. BULGULAR VE ANALİZLERİN DEĞERLENDİRİLMESİ	117
6.1. Anket Bulgularının Değerlendirilmesi	117
6.1.1. Genel Bilgilere İlişkin Bulgular.....	117
6.1.2. Dijital Belge ve EBYS	119
6.1.3. Dijital Belgeler için Bilgi Varlığı, Saklama Planı, Dosya Formatları ve Dijital Süreklilik	124
6.1.4. Uzun Vadede Erişilebilirlik, Koruma, Üst Veri ve Tanımlama Süreçleri.....	135
6.1.5. Dijital Belgelerin E-Değerlendirme, E-Ayıklama, Hassasiyet Değerlendirmesi Süreçleri	141
6.1.6. Politika, Eğitim ve Milli Arşive Transfer Süreci	144
6.2 Doğuştan Dijital Belgelerin Bilgi ve Belge Yönetim Süreçleri Kavram Haritası... ..	153
6.2.1 Kavram Haritası Genel Görünüm.....	154
6.2.1.1 Dijital Belge Bölümü	155
6.2.1.2 Dijital Süreklilik Bölümü.....	156
6.2.1.3 Dijital Koruma Bölümü	157
6.2.1.5 Milli Arşiv Bölümü.....	159
6.3. Analizlerin Değerlendirilmesi.....	160
6.3.1. Araştırma Hipotezleri	160
6.3.2. Basit Doğrusal Regresyon Testi Analiz ve Yorumları	161
6.3.3. Bağımsız Örneklem T Testi Analizleri ve Yorumları	165
6.3.4. ANOVA Testi Analizleri ve Yorumları.....	167
6.3.5. Mann-Whitney U Testi Analizleri ve Yorumları.....	178
YEDİNCİ BÖLÜM	179
7. SONUÇ VE ÖNERİLER	179
KAYNAKÇA.....	189
EKLER	211

ÖNSÖZ

Doğuştan dijital belgelerin milli arşive transferi bilgi ve belge yönetimi alanında güncel takip edilmesi gereken konulardan biridir. Uluslararası alanda bu konudaki teorik ve uygulamalı çalışmaların yıllar önce başladığı görülmektedir. Türkiye’de dijital belgelerin milli arşive transferi henüz başlamamış olsa da önümüzdeki dönemlerde dijital belgelerin milli arşive transferi başlayacaktır. Bu doktora tezi bu konudaki eksiklikleri kapatmaya, çalışmalar sırasında yaşanacak olan sorunlara yol göstermeye yönelik yapılmıştır. Araştırma sürecinde Türkiye’de 120 kuruma anket uygulanmıştır. Literatürden ve saha araştırmasından elde edilen bulgular ışığında doğuştan dijital belgelerin bilgi yönetim süreçleri ele alınmış ve konuya ait sorunlara çözüm önerileri getirilmiştir.

Tez konumun filizlenmesinde, bir ağaç olup yeşermesinde büyük katkısı olan, ders süreci ve tez yazımı boyunca elimi hiç bırakmayan, bir danışmandan daha fazlası olan Dr. Öğr. Üyesi Lale ÖZDEMİR ŞAHİN hocama ne kadar teşekkür etsem az. Danışman hocamın görev değişikliği sebebi ile son yıl danışmanlığımı üstlenen Prof. Dr. Ahmet Oğuz İCİMSOY hocama hem ders sürecinde hem tez sürecinde bilgi ve birikimlerinden yararlanmama olanak sağlaması sebebiyle içtenlikle teşekkür ederim.

Tez savunma jürime katılma inceliği gösteren ve tezin yapılandırılmasında katkı sağlayan Prof. Dr. Remziye Tüba KARATEPE, Prof. Dr. Ümit KONYA ve Doç. Dr. Bahattin YALÇINKAYA hocalarıma teşekkürü borç bilirim.

Doktora ders döneminde “Emine, aklına geleni her zaman yazıya dök, bunlar sonra çok işine yarayacak.” diyerek bana farklı bir pencereden bakma fırsatı sağlayan, verdiği her bilgi farklı bir ışık olan sevgili Prof. Dr. Remziye Tüba KARATEPE hocama çok teşekkür ederim.

Tezin anket soruları ve yapılandırılması sırasında ve istatistiki hesaplamalarında bilgi ve birikiminden yararlandığım, yoğun temposunda çalışmama mekân ve zamandan bağımsız olarak katkı sunan Doç. Dr. Bahattin YALÇINKAYA hocama çok teşekkür ederim. Tezin istatistiki hesaplamalarında bilgisinden yararlandığım meslektaşım Öğr. Gör. Oytun CİBAROĞLU’na ne kadar teşekkür etsem az. Tez ile ilgili ihtiyacım olan bilgilere ulaşmama katkı sağlayan Araş. Gör. M. Emin GEDİKLİ’ye teşekkür ederim.

Tezin saha arařtırmasında desteklerini sunan Devlet Arřivleri Bařkanlıęı Bilgi İřlem ve Elektronik Arřiv Dairesi Bařkanı Alparslan BAřAR ve Cumhurbaşkanlıęı Bilgi ve Belge Yönetimi Daire Bařkanı Serkan MENTEř'e çok teřekkür ederim.

Tezin saha arařtırmasında çalıřmaya katkı sunan, anket sorularını cevaplayan tüm meslektařlarıma ve çalıřanlara teřekkürü borç bilirim.

Marmara Üniversitesi Kütüphane ve Dokümantasyon Daire Bařkanlıęı'nda birlikte çalıřtığım ve bu süreçte bana destek olan mesai arkadaşlarıma teřekkür ederim.

Üniversite ve çalıřma hayatım boyunca benden desteęini esirgemeyen, her konuda yol gösteren, ben dâhil çevresindeki herkese önce iyi insan olmayı ařılayan, sürekli okuyan ve üreten sevgili Prof. Dr. Bülent YILMAZ hocama ne zaman istersem yanımda olduęu için teřekkür ederim. İyi ki varsınız!

Eęitim hayatım boyunca maddi ve manevi desteklerini esirgemeyen, her zaman yanımda olan canım aileme teřekkür ederim. Sizlerin desteęi olmadan bu tez tamamlanamazdı.

Bitmek bilmeyen yoğun ve uykusuz gecelerde hep yanımda olan, tez yazma sürecimi eğlenceli hale getiren hayat arkadaşım Murat Sina MATER'e minnettarım. İyi ki varsın!

Eęitim hayatımın çok büyük ve önemli bir kısmında beni maddi ve manevi destekleyen, bugünlere gelmemde emeęi çok büyük olan yengem Nermin CENGİZ ve amcam Prof. Dr. Bahaettin CENGİZ'e çok teřekkür ederim.

Tezimi bitirdiğimde ilk aramak ve mutluluęumu paylaşmak istediğim, hep örnek aldığım ve gurur duyduğum amcam Prof. Dr. Bahaettin CENGİZ bugün aramızda yok... En çok mutlu olacak ve gurur duyacak kiři de kendisiydi. Bir yerlerden beni görebildiğini biliyorum amcacım. Sana verdiğim sözü tuttum. Bu tezi sana ithaf ediyorum!

İstanbul, 2022

ÖZET

CENGİZ MATER, Emine. Dijital Çağda Doğuştan Dijital Belgelerin Bilgi Yönetim Süreçleri: Kurumdan Arşive Giden Yol. Doktora Tezi, İstanbul.

Bilgi çağı olarak da adlandırılan dijital çağ; teknolojiyi ön plana çıkaran ve teknolojiyi kullanan bir çağ olmasıyla hayatımızı etkilemiştir. Bu etki birçok alanda eğitim, kültür, yönetim gibi kendisini göstermiştir. Bu alanlardan biri de kuşkusuz Bilgi ve Belge Yönetimi'dir. Dijital çağda meydana gelen değişimlerle birlikte belgelerin oluşturulma ve kullanım şekillerinde değişiklikler meydana gelmiştir. Geleneksel yöntemlerle kâğıt ortamında üretilen bilgi ve belgeden, dijital ortamda üretilen/doğan bilgi ve belgeye (born-digital record) geçiş söz konusudur. Genel olarak yurtdışında, dijital belgelerin arşive transferi konusunda bir farkındalık ve bu konunun zorlukları hakkında bir bilinç bulunmaktadır. Yapılan literatür taramasına göre konu ile ilgili çalışmalar ve projeler başlamış ve devam etmektedir. Türkiye'de ise dijital belge süreci var fakat bundan sonraki süreç ile ilgili eksik bir yol haritası mevcuttur. Konu ile ilgili bir yol haritasının ya da bir başka deyişle resmi bir politikanın olmayışı, bu konudaki çalışmaları da kısıtlamaktadır. Çalışmamızın amaçları; dijital çağ ile birlikte Türkiye'deki kamu kurumlarında dijital belgelerin kurumsal bilgi yönetim süreçlerinin nasıl işlediği ortaya koymak, Türkiye'de kamu kurum ve kuruluşlarının dijital belgelerin kurumsal bilgi yönetim süreçlerinde karşılaşılabileceği zorlukları belirlemek, kurumlarda dijital belgelerin ayıklanması, değerlendirmesi, hassasiyet değerlendirmesi, dijital süreklilik ve uzun süreli koruma konularında izlenen yol ve yöntemleri ortaya çıkarmak, Türkiye'de dijital belgelerin milli arşive transferi konusunda kurumlara farkındalık sağlamak ve Türkiye'deki dijital belgelerin kurumsal bilgi yönetim süreçleri ile ilgili bir desen (kavram haritası) geliştirmek olarak belirlenmiştir.

Türkiye'de kamu kurum ve kuruluşlarında dijital belgelerin kurumsal belge yönetim süreçleri (dijital belgelerin arşive transferi) ile ilgili resmi çalışmalar henüz netleşmemiştir ve bu konuda yaşanacak olan sorunların yeterince tespit edilmediği ve bu sorunlara yönelik çözüm önerilerinin gerekliliği bilinmektedir. Çalışmanın problemi; "Türkiye'de kamu kurumlarında doğuştan dijital belgelerin kurumsal bilgi yönetim süreçleri uygulama aşamalarında ulusal ve kurumsal boyutlarda farkındalık eksikliği, teknik ve hukuksal altyapı yetersizliği yaşanmaktadır" şeklinde oluşturulmuştur. Araştırmanın temel hipotezi; "Türkiye'de kamu kurumlarında doğuştan dijital belgelerin

kurumdan arşive transfer aşamasına kadar gerekli olan bilgi ve belge yönetimi süreçlerinin teknik ve hukuksal altyapısı yeterli/beklenen düzeyde değildir” şeklinde tanımlanmıştır.

Araştırma için bahsedilen bu süreçler sadece dijital belgelerin arşive transferi için değil kurumsal, verimli ve etkin bir bilgi yönetim süreci için de gereklidir. Bilginin istendiğinde bulunabilmesi, hassas olup olmadığını bilmek, kullanılan dosya formatlarının sürdürülebilir olup olmadığını bilmek, bu ve benzeri tüm unsurlar etkin bir bilgi yönetim süreci ile ilgilidir. Bu bağlamda çalışma sadece dijital belgelerin arşive transferi olarak düşünülmemeli, kavramlar ve süreçler daha geniş düşünülmesi ve önemsenmelidir.

Araştırmanın kapsamını Türkiye’de dijital belgelerin bilgi yönetim süreçlerine dair veri sağlayabilecek kamu kurum ve kuruluşları ile Devlet Arşivleri Başkanlığı tarafından yayımlanan 2020-2024 Stratejik Planında yer alan dış paydaşlar olarak iş birliği yapılan kurumlar oluşturmaktadır. İlgili kurumlarla anket çalışması yapılmıştır.

Bu çalışma Türkiye’deki dijital belgelerin kurumsal bilgi yönetim süreçlerini konu alan ilk akademik araştırmadır. Konumuz Türkiye’de uygulamada ve teoride henüz kapsamlı olarak ele alınmadığından önemlidir. Ülkemizde konu ile ilgili teknik altyapı istenilen düzeyde değildir. Ayrıca kurumlarda çalışan personelin bu konuda arzu edilen düzeyde bilgi farkındalığı bulunmamaktadır. Bu çalışmanın alanımızdaki önemli açığı bir nebze olsun kapatacağı ve ileride benzeri çalışmalara destek olacağı inancındayız. Çalışmamızın Türkiye’deki kamu kurumlarında dijital belgelerin kurumsal bilgi yönetimi süreçleri konusunda bir farkındalık oluşturması beklenmektedir. Çalışmanın aynı zamanda Türkiye’de dijital belgelerin arşive transferi uygulamaya konulduğu zaman yaşanacak olan zorluklara yol göstermesi de umulmaktadır.

Anahtar Kelimeler

Dijital belge; Kurumsal bilgi yönetim süreçleri; Dijital transfer; Belge yönetimi; Dijital değerlendirme; Dijital ayıklama; Hassasiyet değerlendirmesi; Dijital süreklilik; Dijital koruma; Türk kamu sektörü

ABSTRACT

CENGİZ MATER, Emine. From the Public Body to the Archives: Information Management Processes for Born-digital Records in the Digital Era. Doctoral Thesis. Istanbul

The digital age, also called the information age, has influenced our lives as it is an era where technology and its use is emphasised. The effect of the technological age has been witnessed in many fields including education, culture and management. One of these areas is undoubtedly Information and Records Management. The changes in the digital age, have also impacted on, and changed the way records are created, and the way in which they are used. There has been a transition from paper medium based information and records managed with traditional methods to digital information information, where born records are produced in digital media. Generally speaking, internationally, there is an awareness of the processes relating to the transfer of digital records to the archive, and also an awareness of its difficulties. A review of the literature on the subject reveals that research globally on the subject is underway. In Turkey, there are processes and standards for the management of digital records, however the absence of a road map or formal government policy on certain areas such as digital transfer, restricts the work on this issue. Within this framework, the objectives of this study are as follows; to provide a situational analysis of information management in Turkey in the digital age, to identify the challenges faced by the Turkish public sector in terms of digital information management, to reveal the methods followed in the digital appraisal, selection and transfer, digital continuity and long-term preservation of digital records in institutions, to raise awareness of institutions on the transfer of digital records to the national archive in Turkey and to develop a pattern (mindmap) of corporate information management processes of digital records in Turkey.

Processes relating to born-digital records in the Turkish public sector that provide guidance on how to transfer digital records to the archives, do not exist. The problem statement of the study at hand is, "Turkish public sector organisations lack the desired level of awareness, technical and legal infrasturcture for the implementation of processes for digital information and records management leading to digital transfer ". The basic hypothesis of the research of the study is; "To determine whether Turkish public sector organisations lack the desired level of awareness, technical and legal infrasturcture for

the implementation of processes for digital information and records management leading to digital transfer ".

These processes mentioned above (which also include digital appraisal, selection and transfer) are required not only for the transfer of born-digital records to the archives, but also for effective and efficient corporate information management. To ensure the availability of information when requested, to know if it is sensitive or not, to know which file formats used are sustainable, etc are all related to effective information management processes. The failure of one of these processes will surely impact on others, too.

The scope of the research comprises of obtaining authentic data from various Turkish sector public bodies that will render the data obtained during the research meaningful and reliable and the institutions that cooperate as external stakeholders included in the 2020-2024 strategic plan published by the Presidency of State Archives. A survey was conducted with the relevant institutions.

This thesis will be the first of its kind in Turkey that focuses on born-digital records within the context of digital information management processes. In Turkey, the technical infrastructure on the subject is not at the desired level. In addition, there is a lack of awareness about this issue amongst staff working in the public sector. With the completion of the relevant work, a comprehensive resource in the field will become available. In addition, this will close the important gap that exists with regard to this area. It is expected that the research will increase awareness of the required processes for the realisation of digital information management from the public body to the archives. Challenges faced by the Turkish public sector in Turkey will be used to promote and implement new ways of working required to manage digital information to the point of digital transfer.

Keywords

Born-digital records; Corporate information management processes; Digital transfer; Records management; Digital appraisal; Digital selection; Sensitivity review; Digital continuity; Digital preservation; Turkish public sector

KISALTMALAR

ABD	Amerika Birleşik Devletleri
BGYS	Bilgi Güvenliği Yönetim Sistemleri
COPTR	Community Owned Digital Preservation Tool Registry
EBYS	Elektronik Belge Yönetim Sistemi
ELAS/RM	Elektronik Arşivleme Sistemi Referans Modeli
DAB	Devlet Arşivleri Başkanlığı
DPC	Digital Preservation Coalition
DPM	Digital Preservation Model
DROID	Digital Record Object Identification
ISO	International Standard Organization
JHOVE	Harvard Object Validation Environment
NARA	The National Archives and Records Administration
NLP	Natural Language Processing
NRS	National Records of Scotland
SDP	Standart Dosya Planı
TDK	Türk Dil Kurumu
TNA	The National Archives
TS	Türk Standardı
TSE	Türk Standartları Enstitüsü
YÖK	Yüksek Öğretim Kurumu

TABLÖLER LİSTESİ

Tablo 1. Örnek bir EBYS üst veri alanı.....	61
Tablo 2. Canlı bir EBYS içinden alınan “Gizlilik Derecesi” alanı örneği	62
Tablo 3. Temel içeriğe sahip belge yönetimi politika başlıkları.....	76
Tablo 4. Ayrıntılı içeriğe sahip belge yönetimi politika başlıkları	77
Tablo 5. Katılımcıların eğitim bilgileri.....	117
Tablo 6. Katılımcıların yapmış oldukları görevleri	118
Tablo 7. Katılımcıların mezuniyetleri ile görevleri	118
Tablo 8. Katılımcıların kurum türleri	119
Tablo 9. Kurumlarda belgenin hibrit saklanması.....	119
Tablo 10. Kurumlarda fiziksel belgelerin dijitalleştirilmesi	120
Tablo 11. Kurumların fiziksel belgelerinin dijital ortamda bulunma oranları.....	121
Tablo 12. Kurumlardaki katılımcıların EBYS algıları.....	122
Tablo 13. Kurumlardaki katılımcıların EBYS kullanımları	122
Tablo 14. Kurumların EBYS değişim sebepleri	123
Tablo 15. Kurumların dijital ortamda belge üretme süreleri	124
Tablo 16. Kurumlarda bilgi varlığı envanteri	125
Tablo 17. Kurumlarda bilgi varlığı sorumlusu	125
Tablo 18. Kurumlarda e-arşiv sisteminin varlığı	126
Tablo 19. Kurumların dijital belge saklama sürelerinin belirlenmesi	127
Tablo 20. Dijital belgelere ait standart dosya planı	128
Tablo 21. Kurumların standart dosya planına uymaları	128
Tablo 22. Kurumlarda sistem içerisinde bir belgenin birden fazla nüshasının bulunma sorunu.....	129
Tablo 23. Belgenin sistemde fazla nüshasının olmasında yapılanlar	130
Tablo 24. Kurumlarda dijital belge oluştururken dikkate alınan unsurlar.....	131
Tablo 25. Kurumlarda sistemde saklanan belge format çeşitleri.....	131
Tablo 26. Kurumlarda kullanılan formatların belirlenmesi	132
Tablo 27. Kurumlarda dijital süreklilik terimi algısı	133
Tablo 28. Dijital süreklilik iyi yönetilemediğinde kurumların karşılaşılabileceği zorluklar	134
Tablo 29. Kurumlarda dijital belgelerin uzun vadede erişebilir olması için çalışma yapıp yapılmadığı	135
Tablo 30. Kurumlarda dijital belgelerin uzun vadede erişebilirliği çalışma ihtiyaçları	136
Tablo 31. Kurumlarda dijital belgelerin uzun vadeli korunması ile ilgili kaygıları	137
Tablo 32. Kurumlarda dijital belgelerin uzun vadeli korunmasından sorumlu birim ..	138
Tablo 33. Kurumlarda uzun vadeli koruma politikası	139
Tablo 34. Kurumların politika ihtiyaçları	140
Tablo 35. Kurumların personelin farkındalık ve yeterliliği	140
Tablo 36. Kurumlarda dijital belgelerin e-değerlendirme süreci.....	141
Tablo 37. Kurumlarda dijital belgelerin e-ayıklama süreci	141
Tablo 38. Kurumlarda dijital belgelerin hassasiyet değerlendirmesi süreci	142
Tablo 39. Kurumlarda dijital belgelerin hassasiyet değerlendirmesi süreci	143
Tablo 40. Kurumlarda hassasiyet değerlendirmesi için üst veri tanımlaması	143
Tablo 41. Kurumlarda belge yönetimi politikası	144

Tablo 42. Belge yönetim politikasında olması gereken unsurlar.....	145
Tablo 43. Kurumların belge yönetim politikasına ihtiyaçları.....	146
Tablo 44. Kurumlarda bilgi yönetim süreçlerine dair eğitim verilip verilmediği	146
Tablo 45. Kurumlarda bilgi yönetim süreçlerine dair eğitim ihtiyacı	147
Tablo 46. Kurumlarda verilen eğitimlerin yeterliliği.....	147
Tablo 47. Kurumsal politikanın kim/kimler tarafından oluşturulması gerektiği	148
Tablo 48. Kurumsal bilgi yönetim süreçlerinde kurumların zorlandığı/zorlanacağı alanlar.....	148
Tablo 49. Dijital belgelerin bilgi yönetim süreçlerinde sorumlu birim	149
Tablo 50. Dijital belgelerin arşive transferi için teknik altyapının yeterliliği	149
Tablo 51. Kurumların dijital belgeleri için Devlet Arşivlerine transfer yükümlülüğü.	150
Tablo 52. Kurumlarda Devlet Arşivlerine transfer edilecek materyal bilinci	150
Tablo 53. Dijital belgelerin arşive transferi için Devlet Arşivleri ile bağlantıya geçilip geçilmediği.....	151
Tablo 54. Dijital transfer ile ilgili bir çalışma olup olmadığı	151
Tablo 55. Kurumların dijital transferi gerçekleştirmeyi düşündükleri zaman aralığı... ..	152
Tablo 56. Kurumlarda dijital belgelerin transferinin denetlenmesi	152
Tablo 57. Devlet Arşivlerinin rolleri	153
Tablo 58. Anketin Cronbach-Alpha değeri.....	160
Tablo 59. Araştırma hipotezleri	161
Tablo 60. H1-H7- H8-H12 hipotezleri regresyon analizi testi sonuçları.....	162
Tablo 61. H2 ve H4 hipotezleri T testi analizi sonuçları	165
Tablo 62. H3 hipotezi anova testi sonuçları	167
Tablo 63. H3 hipotezi Tamhane's T2 testi sonuçları.....	168
Tablo 64. H5 hipotezi Anova testi sonuçları	169
Tablo 65. H5 hipotezi Tukey testi sonuçları.....	170
Tablo 66. H6 hipotezi Anova testi sonuçları	171
Tablo 67. H6 hipotezi Tukey testi sonuçları.....	172
Tablo 68. H9 hipotezi Anova testi sonuçları	174
Tablo 69. H9 hipotezi Tamhane's T2 testi sonuçları.....	174
Tablo 70. H11 hipotezi Anova testi sonuçları	175
Tablo 71. H13 hipotezi Anova testi sonuçları	176
Tablo 72. H14 hipotezi Anova testi sonuçları	177
Tablo 73. H10 hipotezi Mann-Whitney U testi analizi sonuçları	178

ŞEKİLLER LİSTESİ

Şekil 1. Bilginin hiyerarşisi piramidi (Tecim, 2020, s. 48)	34
Şekil 2. Bilgi yönetimi süreçleri için yaşam döngüsü modeli (Sağsan, 2006)	36
Şekil 3. Kurumsal bilgi yönetimi modeli (KBYM) (Arslankaya, 2017)	37
Şekil 4. Kurumlarda bilgi yönetim sistemleri (Külcü, 2018, s. 48).....	39
Şekil 5. Gizlilik dereceleri ve açıklamaları tablosu (Resmi Yazışmalarda..., (2020))....	60
Şekil 6. Belgelerin Gizlilik dereceleri.....	61
Şekil 7. Dijital süreklilik modeli (Managing Digital Continuity, 2017, s. 6)	67
Şekil 8. Varlık envanteri örneği.....	70
Şekil 9. DCC Dijital kütasyon yaşam döngüsü modeli (Higgins, 2008, s. 136; Öztemiz ve Özel, 2019, s. 1211).	82
Şekil 10. Açık arşiv bilgi sistemi referans modeli (Çakmak, 2016, s. 30; Reference Model For An Open Archival Information System (OAIS), 2012, s. 41).	83
Şekil 11. Dijital koruma modeli: Beş aşamalı ve üç ayaklı tabure (Digital Preservation Management Workshop 2003; Kenney ve McGovern, 2003).	84
Şekil 12. Doğuştan dijital belgelerin bilgi ve belge yönetim süreçleri kavram haritası	154
Şekil 13. Kavram haritası dijital belge bölümü	155
Şekil 14. Kavram haritası dijital süreklilik bölümü.....	156
Şekil 15. Kavram haritası dijital koruma bölümü.....	157
Şekil 16. Kavram haritası transfer süreçleri bölümü	158
Şekil 17. Kavram haritası milli arşiv bölümü.....	159

BİRİNCİ BÖLÜM

1. GİRİŞ

Tarihsel süreçte yaşanmış ve toplum yapısını tamamı ile etkilemiş ve şekillendirmiş devrimler bulunmaktadır. Bunlardan ilki; insanların ilk kez tarım yapması ile ortaya çıkan Tarım Devrimi'dir (Tarım devrimi, 2020). Diğer bir devrim ise Endüstri Devrimi olarak da anılan, Avrupa'da 18. ve 19. yüzyıllarda buhar makinesinin bulunması ile birlikte üretime etki sağlayan Sanayi Devrimi'dir (Sanayi devrimi, 2020). Bu devrimlerden sonuncusu ise Endüstri 4.0, 4. Endüstri Devrimi ya da 4. Sanayi Devrimi olarak adlandırılan devrimdir. Bu devrim temel olarak bilişim teknolojileri ile endüstriyi birleştirmeyi amaçlamış, böylelikle zaman içinde yaşanan gelişmelerle birlikte nesnelerin interneti, yazılım, donanım, bilgi iletişim teknolojileri, yapay zekâ gibi kavramlar da yaşamımızın içinde geniş bir yer tutmaya başlamıştır (Endüstri 4.0, 2020). Diğer bir önemli kavram ise sanayi ötesi toplum olarak adlandırılan Bilgi Toplumu'dur. Bilgi toplumu; bilginin yönetim süreçlerinde bilgi ve iletişim teknolojilerinin kullanılması ve bu teknolojilerin oldukça gelişmesine bağlı olarak hayatımızı şekillendirmesine sebebiyet veren bir kavramdır (Bilgi toplumu, 2020; Tonta, 1999, s. 364).

Bilgi çağı olarak da adlandırılan dijital çağ, teknolojiyi ön plana çıkaran ve teknolojiyi kullanan bir çağ olmasıyla hayatımızı etkilemiştir. Bu etki eğitim, kültür, yönetim olmak üzere birçok alanda etkisini göstermiştir. Bu alanlardan biri de kuşkusuz Bilgi ve Belge Yönetimi alanıdır. Dijital çağda meydana gelen değişimlerle birlikte belgelerin oluşturulma ve kullanım şekillerinde değişiklikler meydana gelmiştir. Bilgi ve belge, hayatımızın her alanında var olan unsurlardır. Kurum ve kuruluşlarda üretilen bilgi ve belgenin de zamanla doğası değişmiştir. Burada öne çıkan bir etken ise kuşkusuz dijital dönüşümdür. Dijital çağ ve etkileri dijital dönüşümü zorunlu kılmıştır. Dijital dönüşüm ile birlikte pek çok kavram (Sanayi 4.0, nesnelerin interneti, endüstriyel devrim, yapay zekâ, artırılmış gerçeklik, dijital medya) hayatımızda yer etmeye ve kullanım alanı oluşturmaya başlamıştır. Geleneksel yöntemlerle kâğıt ortamında üretilen bilgi ve belgeden, dijital ortamda üretilen/elektronik ortamda doğan bilgi ve belgeye (born-digital record) geçiş söz konusudur. Belgeler artık fiziksel ortamlar yerine dijital ortamda üretilmeye başlanmıştır. Bu tür belgeler "born-digital record" olarak adlandırılmaktadır. Dijital belgeler (born-digital record) veri setleri, veri tabanları, mailler, metin tabanlı

belgeler, sunumlar gibi dijital formatta oluşturulmuş belgelerdir (What are born-digital records?, 2020). Dijital belge sayısallaştırılmış belgeden farklıdır. Sayısallaştırılmış belge daha önce fiziksel ortamda üretilip sonrasında çeşitli yöntemlerle elektronik ortama aktarılırken dijital belge dijital ortamda oluşturulan verilerden meydana gelmektedir.

Dijital ortamda yaşanan gelişmelere paralel olarak “bilgiye erişim” daha da önemli bir unsur haline gelmiştir. Dijital alanda erişim ise giderek hem kolaylaşmakta hem de bilgiye erişimde yaşanan beklenmedik zorluklar, büyük hacimde bir bilgi miktarının erişimini yönetmek, bağlam sorunu (eriştiğin bilgiyi anlamamak), bilgi güvenliği ve gizliliği sorunu, bilgiyi yaratanların ve kullananların rol ve sorumluklarını belirlemek gibi karmaşık bir hal almaktadır. Dijital çağda erişime belge yönetimi açısından baktığımızda getirdiği birtakım riskleri ve avantajları bulunmaktadır. Birçok kaynaktan bilgiye kısa sürede zaman ve mekân kısıtlaması olmadan ulaşmak, görsel arama gibi yeni erişim olanakları avantajlardan bazılarıdır (McLeod, 2015, s. 224-226; Özdemir, 2017, s. 47).

Bilgiye erişim denildiğinde ise akla ilk gelen kurumlardan birisi arşivlerdir. Arşivlerin en temel görevlerinden biri kurumsal hafızayı sağlamak ve korumaktır. Arşivler sahip olduğu her türlü materyali (fiziksel ve dijital belgeler, görüntü, video ve ses dosyaları, medya verileri, web siteleri, veri tabanları, veri setleri, e-postalar vb.) gelecek kuşaklara sorunsuz bir şekilde aktaran kurumlardır. Arşivlerin elinde bulunan materyallerin türleri de değişen çağ ile birlikte çeşitlenmiştir. Bu çeşitliklerden birisi de “dijital ortamda üretilen belgeler”dir. Dünya genelinde pek çok ülke dijital materyallerini nasıl yöneteceğini, nasıl koruyacağına ve arşivleyeceğine yönelik çalışmalar, projeler gerçekleştirmektedir. Tüm bunların yanında bir de dijital belgelerin milli arşivlere devredilmesi söz konusudur. Türkiye’de henüz dijital belgelerin (born digital records) milli arşive transferi başlamamıştır fakat bu durum kaçınılmazdır.

Dijital belgelerin arşive transferi konusunda dünyanın önde gelen arşivlerinden biri olan İngiliz Milli Arşivi (The National Archives) dijital belgelerin transferi aşamasına geçmiştir. Fakat dijital belgelerin arşivlere transferi fiziksel belgelerinki kadar basit değildir. Öncelikle İngiltere’de konu ile ilgili kanun yapısı değişmiştir. İngiltere Bilgi Edinme Hakkı Kanun’una göre hükümet belgelerinin halka açılması ve serbestçe sunulması gerektiğini belirtmektedir (Freedom of Information Act, 2000). Bununla birlikte resmi bilgiler halka açık sunulduğunda istemeden de olsa ülkenin uluslararası ilişkilerine zarar verebilecek ve nitelikli kişisel veri gibi hassas bilgilerin halkın eline

geçmesi ihtimaller arasındadır. Bilgi Edinme Hakkı Kanunu'nun her ülkede bilgiyi paylaşma konusu ile ilgili birçok sınırı ise uluslararası ilişkiler konusundadır ve en yaygın olan sınır mahremiyet kapsamında nitelikli kişisel veri konusudur. Bu sebeple herkese erişimi olacak resmî belgelerin hassas içeriklerinin tanımlanması ve hassasiyet değerlendirmelerinin yapılması gerektiği kanısına varılmıştır (McDonald, 2019, s. 1).

Bilgi Edinme Hakkı Kanunu'nun yürürlüğe girmesinden önce hükümet kayıtları 30 yaşına gelene kadar genel olarak herkesin erişimine açık değildi fakat Bilgi Edinme Hakkı Kanun'u (2005) gereği belgenin tarihi ne olursa olsun yasa gereği belirlenen gizlilik şartlarının kapsamı dışındaysa herkesin erişimine açık olmalıdır (*Records Review*, 2014, s. 26). İngiltere'de 2009 yılında Bilgi Edinme Hakkı Kanunu gereği belgelerin arşive transferi süresi 30 yıldan 20 yıla düşürülmüştür. Belgelerin transferinde ilk aşama 2013'te başlamıştır. Bu değişim kamu kurumları ve çalışanları için büyük bir değişim olarak görülmüş, aşamalı olarak gerçekleştirilmesi ve yönetilmesi uygun bulunmuştur (20-year rule, 2020).

Konu kapsamında İngiliz Milli Arşivi Glasgow Üniversitesi ile birlikte ortak bir çalışma gerçekleştirmiştir. Çalışma, belgelerin teknoloji destekli hassasiyet değerlendirmesini içermektedir ve bir doktora tezi kapsamında tamamlanmıştır. Kurumlardaki dijital belgelerin hassasiyet değerlendirmesini içeren ilk tez çalışması olarak önemli bir çalışmadır (McDonald, 2019).

İngiltere'de dijital belgelerin transferinin 30 yıldan 20 yıla indirilme kuralına kamu kurumlarının ne kadar hazır olduğu hakkında yapılan bir çalışmaya göre sadece bir kurum dijital belgelerini İngiliz Milli Arşivi'ne aktarmıştır. Ayrıca çoğu kamu kurumu dijital belgeler için gerekli olan farklı zihinsel süreçler ve beceriler gerektiren arşivsel süreçlerin planlamasını hesaba katmadığını belirtmiştir (Özdemir, 2019, s. 224). İngiliz Milli Arşivi'nin konu ile ilgili öncü çalışmaları bulunmaktadır. Konu ile ilgili süreçlerde İngiliz Milli Arşivi'nin dahi zorluk yaşaması ve kurumlarının birçoğunun duruma hazır olmaması, Türkiye ve diğer ülkeler için de süreci (dijital belgelerin transferi) başladığı zaman bir hayli sıkıntılı olacağının göstergesidir.

İngiliz Milli Arşivi dijital belgelerin yönetilmesi, dijital belgelerin transferi aşamaları olan, ayıklama, değerlendirme, hassasiyet değerlendirmesi ve bu işlemlerle birlikte eş zamanlı ilerleyen dijital süreklilik, uzun vadeli koruma ve erişim süreçlerinin sağlıklı ilerlemesi için birbiriyle bağlantılı birçok çalışma yapmıştır. İngiliz Milli Arşivi

kendi dijital stratejisini oluşturmuş ve bu çalışmayı bir rapor olarak yayımlamıştır (*Digital Strategy*, 2017). Yayımlanan rapora göre dijital çağ ile birlikte bir takım dijital zorlukların oluştuğu belirtilmiştir. Belirtilen bu zorlukların başlıcaları; belgelerin fizikselden dijitalle taşınması, dijital korumanın zor olması, kullanıcı beklentilerinin değişmesi, değişimin ilerleyen süreçlerde de devam edecek olması ve dijital becerilere sahip personel ihtiyacı'dır (*Digital Strategy*, 2017, s. 3-4). Tüm bu zorluklara karşı İngiliz Milli Arşivi yeni bir arşiv modeli tasarlamış ve "yıkıcı dijital arşiv" (disruptive digital archive) olarak adlandırılan modele geçiş yapmışlardır. Bu model, geleneksel birinci nesil arşiv modelinden ziyade ikinci nesil arşiv olarak da nitelendirilen içgüdü ve tasarımla şekillenen bir dijital arşiv olma isteğine yönelik hazırlanmıştır (*Digital Strategy*, 2017, s. 2).

Genel olarak kimi ülkelerde özellikle ABD ve Avrupa'da dijital belgelerin arşivlere transferi konusunda bir farkındalık ve bu konunun zorlukları hakkında bir bilinç bulunmaktadır. Yapılan literatür taramasına göre bu konu ile ilgili çalışmalar ve projeler başlamış ve devam etmektedir. Türkiye'de ise yıllardır dijital belge üretimi olmasına rağmen bundan sonraki süreç ile ilgili eksik bir yol haritası olduğu bilinmektedir. Konu ile ilgili bir yol haritasının ya da bir başka deyişle resmi bir politikanın olmayışı, bu konudaki çalışmaları da kısıtlamaktadır. Bu konuda bir yol haritası gereksinimi oldukça elzemdir. Çoğu elektronik işlem bilgi yönetim sistemleri üzerinden yapılmakta ve süreçler sistemden ileri gidememektedir. Bir bilgi yönetimi sistem olarak EBYS'den sonraki süreçlere yönelik bir planlama yapılamamakta ve dijital transfer konusunda kurumların önünde yol gösteren resmi bir politikanın da olmayışı ise yapılacak olan çalışmaların önünü kapamaktadır. Aynı zamanda bu süreçler sadece dijital belgelerin arşive transferi için değil kurumsal, verimli ve etkin bir bilgi yönetim süreci için de gereklidir. Bilginin istendiğinde bulunabilmesi, hassas olup olmadığını bilmek, kullanılan dosya formatlarının sürdürülebilir olup olmadığını bilmek, bu ve benzeri tüm unsurlar etkin bir bilgi yönetim süreci ile ilgilidir. Tüm bu süreçler de risk yönetimi ile ilgilidir ve tüm süreçler birbiri ile bağlantılıdır. Bu süreçlerden birinin düzgün ilerlemeyişi diğer süreçlerin sekteye uğramasına sebebiyet verecektir. Bu bağlamda çalışma sadece dijital belgelerin arşive devri olarak düşünülmemeli, kavramlar ve süreçler daha geniş düşünülmesi ve önemsenmelidir.

Çalışma boyunca değinilecek olan bazı kavramları çalışmanın başında açıklamanın faydalı olacağı düşünülmektedir. Çalışmada kurum arşivlerinden milli arşive transfer süreçlerinden sık sık söz edilmiştir. Bahsi geçen milli arşiv Türkiye’de bulunan Devlet Arşivleri’dir. Birçok ülkede “milli arşiv” olarak adı geçen ve kabul görmüş terim ülkemizde Devlet Arşivleri olarak geçmektedir. Milli Arşiv (Devlet Arşivleri) tüm kurumlardan ve arşivsel süreçlerinden sorumludur. Kurum arşivi ise kurum ve kuruluşların arşiv malzemelerini sakladıkları korudukları ve ilgili süreçlerin takibini yaptıkları arşivlerdir.

1.1. Araştırmanın Amacı

Dijital çağın bir yansıması olarak gelişen bilgi teknolojileri bilgi yöneticilerini yakından ilgilendirmektedir. Çevrimiçi kaynaklara güvenen araştırmacılar fiziksel mekânlara kıyasla araştırmalarında çevrimiçi platformlara yönelmişlerdir. Dijital çağda kullanıcılar için çevrimiçi ortamlarda e-kitap, makale, sanat eseri, sergiler gibi birçok materyal bulunmakta ve bu işlemler yine bilgi yöneticilerinin süzgecinden geçmektedir (Cox, 2011, s. 214). Dijital çağda yaşanan bu ve benzeri değişimler belgelerin doğasını da değiştirmiş ve bunun gereği olarak belge yaşam döngüleri ve süreçlerinde de değişiklikler meydana gelmiştir. Kamu kurum ve kuruluşları da yaşanan bu değişikliklerden nasibini almıştır. Kurumsal bilgi yönetim süreçlerinde geleneksel yöntemlerden farklı olarak dijital çağa yönelik metotların izlenmesi gerekliliği her geçen gün kendini hissettirmeye başlamıştır. Bazı ülkelerde dijital belgelerin milli arşivlere devri başlamış olmakla birlikte Türkiye için bu uygulama henüz yürürlüğe girmemiştir. Türkiye’de bu konu ile ilgili çalışma sayısı çok azdır ve akademik çalışma bağlamında yapılmış bir tez bulunmamaktadır.

Bu doğrultuda çalışmamızın amaçları;

- Dijital çağ ile birlikte Türkiye’deki kamu kurumlarında dijital belgelerin kurumsal bilgi yönetim süreçlerinin nasıl işlediğini ortaya koymak,
- Türkiye’de dijital belgelerin kurumsal bilgi yönetim süreçlerinde farklı kurumlar arasında farklılıklar bulunup bulunmadığını belirlemek,
- Türkiye’de kamu kurum ve kuruluşlarının dijital belgelerin kurumsal bilgi yönetim süreçlerinde karşılaşılabileceği zorlukları belirlemek,

- Kurumlarda dijital belgelerin ayıklanması, değerlendirmesi, hassasiyet değerlendirmesi, dijital süreklilik ve uzun süreli koruma konularında izlenen yol ve yöntemleri ortaya çıkarmak,
- Türkiye’de doğuştan dijital belgelerin milli arşive devri konusunda kurumlara farkındalık sağlamak,
- Türkiye’deki dijital belgelerin kurumsal bilgi yönetim süreçleri ile ilgili bir desen (kavram haritası) geliştirmek olarak belirlenmiştir.

1.2. Araştırma Problemi ve Araştırma Soruları

Çalışmanın problemi; “Türkiye’de kamu kurumlarında doğuştan dijital belgelerin kurumsal bilgi yönetim süreçlerinin uygulama aşamalarında ulusal ve kurumsal boyutlarda farkındalık eksikliği, teknik ve hukuksal altyapı yetersizliği yaşanmaktadır”.

Araştırma probleminden hareketle aşağıdaki araştırma sorularına cevap aranmaktadır:

- Dijital belgelerin kurumsal bilgi yönetim süreçlerinde kamu kurum ve kuruluşlarının mevcut durumu nedir?
- Kurumlarda dijital belgelerin ayıklanması, değerlendirmesi, hassasiyet değerlendirmesi, dijital süreklilik ve uzun süreli koruma konularında ne gibi yol ve yöntemler izlenmektedir?
- Dijital belgelerin kurumsal bilgi yönetim süreçleri konusunda kurumların karşılaştıkları engeller nelerdir?
- Dijital belgelerin kurumsal bilgi yönetim süreçlerini yürütebilecek nitelikli ve yeterli personel durumu nedir?
- Dijital belgelerin Milli Arşive transferi sürecinde süreç nasıl yürütülmelidir?

1.3. Araştırmanın Hipotezleri

Türkiye’de kamu kurum ve kuruluşlarında dijital belgelerin kurumsal belge yönetim süreçleri, dijital belgelerin arşive transferi ile ilgili resmi çalışmalar henüz netleşmemiştir ve bu konuda yaşanacak olan sorunların yeterince tespit edilmediği ve bu sorunlara yönelik çözüm önerilerinin gerekliliği bilinmektedir.

Araştırmanın problem ve soruları doğrultusunda temel hipotez; Türkiye’de kamu kurumlarında doğuştan dijital belgelerin kurumdan arşive transfer aşamasına kadar

gerekli olan bilgi ve belge yönetimi süreçlerinin teknik ve hukuksal altyapısı yeterli/beklenen düzeyde değildir” şeklinde tanımlanmıştır.

Araştırmanın alt hipotezleri ise şu şekilde belirlenmiştir;

- Dijital belgelerin milli arşive transfer sürecine dair bilinç ile Devlet Arşivleri Başkanlığı etkinliği arasında anlamlı ve pozitif yönlü bir ilişki bulunmaktadır.
- Dijital belgelerin bir bilgi varlığı olarak görülmesi ile kurumsal politika oluşturma arasında anlamlı ve pozitif yönlü bir ilişki vardır.
- e-değerlendirme, e-ayıklamayı doğrudan ve pozitif olarak etkilemektedir.
- Belge yönetim politikasına sahip olmak, dijital belgelerin oluşturulmasında "gizliliği" olumlu ve pozitif yönde etkilemektedir.
- Dijital belgelerin saklama sürelerinin belirlenmesi, standart dosya planına uyumu olumlu ve pozitif yönde etkilemektedir.
- Kurumsal bilgi yönetim süreçlerinin zorluğu, eğitime ihtiyaç duyulan alanları artırmaktadır.
- Dijital belge yönetimine dair eğitimler, EBYS yeterliliğini artırmaktadır.
- Devlet arşivlerinin kurumlara desteği, kurumların dijital belgeleri arşive devretme yükümlülüğün farkında olmasını anlamlı ve olumlu yönde etkilemektedir.
- Dijital süreklilik farkındalığı dijital belgelerin uzun vadede erişilebilir olması çalışmalarını artırmaktadır.
- Kurumlarda e-arşiv sistemi bulunması ve hassasiyet değerlendirmesinin etkinliği arasında anlamlı ve pozitif yönlü bir ilişki bulunmaktadır.
- Kurum türüne göre dijital süreklilik farkındalığı anlamlı ve pozitif yönde ayrılmaktadır.
- Kurumların EBYS'yi değiştirmeleri, uzun vadeli korumadaki kaygıyı artırmaktadır.
- Dijital belgelerin saklandığı formatın çeşitliliği, uzun vadede erişim çalışmalarını artırmaktadır.
- Dijital süreklilik farkındalığı, dijital sürekliliğin iyi yönetilmesini olumlu ve pozitif yönde etkilemektedir.

1.4. Araştırmanın Kapsamı ve Sınırlılıkları

Araştırmanın kapsamını Türkiye’de dijital belgelerin bilgi yönetim süreçlerine dair veri sağlayabilecek kamu kurum ve kuruluşları ile Devlet Arşivleri Başkanlığı

tarafından yayımlanan 2020-2024 stratejik planında yer alan dış paydaşlar olarak iş birliği yapılan kurumlar oluşturmaktadır. Bu bağlamda 2021 yılında var olan Türkiye’deki bakanlıklar (17), e-belediye bilgi sistemine sahip olan büyükşehir belediyeleri (20) ve il belediyeleri (37), üniversiteler (131) ve diğer ilgili kamu kurum ve kuruluşları (25) araştırmanın kapsamını oluşturmaktadır. Çalışma evrenini 230 kurum oluşturmakta, 0,99 güven düzeyi, 0,5 hoşgörü miktarına göre 230 kurumdan oluşan bir evren 118 kurum ile örneklenebilmektedir (Raosoft, 2004). Çıngı’ya göre ise; 0,99 güven düzeyi, 0,5 hoşgörü miktarına göre 500 kurumdan oluşan bir evren 101 kurum ile örneklenebilmektedir (1990, s. 261). Bu bağlamda, araştırma kapsamında 120 kurumda anket çalışması gerçekleştirilmiştir. Örneklem evreni temsil eder niteliktedir. Bu çerçevede veriler 2021 yılı Temmuz–Aralık ayları arasında kurumlardan yüz yüze, çevrimiçi görüşme, telefon gibi araçlarla elde edilmiştir. Araştırma verilerinin toplanması sürecinde bazı kurumlardan yeterli yanıt alınamaması veya olumsuz geri dönüş alınması zorluklarıyla karşılaşmış ve bu kapsamda Bilgi Edinme Hakkı Kanunu esas alınarak e-devlet üzerinden kurumlara başvuruda bulunulmuştur.

Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi’ne göre belge transfer etmekle yükümlü kurumlar kamu kurumlarıdır. Bu nedenle araştırma, kamu kurumları ile sınırlandırılmıştır. Bununla birlikte araştırma kapsamında var olan belediyeler içerisinde e-belediye bilgi sistemini kullanan büyükşehir ve il belediyeleri araştırmaya dâhil edilmiş, ilçe ve belde belediyeleri bir anlamda büyükşehir ve il belediyelerini temsil edeceğinden ötürü araştırma dışında tutulmuştur. E-belediye bilgi sistemini kullanan belediye bilgilerine İçişleri Bakanlığı e-belediye resmî web sayfasından¹ erişilmiştir. Ek olarak araştırma sürecinin pandemi (Covid19) dönemine denk gelmesi sebebi ile daha önce belirlenen hedef kurumlarla birebir görüşme isteklerimizin olumlu karşılanamaması üzerine araştırma için daha ayrıntılı bilgi almak amacıyla görüşme soruları geliştirilerek ankete eklenmiş ve kapsamlı bir anket oluşturulmuştur. Her kurumdan temsilen araştırma konumuzla ilgili bir personel ankete katılmıştır.

1.5. Özgün Değer

Literatürde ilk defa Türkiye’deki dijital belgelerin kurumsal bilgi yönetim süreçlerini konu alan akademik çalışma bağlamında bir tez yazılmıştır. Türkiye’de henüz dijital belgelerin milli arşive transferi başlamamıştır fakat bu konunun kaçınılmaz olduğu

¹E-belediye bilgi sistemini kullanan belediye bilgilerine <https://www.belediye.gov.tr/> adresinden erişim sağlanmıştır.

bir gerçektir. Dijital belgelerin arşive transferi başlama kararı alındığında bu konuda çalışacak olan personelin konu ile ilgili bilgi ve deneyim eksikliği, işin sorunlu bir şekilde ilerlemesine sebep olması ihtimal dâhilindedir. Aynı zamanda konu ile ilgili yasal dayanakların eksikliği, benzer bir çalışmanın henüz uygulamaya konulmaması birtakım sorunları ve yanlış uygulamaları beraberinde getirerek milli hafızayı da zedelemesi olası sonuçların başında gelmektedir. Yine yapılacak olan işlemlerin fiziksel belgelerdeki işlemlerle aynı olmayacak olması ve farklı teknik ve yöntemlerin izlenecek olmasından dolayı bu konunun önemli ve bir o kadar da basit olmadığını kabul etmek gerekir. Türkiye’de dijital belgelerin kurumsal bilgi yönetim süreçlerinin yönetimi ve bu konuda teorik ve teknik anlamda bir uygulama yapılmadığı ortadadır. Bu tez literatürde uygulamaya dayalı yapılmış bir çalışma olduğundan önemlidir. Türkiye’de dijital belgelerin kurumsal bilgi yönetim süreçleri aşamalarına hazırlık bölümünde ilgili tez, referans kaynağı olarak kullanılabilir. Bununla birlikte tezin yapılacak uygulamalara öncülük etmesi beklenmektedir. Tezin Türkiye’deki kamu kurumlarında dijital belgelerin kurumsal bilgi yönetimi süreçleri konusunda bir farkındalık oluşturacağı umulmaktadır. Aynı zamanda bu çalışma ile Türkiye’de dijital belgelerin arşive transferi başlayacağı zaman yaşanacak olan zorlukları da ortadan kaldırması ve ihtiyaç duyan kişi ve kurumlara yol göstermesi umulmaktadır. Bu çalışma alanımızdaki önemli açığı bir nebze olsun kapatacağı ve ileride benzeri çalışmalara destek olacağı inancındayız.

1.6. Araştırma Yöntemi, Veri Toplama ve Değerlendirme Teknikleri

Araştırma kapsamında hipotezi sınavabilmek ve araştırma sorularına yanıt bulabilmek için kurumlardan veri elde edebilmek amacıyla olasılığa dayalı tabakalı örneklem yöntemine göre basit rastgele örnekleme yöntemi kullanılmıştır. Konu kapsamında araştırmaya nitelikli veri sağlayabilecek kütüphaneci, arşivci, EBYS sorumlusu, belge yöneticisi vb. ilgili alanda çalışan personel (bilgi profesyoneli) ile anket çalışması gerçekleştirilmiştir (Neuman, 2013, s. 337).

Araştırmada sosyal bilimlerde gerekli verilerin sistematik olarak toplanmasında yaygın olarak kullanılan uygulama tekniklerinden birisi olan anket tekniğine başvurulmuştur (Al, 2007, s. 84). Anket, nicel ve nitel verilerin elde edilmesine yarayan uygun bir araç olarak bilinmektedir (Walliman, 2011, s. 97). Araştırmada ayrıca betimleme yöntemi de kullanılmıştır. Kaptan’a göre betimleme yöntemi “olayların, grupların, kurumların vb. çeşitli alanların ne olduğu ve bu sırada gerçekleşen eylemleri daha iyi anlayabilme, aktarabilme adına aralarındaki ilişkinin açıklandığı bir unsur”dur

(Kaptan, 1998, s. 59). Araştırmada ayrıca kurumlardaki konu uzmanları ile yapılandırılmış görüşme tekniği uygulanmıştır. Yapılandırılmış görüşme tekniği; araştırmacının belirli bir düzenle önceden hazırlanmış soruları uzman kişilerle karşılıklı görüşmesidir (Büyüköztürk ve diğerleri, 2012, s. 151). Bu yöntemlere ek olarak araştırmanın yapısına bağlı “araştırmada yer alan anahtar kelimelerin basılı ve elektronik kaynaklar ve referans kaynaklarında taranarak konu ile ilgili yayınlara ulaşılması” olarak tanımlanan derinlemesine literatür taraması gerçekleştirilerek araştırmanın çerçevesi çizilmiştir (Arlı ve Nazik, 2003, s. 20; Eroğlu, 2017, s. 10; İslamoğlu, 2003, s. 67).

Bu araştırma Marmara Üniversitesi Sosyal Bilimler Araştırma Etik Kurulu’nun 08 Haziran 2020 tarihli toplantısında etik açıdan uygun bulunmuş ve 2020/09 sayılı yazıda gerekli etik kurul izni verildiği belirtilmiştir.

Araştırma sürecinde, Devlet Arşivleri Başkanlığı Bilgi İşlem ve Elektronik Arşiv Dairesi Başkanı Alparslan BAŞAR ve Cumhurbaşkanlığı Bilgi ve Belge Yönetimi Daire Başkanı Serkan Menteş ile görüşmeler gerçekleştirilmiştir. Yapılan görüşmeler anketin hazırlanmasına da katkı sağlamıştır. Aynı zamanda anket yapılacak kurumların belirlenmesinde görüşmelerin faydası olmuştur.

Çalışmada literatürün analiz edilmesiyle ortaya çıkan açık uçlu, çoktan seçmeli, şıklı ve likert ölçekli soruları kapsayan bir değerlendirme aracı geliştirilmiştir. Aynı zamanda değerlendirme aracı oluşturma sürecinde Özdemir’in makalesindeki (The inevitability of digital transfer: How prepared are UK public bodies for the transfer of born-digital records to the archives?) anket sorularından da yararlanılmıştır. Değerlendirme aracı 52 sorudan oluşturulmuş, kapsamlı bir ankettir. EK 1’de sunulan değerlendirme aracındaki soruların dağılımı aşağıdaki gibidir:

- Genel bilgiler: Şıklı iki soru, açık uçlu iki soru.
- Dijital belge ve EBYS: Şıklı yedi soru.
- Dijital belgeler için bilgi varlığı, saklama planı, dosya formatları ve dijital süreklilik bilgileri: Şıklı dokuz soru, beşli likert ölçekli altı soru, birden çok seçenek işaretlenebilir bir soru.
- Uzun vadede erişilebilirlik, koruma, üst veri ve tanımlama süreçleri: Şıklı üç soru, beşli likert ölçekli üç soru.
- Dijital belgelerin e-değerlendirme, e-ayıklama, hassasiyet değerlendirmesi süreçleri: Şıklı beş soru.

- Politika, eğitim ve milli arşive transfer süreci: Şıklı dokuz soru, beşli likert ölçekli altı soru, birden çok seçenek işaretlenebilir bir soru, açık uçlu bir soru.

Anketin ön testi yapılmış. Alanda uzman akademisyenlerden anketle ilgili geri dönüşler alınmış ve anket geliştirilmiştir. Araştırmanın ön testi Tapu Kadastro Genel Müdürlüğü, Marmara Üniversitesi Yazı İşleri Birimi ve EBYS birimlerine uygulanmıştır. Anket soruları yapılan ön test değerlendirmeleri sonucunda güncellenmiştir.

Araştırmada soruların değerlendirilmesi için SPSS 21 programından yararlanılmıştır. Bu programda toplam 135 değişkenle birlikte çalışılmıştır. Elde edilen bulguların sunumunda ve verilerin analizinde, tanımlayıcı istatistikler olan sıklık değerleri, oranlar, aritmetik ortalama, standart sapma değerleri kullanılmıştır. Aynı zamanda güvenilirlik ve geçerlik testleri, Mann Whitney testi, ANOVA testi, Bağımsız Örneklem t-Testi, Korelasyon testi, Basit Doğrusal Regresyon testi ve Post-Hoc testi, Tamhane's T2 testi uygulanmıştır.

1.7. Araştırma Düzeni

Araştırma sürecinde yapılan tüm sentezleme, raporlama, değerlendirme ve analizler toplam sekiz bölüm halinde sunulmuştur. Aşağıdaki bölümlere ait ayrıntılı bilgiler verilmektedir.

Birinci bölümde konunun önemi, araştırmanın amacı, problemi, soruları, hipotezleri, kapsamı, sınırlılıkları ve özgün değeri sunulmaktadır. Bunlara ek olarak araştırma yöntemi, veri toplama ve değerlendirme teknikleri, düzeni ve araştırma sürecinde hangi kaynaklardan yararlanıldığı bilgilerine yer verilmiştir.

İkinci bölüm literatür değerlendirmesinin sunulduğu bölümdür. Doğuştan dijital belgelerin milli arşive transferi ile ilgili yapılan uluslararası çalışmalar ve konu ile ilgili Türkiye'deki durumdan bahsedilmektedir.

Kuramsal bilgi yönetim süreçlerini ele alan üçüncü bölümde, bilgi, kuramsal bilgi, bilgi yönetimi ve kuramsal bilgi yönetimi süreci değerlendirilmiştir. Bunlara ek olarak kuramsal bilgi yönetim modelleri ve Türkiye'de kuramsal bilgi yönetiminin mevcut durumu bu bölümde yer almaktadır.

Dördüncü bölüm doğuştan dijital belge ve bilgi yönetim süreçlerinin ayrıntılı olarak işlendiği bölümdür. Doğuştan dijital belgelerin milli arşive transfer aşamaları olan dijital değerlendirme, dijital ayıklama, hassasiyet değerlendirmesi aşamaları ve bu

aşamalarının uygulamada nasıl yapıldığı ile ilgili bilgiler bu bölümde sunulmuştur. Dijital belgelerin milli arşive transfer aşamaları ile yakından ilgili olan dijital süreklilik, dijital koruma, belge yönetiminde politika konuları da ayrıntılı olarak bu bölümde sunulmuştur.

Beşinci bölümde dijital belgelerin arşive transfer süreci ile ilgili yaklaşımlar, ulusal ve uluslararası çalışmalar sunulmuştur. İngiltere, Avustralya, ABD, Fransa, Yeni Zelanda, Hollanda, Macaristan, İsviçre, Estonya, İrlanda, İskoçya, Danimarka, Türkiye ülkelerine ait incelemeler bu bölümde yer almaktadır.

Altıncı bölümde konu ile ilgili kurumlara yapılan ankete ait bulgular ve analiz sonuçları sunulmuştur. Aynı zamanda bu bölümde çalışmanın tüm süreç ve bulgularından yararlanılarak oluşturulan doğuştan dijital belgelerin bilgi yönetim süreçlerine dair bir desen (kavram haritası) sunulmuştur.

Yedinci ve son bölümde ise çalışmaya ait sonuç ve öneriler yer almaktadır.

1.8. Kaynaklar

Araştırma sürecinde basılı ve elektronik çok sayıda kaynak çalışmaya dayanak olmuştur. Teorik kısımda uluslararası ülkelerin ve arşivlerinin web sayfalarından ulaşılan yasal dayanaklar (politika, strateji, yönetmelik, yasa vb.) çalışmanın sağlam bir zemine oturtulmasında önemli rol oynamıştır. Konu ile ilgili daha çok uluslararası kaynaklar, kitaplar, makaleler ve yasal dayanaklardan yararlanılmıştır. Bu durumun temel sebebi henüz ilgili konu hakkında ülkemizde çok fazla kaynağa rastlanamamasındandır. Çalışmada aşağıdaki elektronik kaynaklardan yararlanılmıştır.

- | | |
|--|--|
| -Arşiv Dünyası | -Bilgi Dünyası |
| -Directory of Open Access Journals (DOAJ) | |
| -Dissertation Abstracts | -Ebrary |
| -EBSCOHost - Library, Information Science & Technology Abstracts (LISTA) | |
| -EMERALD | -E-prints in Library and Information Science |
| -ERIC | -IEEE Xplore |
| -JSTOR | -Proquest (1986-) |
| -UMI ProQuest Digital Dissertations | |
| -SAGE | -ScienceDirect |
| -Scopus | -Springer Link |
| -Taylor & Francis | -Türk Kütüphaneciler Derneği Bülteni |
| -Türk Kütüphaneciliği | -Türkiye Makaleler Bibliyografyası |
| -Web of Science | -Wiley Interscience |

-YÖK Tez Kataloğu

Çalışmada arama motorlarında yaygın olarak kullanılan anahtar kelimeler aşağıda verilmiştir.

- | | |
|---------------------------|------------------------------|
| -Born-digital record | - Doğuştan dijital belge |
| -Digital transfer | - Dijital transfer |
| -Digital appraisal | - Dijital değerlendirme |
| -Digital selection | - Dijital seçim/ayıklama |
| -Sensitivity review | - Hassasiyet değerlendirmesi |
| -Digital preservation | - Dijital koruma |
| -Digital continuity | - Dijital süreklilik |
| -Record management policy | - Belge yönetimi politikası |

Tezin yazımında Marmara Üniversitesi Türkiyat Araştırmaları Enstitüsünün “Tez Yazım Kılavuzu” kullanılmıştır.² Ek olarak tezin yazımında EndNote X9 referans yönetimi yazılımından yararlanılmıştır.

² Marmara Üniversitesi Türkiyat Araştırmaları Enstitüsü Tez Yazım Kılavuzu’na <https://turkiyat.marmara.edu.tr/dosya/tae/ogrenci/2022%20Tez%20Yaz%C4%B1m%20K%C4%B1lavuzu.pdf> adresinden erişilmiştir.

İKİNCİ BÖLÜM

2. LİTERATÜR DEĞERLENDİRMESİ

Bu bölümde çalışma kapsamına giren doğuştan dijital (born-digital) belgelerin bilgi yönetim süreçlerine dahil olan unsurlar; dijital belgelerin değerlendirilmesi, ayıklanması, hassasiyet değerlendirilmesi, dijital süreklilik, dijital koruma unsurları değerlendirilmiş, ilgili ulusal ve uluslararası literatür incelenmiştir. Bu süreç içinde dijital belgelerin değerlendirilmesi, ayıklanması, hassasiyeti, korunması, arşive transferi gibi birçok unsur birbirileri ile bağlantılı bir biçimde ilerlemektedir. Hiçbir unsuru yönetsel süreçte birbirinden ayıramamakla birlikte yapılan çalışmalarda tüm süreçlerden farklı farklı örneklerle literatürdeki çalışmalara değinilmiştir.

Günümüzde teknolojinin getirdiği imkânlarla birlikte bilgi ve belgeye erişim değişmektedir. Bu değişim kütüphanecileri, arşivcileri, bilgi ve belge uzmanlarını kendilerini geliştirmeyi ve değişen düzene uyum sağlamayı zorunlu kılmaktadır. Dijital belgelerin farklı alanlarda kullanımı ve dijital belgelerdeki değişikliklerle ilgili sıra dışı örneklerle vurgu yapan Moss ve Thomas, çalışmalarında hukuk ve sanat alanlarındaki belgelerle ilgili örneklerde bulunmuşlardır. Çalışmaya göre son dönemlerde İngiltere’de hukuk davalarında hâkimler “sayfanın dört bir yanı” terimi kullanımı ile belgeye bakış açılarını genişletme eğilimindedirler. Yine ressamın çizimlerinde resme aynı bakış açısı ile bakıp resmin boyutlarından farklı bir dış dünya fikrini tartışmaktadırlar. Tüm bunlar bizlere belgelerin yapısal olarak dönüşüm geçirdiğini ve çok boyutlu bir hale geldiği göstererek dijital belge dünyalarının farklı yönlerini işaret etmektedir (Moss ve Thomas, 2020). McLeod, dijital alanda erişimin giderek kolaylaştığını fakat aynı zamanda da karmaşık bir hal aldığını dile getirmiştir. Bu sebeple oluşan karmaşıklık belge yönetim süreçlerinde de zorluklar meydana getirmiştir (McLeod, 2015, s. 4). Açık devlet, açık veri ve büyük veri ikliminde, bilgiye erişimin tek ve ana amacının şeffaflık ve hesap verebilirlik olduğu vurgulanmıştır (McLeod, 2015, s. 1). Bir başka görüşe göre ise; dijitalleşme, arşivler için bir tehdit değil bir fırsattır. Eğer dijitalin özünü kavrayabilirsek arşivlerde yalnızca okunabilen belgeler değil, aynı zamanda tanımlanabilen, keşfedilebilen ve kullanılabilen veriler ortaya çıkması sağlanacaktır. Bu durum ise bizlere yeni olasılıkların da kapılarını açacaktır (Ranade, 2018, s. 79).

Değişimler sürekli olduğundan farklı stratejileri bir arada uygulamak zorunlu hale gelmektedir. McLeod bu konuya yenilikçi bir bakış açısı sağlamıştır. İlk olarak bilgi hacminin giderek büyüyen ve önüne geçilemeyen bir bilgi yığını, bir buz dağı olduğunu

ileri sürmüştür. Oluşturulan bilgiler iki yılda bir iki katına çıkmakta ve beş yılda 44 zettabayta ulaşılacağı öngörülmektedir. Dijital çağda üretilen bilgilerin bir kısmı gerekli, bir kısmı ise kurumsal/uzun vadeli önem taşımadığı için hepsinin kayıt altına alınması mümkün gözükmemektedir. McLeod çözüm olarak bir “Belge Yönetim Aracı” olduğundan bahsetmiştir. Belgeler açısından bakıldığında esas olanın neyin önemli olduğunu değerlendirmek, imha sürecine karar vermek, gerekirse saklamak, korumak ve bu işlemleri yasal çerçeve içerisinde yapmaktır. Bahsedilen tüm aşamalar aslında değerlendirme ile ilgilidir. Dijital dünyada değerlendirme ise risk yönetimini gerektirmektedir. Dijital dünyada bilgi ve belgeye erişim daha kolaydır fakat beklenmedik zorluklara da yol açtığını söylemek mümkündür. Örneğin hassas bilgiler içeren belgelerin kullanıcıya açılması olumsuz sonuçlar arasında yer almaktadır. Bu sonuçların olmaması için belgelerin nasıl düzenleneceğine karar verilmeli, bir belge erişimine izin verildiyse bunun sonucu düşünülmeli, erişim izni verildikten sonra bilginin kullanımına ilişkin kontroller yapılmalıdır. Erişilen bilgileri anlamak için yeterli bağlamı sağlamak dijital ortamda oldukça zordur. Erişim açısından bakıldığında bilginin nerede olduğunu bilmek, bilginin hangi koşullarda oluşturulduğunu ve diğerleri ile ilişkisini bilmek, bilginin tam olarak anlaşılması ve yetkilendirilmesi için yaşamsal önem taşımaktadır (McLeod, 2015, s. 5-7). Erişim, dijital belgelerin arşive transferi sonrasında karşımıza çıkacak unsurlardan birisidir. Transfer edilecek belgelere erişim dijital çağda elzemdir. Erişim aynı zamanda dijital süreklilik ile de bağlantılı olarak ilerlemektedir. Tüm unsurlar birbirleri ile bağlantılıdır. Özdemir, erişimin eskiye oranla dijital çağda daha kolay olduğunu fakat bazen bilgi güvenliği riski oluşturup mahremiyet olgusuna da zarar verdiğine değinmiştir (Özdemir, 2017, s. 49).

Dijital çağda belgelerin doğası değişmiştir. Bu nedenle arşivlerde dijital belgelerin bilgi yönetim süreçlerinde arşivcilerin şimdiye kadar aşına olmadığı farklı yetenekler ve konulara ihtiyaç duyulmaktadır. Bu durum ise arşivlerin zorunlu olarak büyük değişiklikler yapmasını öngörmektedir (*Digital Strategy*, 2017, s. 2). Dünyanın her yerinde arşivler dijital ortamdaki zorluklarla boğuşmaktadır. Bunun elbette birkaç nedeni bulunmaktadır. Bunlar;

- Belgelerin fizikselden dijital ortama taşınması,
- Dijital korumanın zor olması,
- Kullanıcı beklentilerinin değişmesi,
- Belgelerin doğasının değişmesi ve değişimin sürekli devam edecek olması,

- Dijital belgelerin güvenilirliğinin fiziksel belgelerden farklı olması,
- Dijital yeteneklerin ön planda olması (*Digital Strategy*, 2017, s. 3-5).

Teknolojik gelişmelerin dijital belge yönetimi üzerine etkileri sebebiyle dünyanın birçok yerinde “dijital” algısı yer edinmiş ve hayatımıza girmiş bulunmaktadır. Bu doğrultuda bilgi ve belge yönetimi alanında mevcut sorunları çözmek ve çağa ayak uydurmak adına dijital dönüşüm çalışmaları, çeşitli dijital arşiv çalışmaları, projeler yapılmaya başlanmıştır. Çoğu ülkede bu hedefler Milli Arşivler öncülüğünde gerçekleştirilmektedir. Henüz her ülkede tam anlamıyla dijital belgelerin bilgi yönetim süreçleri, arşive transfer uygulamaları başlamasa da doğuştan dijital belgelerin bilgi yönetim süreçleri ile ilgili çalışmalar yapan ülkeler bulunmaktadır. Uluslararası literatür incelendiğinde genel olarak yurtdışında dijital belgelerin arşive transferi ve konunun zorlukları hakkında bir bilinç bulunmaktadır.

Dijital arşivleme ile ilgili tek bir çözüm yolu ya da örnek yoktur. Kurumlar kendi çözümlerini kendi oluşturdıkları politika ve yönetim süreçleri içerisinde bulma yoluna gitmektedir. Dünyanın pek çok ülkesinde dijital belgelerin transfer süreci ile ilgili adımlarla ilgili çalışmalar öncelikle Milli Arşivler öncülüğünde ve devlet yönetiminde ilerlemektedir. Konu ile ilgili öncelikle arşiv kanunu, dijital strateji, belge yönetimi politikası gibi yasal mevzuatlara sahip olunmalıdır. Dünyada dijital transfer sürecini başlatan ülkeler bulunmakla birlikte bazı ülkeler dijital transfer sürecine henüz geçmemiş, bazıları ise hazırlık sürecinde bulunmaktadır.

Öncelikle dijital transfer için gerekli olan adımların tanımlarını vermek yerinde olacaktır. Fakat şunu rahatlıkla söyleyebiliriz ki, dijitalin hayat bulması ile birlikte kavramlar da artık sabit kalmamaktadır. Bazı yazarlar yeni dünyayı anlamak için eski kavramları yetersiz bulmaktadır. Yeni düzenle başa çıkmak için tamamen yeni kavramlara ve yaklaşımlara ihtiyaç duyulduğunu beyan etmektedirler (Eastwood, 2007, s. 1).

Dijital transferin ilk adımlarından birisi dijital değerlendirmedir. Arşivler açısından değerlendirme genellikle şu şekilde kabul edilir: “belgelerin korunmaları, ayıklanmaları ya da yok edilmelerini belirleme işlevi” ve aynı zamanda “arşiv malzemesinin korunmasının devam eden değerine ilişkin bir tahmin veya yargıya varma durumu” dur (Eastwood, 2007, s. 2). Eski tanımlamalar ve kavramlar artık günümüzde yeterli değildir. Teknolojik değişikliklerle birlikte eski değerlendirme yöntemlerinin ve

kavramlarının kalıpların içinde kaldığı ve dijital değerlendirmenin kaçınılmaz olduğu bir gerçektir. Dijital değerlendirme; dijital materyalin arşivsel değerini belirleme süreci yani bir bağlamda arşive transfer edilip edilmemesi gerektiğinin belirlenme süreci olarak ifade edilebilir. Dijital değerlendirme açısından yeni bilgi teknolojileri bir zorluk olarak tanımlanabilir ancak dijital belgelerin değerlendirilmesi daha fazla deneyime, araştırmaya ve başarıya ihtiyaç duyulan bir alan olmaya devam edecektir. Bilinen tüm dijital formlar için arşivcilerin dijital değerlendirme yöntemlerini bilmeleri gerekecektir (Cox, 2011, s. 227).

Birçok araştırmacı değerlendirmenin zamanlaması sorununu tartışmıştır. Neredeyse hepsinin vardığı sonuç; “değerlendirme, belgeleri üreten sistemlerin ömrünün başlarında yapılmalıdır” şeklinde olmuştur (*Appraisal task force report*, [t.y.], s. 3). Dijital belgelerin arşive transferi düşünüldüğünde bir değerlendirme sürecinden geçmesi elzemdir. Dijital belgelerin değerlendirilmesi belge oluşturulduğu andan itibaren yaşam döngüsü içinde yapılmalı ve arşive transfer süreci beklenmemeli ve bu bağlamda kurum ve belge yöneticileri tarafından dijital belge transfere hazır hale getirilmelidir. Dijital belgelerin değerlendirme süreci fiziksel belgelerden farklıdır ve belgelerin yapısı gereği farklı olmak zorundadır.

Dijital bilgi ve belge kavramlarının kurumlarda yer bulması ile de birtakım değişimler yaşanmıştır. Örneğin İngiltere’de belgelerin değerlendirme süreci 1954’ten bu yana Grigg raporu baz alınarak yapılmaktaydı. Bu rapora göre değerlendirme sisteminde 5 yıl (devam eden iş değeri ve potansiyel arşivleme için değeri) ve 25 yıl (arşiv değeri) sistemi geçerli kılınmış ve toplamda seçilen belgelerin milli arşive aktarılma süresi 30 yılı bulmaktaydı. Bu sisteme göre değerlendirme günümüz koşullarında birtakım unsurlardan dolayı artık mümkün gözükmemektedir (*Best practice guide to appraising and selecting records for The National Archives*, 2013, s. 3). Bu unsurlar;

- Dijital bilgi savunmasızdır. Dosya biçimi eskimesi veya silinmesi gibi sebeplerden bilgiye erişilememesi ve bu sebeple kurumların bilginin değeri ile ilgili kararları bilgi yaşam döngüsü sürecinden erken dönemde alması gerekir.
- Dijital bilgide meydana gelen artan hacim ve çoğalma karışıklığa sebep olur ve tek tek dosyaları değerlendirmeyi mümkün kılmaz.
- Fiziksel belgeleri değerlendirmek zaman alır ve bu durum kurumların ilgili belgeleri etkili bir biçimde kullanmasına engel olur.

- 2013 yılında 30 yıl transfer kuralının 20 yıla indirilmesi ile belgeleri değerlendirirken kısa sürede daha fazla belgenin incelenmesi gerekecektir.
- Kısa sürede büyük hacimde belgenin değerlendirilmesi gerekmektedir (*Best practice guide to appraising and selecting records for The National Archives*, 2013, s. 3).

Dijital değerlendirme ile ilgili bir çalışmada; dijital nesnelerin yaşam döngüsü sürecinde otomatikleşme olgusu ile birlikte değerlendirmesinin nasıl yapılabileceği ve gereksinimlerin neler olduğu amaçlanmıştır. Çalışmanın sonucunda, otomatik değerlendirme sistemlerinin ve ilgili araçların geliştirilmesinin çok yoğun emek gerektiren bir süreç olduğu, tasarımı, geliştirilmesi, uygulaması, karışık olması ve maliyetli olmasına rağmen bunun için çaba sarf etmenin yine de olumlu olacağı kanısına varılmıştır. Bununla birlikte otomatik bir değerlendirme sistemi yalnızca bazı bağlamlarda sınırlı faydalar sağlamaktadır. Önerilen yaklaşım, üst veri gereksinimleri ve güvenilirlik gibi faktörlerden kaynaklanan sınırlamalara sahiptir (Harvey ve Thompson, 2010). Üst veri bahsi geçen veri hakkında ayrıntılı bilgi vermeyi ifade eder.

İngiltere'nin başkenti Londra'da bulunan Wellcome Kütüphanesi'nin³ belgelerin değerlendirmesi ile ilgili bir deneyimi bulunmaktadır. Bu deneyime göre doğuştan dijital belgelerin bir çeşit değerlendirmeden geçeceğini tespit eden Wellcome Kütüphanesi, ileriye yönelik bir yol haritası belirlemek için standart belge değerlendirme yöntemlerini incelemiştir. Bu konudaki profesyonel görüşler bölünmüş durumdadır. Bazı görüşler eski değerlendirme yöntemlerinin doğuştan dijital belgelerle başa çıkma konusunda yetersiz kalacağını savunurken, bazı görüşler ise iki değerlendirmenin benzer yaklaşımlar sergilediği noktasında hem fikirdirler (Sloyan, 2016, s. 23).

Değerlendirme ve ayıklama birbirini ile ayrılmaz bir parça kadar yakın olan unsurlardır. Ayıklama; kalıcı olarak korunması gereken ve arşivsel değere sahip olan belge ve bilgilerin tanımlanması sürecidir (*Best practice guide to appraising and selecting records for The National Archives*, 2013, s. 15). Uzmanlar ve alanın uygulamacıların bir kısmı değerlendirme süreci gibi ayıklama sürecinin de fiziksel ve dijital ayıklama arasında çok fark olmadığını belirtse de bir kısmı da bu uygulamada farklı süreçler gerektiği görüşündedirler. Fiziksel ayıklama sürecinde belgelerin arşive transferi için manuel (geleneksel) olarak ayıklama yapılabilir, değer durumuna bakılabilir. Fakat doğuştan dijital belgeleri tek tek el ile ayıklamamız artan belge hacmi

³Döneminin iddialı koleksiyonlarını bünyesinde barındıran bir kütüphanedir. Erişim adresi: <https://wellcomelibrary.org/>

ve teknolojik durum nedeniyle pek mümkün gözükmemektedir. Bu sebeple dijital ayıklama sürecinde gelişen teknolojinin olanaklarından faydalanmak kurumların işlerini oldukça kolaylaştıracaktır.

Doğuştan dijital belgeleri ayıklamaya başlamış olan kurumlar birtakım programlardan yardım almaktadırlar. Dijital ayıklama için uluslararası platformlarda kullanıldığı bilinen programlara DROID⁴, PRONOM⁵ ve JHOVE⁶ örnek gösterilebilir. Bu ve benzer programlar ve/veya yazılımlar sayesinde kurumlar kapsamında bulunan farklı formatlardaki belgeleri, kopya/yedek belgeleri, hatalı belgeleri, mevcut belgelerin son değiştirme tarihleri, boyutları vb. bilgilere kolayca ulaşp ayıklama işlemini daha kısa sürede ve standart bir şekilde yapmak mümkündür.

Dijital transferin diğer bir aşaması ise hassasiyet incelemesidir. Dijital hassasiyet incelemesi, dijital belgelerin erişimi kamuya açılıp açılmaması konusunda karara vermek için yapılan bir içerik analizi, risk değerlendirmesidir. Bu sayede belgelerin hangilerinin erişime açık hangilerinin kapalı sunulacağına dair kararı alınır, özel ve hukuken gizli kalması gereken bilgilerin açığa çıkmasının önüne geçilmiş olunur. Doğuştan dijital ortamda hassasiyet incelemesi karşılaşılan en zorlu süreçlerden biridir. Fiziksel belgelerin aksine doğuştan dijital belgelerin içeriğini genel bir bakışla hızlı bir şekilde gözden geçirmek mümkün değildir. Dosyaların ayrı ayrı açılması, gözden geçirilmesi ve incelenmesi büyük miktarda depolanan dijital belgeler göz önüne alındığında çok daha zahmetli ve çoğu zaman mümkün değildir. Bununla birlikte, arşivcilerin yasal ve ahlaki sorumlulukları vardır. Bu bağlamda hassas bilgiler kamu malı olarak yayımlanamaz. Diğer arşivleme süreçlerinde bilgisayarların ve otomatikleştirilmiş (veri ve metin madenciliği) süreçlerin kullanılmasıyla işlemler giderek daha verimli hale getirilmekte, bu bağlamda hassasiyet incelemesinde Türkiye’de henüz ciddi bir çalışma olmasa da yurtdışında ciddi akademik çalışmalar yapılmaktadır. Hassasiyetin doğası gereği tanımlanması zordur ve bağlama çok bağlıdır. Duyarlılık (hassasiyet) sadece ne söylendiği meselesi değildir, aynı zamanda kimin, ne zaman, nerede ve ne söylediğine bağlı olarak değişmektedir. Tüm bu inceliklerin üstesinden gelmek için anahtar sözcük

⁴DROID (Dijital Kayıt Nesnesi Tanımlama), İngiliz Milli Arşiv’i tarafından geliştirilen bir dosya formatı tanımlama aracıdır. Erişim adresi: <https://www.nationalarchives.gov.uk/documents/information-management/droid-user-guide.pdf>

⁵PRONOM, veri dosyası formatları ve destekleyici yazılım ürünleri hakkında çevrimiçi bir bilgi sistemidir. Erişim adresi: <http://www.nationalarchives.gov.uk/PRONOM/Default.aspx#>

⁶JHOVE (Harvard Object Validation Environment), dosya formatı tanımlama, doğrulama ve karakterizasyon için açık kaynaklı, genişletilebilir bir yazılım çerçevesidir. Erişim adresi: <https://jhove.openpreservation.org/>

aramalı hassas sözcüklerin tanımlanmasına dayalı yazılım programlarına yüzde yüz güvenmek de çözüm olmayacaktır. Bu durum bilgi profesyonellerini zorluklarla karşı karşıya bırakabilmektedir (Sloyan, 2016, s. 30).

2019 yılında günlük üretilen bilgi miktarı 2.5 milyon kentilyon byte ulaşmıştır. Kentilyon sayısal olarak on dokuz haneli bir rakamı ifade etmektedir (Örneğin; 1.000.000.000.000.000.000). Bu bağlamda 2.5 milyon kentilyon veri, otuz sıfırlı bir rakama eşdeğer olmaktadır. Günlük oluşturulan istatistiklere bakıldığında; 500 milyon tweet gönderildiği, 294 milyar e-posta gönderildiği, Facebook'ta 4 petabayt veri oluşturulduğu, WhatsApp üzerinden 65 milyar mesaj gönderildiği, arama motorlarından 5 milyar arama yapıldığı gözlemlenmektedir. Tüm dijital evrenin 2020 yılına kadar 44 zettabayta ulaşması beklenmektedir. Bu sayı ise evrendeki gözlemlenebilir yıldızlardan 40 kat daha fazla bayt olduğu anlamına gelmektedir. 2025 yılında ise dünya genelinde bu rakamın günlük 463 exabyte veriye ulaşacağı tahmin edilmektedir. Bu veri ise günde 212.765.957 DVD'ye eşdeğerdir (Elem, 2020). Doğuştan dijital belgelerin hassasiyet değerlendirmesi sürecinde binlerce belgeyi bilgisayarda tek tek okumak hassas olup olmadıklarını belirlemek çok zaman alıcı bir eylemdir ve hassas içeriği kaçırma olasılığı kuvvetlidir. Bunun yerine uygulamacı ve uzmanların doğuştan dijital belgelerin hassasiyet değerlendirmesi için önerdiği yöntem bu işlem için belirli yazılımlar kullanmaktır. Bu konularda çalışmaları bulunan ve daha önce uygulamada da yer alan akademisyen Özdemir, fiziksel belgelere uygulanan değerlendirme, ayıklama ve hassasiyet değerlendirmesi işlemlerinin dijital belgelere de manuel olarak uygulanamayacağının zamanla ortaya çıkacağı ve kurumların bu konuda artık farkındalık kazanması gerektiğinin, yapılacak işlemler için yazılımcılardan vb. meslek gruplarından yardım alınması gerektiğinin altını çizmiştir (Özdemir, 2017, s. 54). Bu yazılımlar sayesinde kurumda bulunan dijital belgelerin hangilerinin hassas içerikli olduğunu bulmak ve ona göre belgeleri kullanıcı erişimine sunmak ya da kapatmak daha mümkündür. Şunu da belirtmek gerekir ki yazılımın önemli ve gerekli olduğu kadar o yazılım tanımlamalarını yapan bilgi profesyonellerinin yaptığı iş süreçleri daha değerlidir. Yazılım kodlanılan, tanımlanan bilgi kadar var olabilir, fakat sadece yazılımlarla da hassasiyeti belirlemek çok kolay değildir. Yazılım kullanarak bilinen kişileri tanımlayıp, filtreleyerek aramak mümkündür, fakat örneğin Muammar Kaddafi'nin (orijinalinde Moammar Gaddafi) bilinen 112 farklı şekilde yazımı bulunmaktadır (Gibson, 2009). Aranılan sonuçlardaki karakter değişimleri de bizi doğru

sonuca ulařtırmayabilir. Örnek vermek gerekirse; John Smith ve J'yi aramak doğru sonuç getirebilir fakat J. Smith veya Smith, J. yanlış sonuçlar getirebilir. Bu sebeple teknolojiye yüzde yüz güvenmek de doğru değildir ve her zaman ilgili belgeler konusunda uzmanlar gerekecektir (*The application of technology assisted review to born-digital records transfer, Inquiries and beyond*, 2016, s. 20).

Belgelerin hassasiyet incelemesi ile ilgili yapılan bir çalışmada; kişisel bilgiler, uluslararası ilişkilere zarar verecek bilgiler vb. hassas bilgilerin açığa çıkmasını önlemek için milli arşivlerde arařtırmaya açılmadan önce hassasiyet denetiminin yapılması gerektiğini savunmaktadır. Bunun yanı sıra NARA ve TNA gibi milli arşivlerde transfer öncesi kamu kurumlarının hassasiyet denetimi yapması zorunludur ve bu uygulama ilgili kurumların politikalarında yer almaktadır. Dijital belgelere geçiş, dijital belge hacminin artmasına baėlı olarak mevcut uygulamaların kullanılmasını imkânsız hale getirmesi gibi yeni dijital zorluklar meydana getirmiştir. İlgili çalışma potansiyel olarak hassas dijital belgeleri tanımlayabilen ve önceliklendirebilen bir duyarlılık gözden geçirme sınıflandırıcısı geliřtirmeye yönelik bir çalışmadır. Devlet kurumlarındaki uzmanlar tarafından belirlenen gerçek hassasiyetlere sahip devlet belgelerinden oluşturulmuş bir test koleksiyonunu kullanarak, her belgede bulunan varlıkları göz önünde bulundurmanın bir metin sınıflandırma temeline göre önemli ölçüde gelişebileceğini göstermektedir (McDonald, Macdonald, Ounis ve Gollins, 2014, s. 500)

Her yapılan çalışma aslında bir ihtiyaçtan doğmaktadır. İngiltere’de belgelerin arşive transfer süresinin kısalması⁷ ve dijital belgelerin hassasiyet deėerlendirmesinin fiziksel belgelerinki gibi el ile yapılamayacağı gerçeėi ve ihtiyacı doğrultusunda çözüm arama niyetiyle yola çıkılmıştır. Hassasiyet deėerlendirmesi, dijital transfer aşamalarındaki en zorlu süreçlerden biri olarak görölmektedir. İngiliz Hükümeti ve Glasgow Üniversitesi iş birliėi ile “dijital belgelerin hassasiyet deėerlendirmesi” odaklı bir proje⁸ çalışması gerçekleştirilmiştir. Bu kapsamda yapılan çalışmalar aynı zamanda bir doktora tezinin parçası haline gelmiştir. Çalışmadaki amaç dijital belgelerin teknolojik tabanlı bir uygulama ile hassasiyet incelemesini yapabilmektir. Aynı zamanda amaç kısa sürede dijital belgelerin hassasiyetini inceleyebilmek ve daha fazla belgeyi halka

⁷İngiltere’de 2013 yılında 30 yıl milli arşive transfer kuralının 20 yıla indirilmesi kararı alınmıştır ve bu durum belgeleri deėerlendirirken kısa sürede daha fazla belgenin incelenmesi zorunlu hale gelmiştir.

⁸Abacá projesi, dijital belgelerin bir arşive aktarılmadan önce makul bir maliyetle ve yönetilebilir bir risk düzeyinde hassasiyet incelemelerine olanak tanıyan bir “Dijital Hassasiyet İncelemesi Çerçevesi” geliřtirmek amacıyla kurulmuştur. Ayrıntılı bilgi için inceleyiniz: <https://projectabaca.wordpress.com/>

açabilmektir. Teknolojik metin sınıflandırması destekli yapılan bu çalışma sonuç olarak dijital belgelerin hassasiyet değerlendirmesinde işe yarar ve kullanılabilir bir örnek olarak literatüre eklenmiştir (McDonald, 2019).

Hassasiyet değerlendirmesi ile ilgili yapılan bir diğer çalışma ise, NARA'nın karşılaştığı erişim zorluğuna hassas içeriğe sahip belgelerin nasıl erişime açılacağı konusunda çözüm arama amaçlı yapılmıştır. Çalışmada gelecekte çoğu arşivin bu sorunla karşı karşıya kalacağı bu sebeple bu sorunun çözümü için yapay zekâ, makine öğrenmesi gibi yeni teknoloji fırsatlarını kullanmak gerektiğini savunmaktadır (Baron ve Borden, 2016).

Teknolojinin ilerlemesi ve dijital dönüşüm ile birlikte hayatımızda yer edinen yeni kavramlar oluşmaktadır. Bunlardan birisi makineler aracılığıyla kendini gösteren zekânın dışı vurumu olan yapay zekâdır. Günümüzde makine öğrenmesi, NLP (Natural Language Processing) doğal dil işleme ve yapay zekâ gibi teknoloji odaklı konular bilgi ve belge yönetimi alanında da kullanılmaktadır. Kullanıldığı alanların bazıları ise arşivlerde hassasiyet değerlendirilmesi ve e-değerlendirme/e-ayıklama konularıdır.

McDonald ve meslektaşları yaptıkları bir çalışmada, hassas belgelerin kamuya açılmadan önce hassasiyet denetiminin yapılması gerektiğini, bu işlemin ise geleneksel yöntemlerden ziyade otomatik duyarlılık sınıflandırma teknikleriyle yapılmasına ihtiyaç duyulduğunu savunmaktadırlar. Fakat otomatik duyarlılık sınıflandırmasının da bağlamla ilgisinin bulunması sebebiyle zor bir iş olduğunun altını çizmektedirler. Bir test koleksiyonu üzerinde denedikleri bu yöntemle gerçek hassasiyet içeren devlet belgelerinin tespit edilmesinin diğer yöntemlere göre daha fazla başarılı olduğunu bulmuşlardır (McDonald ve diğerleri, 2017)

Yapılan bir diğer çalışmada, e-değerlendirme/e-ayıklama ve hassasiyet değerlendirmesi konularında arşiv kurumları ve uygulamalarında makine öğrenimi ve doğal dil işleme işlemleri kullanımı ve etkili yarar sağlama amaçlanmıştır. Sonuçta doğuştan dijital belgelerin arşiv süreçlerinde makine öğrenmesi ve doğal dil işlemenin faydası olabileceği sonucuna varılmıştır (Hutchinson, 2020).

Bilgi değerlidir bu bağlamda bir varlık olarak görülmeli ve etkin bir şekilde yönetilmelidir. Dijital bilginin sürekliliğinin sağlanması dijital süreklilik ile mümkündür. Dijital süreklilik; bilgilerinizi ihtiyaç duyduğunuz şekilde, ihtiyaç duyduğunuz sürece kullanma yeteneğidir (*Understanding Digital Continuity*, 2017, s. 4). Tanımından da

anlaşıldığı üzere aslında tüm kavramlar birbiri ile iç içedir ve dijital süreklilik tüm süreçlerin başında yer almaktadır. Bilgi ve belgenin uzun süre erişilebilir, kullanılabilir olması her şeyden önce sürekliliğinin sağlanması ile mümkündür. Bu da yine dijital koruma, risk değerlendirmesi gibi unsurlarla da bağlantılı şekilde ilerlemektedir. Dijital sürekliliğin düzgün bir şekilde uygulanabilmesi için her şeyden önce bilginin varlık olarak kabul görmesi ve ona göre işleme alınması gerekmektedir. Bu konuya önem verilmeli ve kurumlarda bu konudan sorumlu bir yetkili ilgili çalışmanın başına atanmalıdır. Dijital süreklilik ile ilgili bir örnek vermek konunun daha iyi anlaşılmasına yardımcı olacaktır. Örneğin; 2020 yılının başında ilk olarak Çin’de varlığını göstererek tüm dünyayı etkisi altına alan ve Dünya Sağlık Örgütü tarafından “Pandemi” ilan edilen COVID-19 (koronavirüs hastalığı) adlı salgın hastalık baş göstermiştir (COVID-19, 2020). Bu salgın hastalığın aşısı bir yıla yakın süre devam çalışmalar sonucunda bulunmuştur. Bu zamana kadar yapılan tüm çalışmaların (virüsün oluşumu, aşı verileri, aşı ile ilgili yapılan ön test son test çalışma bulguları, hastalara verilen ilaç kodları vb.) bir anda ortadan kaybolduğunu ve dijital ortamda tutulan tüm verilerin yok olduğunu düşünelim. Olası bir yeni virüs vakası patlak verdiğinde elimizde hiçbir bilgi olmayacak, verilen emekler ve yapılan çalışmaların hepsi boşa gitmiş olacaktır. Tüm süreç yeni baştan yaşanacak ve üstelik hastalık ile ilgili verilere ulaşamadığında toplumsal sağlığın olumsuz etkilenmesi ve veriyi tekrar elde etmek için maliyete sebep olacaktır. İşte bu örnek bizlere aslında her alanda dijital süreklilik kavramının hayat bulduğunu ve ne kadar önemli olduğunu göstermektedir. Her türlü felakete ve riske karşı bilgilerimizi, verilerimizi korumak ve sürekliliğini sağlamak oldukça zor ve önemlidir. Aynı zamanda bu konuda Tim Gollins’in bir görüşü bulunmaktadır. Gollins’e göre “parsimonious preservation-asgari koruma” gelecek nesiller için dijital mirasımızı korumak adına gerekli asgari müdahale anlamına gelen bir yaklaşımdır. Bu yaklaşıma göre dijital verilerin sürekliliğinin sağlanamaması, bilgiye erişememek, dosyaları açamamak gibi olası felaketlerden ötürü insanlar oldukça endişe duymaktadırlar. Fakat her şey bu kadar olumsuz değildir. Bu yaklaşım sayesinde veriler öncelikle “ingest” edilmeli yani sistem içine alınmalı ve sonraki işlemlerin ileri bir tarihte nasıl yapılacağına bakılmalıdır. Bu sayede uzun vadede verilerimizi kurtarmak ve sürekliliği sağlamak mümkündür (Gollins, 2009, s. 75-76).

Dijital süreklilik konusu ile ilgili Özdemir ve Cengiz’in bir çalışması bulunmaktadır. Çalışmada Türkiye’de bulunan yasal mevzuattan yola çıkarak dijital

sürekliliğin mevcudiyeti sorgulanmış ve araştırılmıştır. Çalışma sonucuna göre Türkiye’de dijital süreklilik tam anlamıyla uygulanmasa da yasal mevzuatta dijital süreklilik ile bağlantısı bulunan kavramlara ulaşılmıştır (Özdemir ve Cengiz, 2019). Çalışmada incelenen mevzuatlar kapsamında dijital sürekliliğin başlı başına bir kavram olarak Türkiye’de henüz önemselenmediği ve konu hakkında farkındalığın pek yüksek olmadığını söylemek mümkündür.

Bilgi profesyonellerinin yoğun çaba gösterdiği, başlı başına önemli bir konu ise dijital korumadır. Dijital koruma; dijital koleksiyonların uzun vadeli korunmasını sağlamak için etkili stratejiler geliştirmeyi ifade etmektedir (Sadiku, Shadare ve Musa, 2017, s. 5). Dijital dünyada dijital koruma zor olmakla birlikte kesin bir çözümü bulunmamaktadır. Hızla evrim geçiren dijital dönüşüm süreci olarak adlandırılan dönemde henüz dijital korumanın bilinen net bir çözümü bulunmamaktadır. Çoğu zaman kurumlar kendi işlem önceliklerine göre bir koruma yöntemi bulmaktadırlar. Bazı kurumlar koruma politikalarına sahiptir. Koruma politikası en başında bir kurumun sahip olması gereken bir unsurdur. Eğer yapacağınız kurumsal faaliyetlerle ilgili bir yazılı kurala sahip değilseniz, yapılacak olan iş tam anlamıyla düzgün bir işleyişe sahip olmayacaktır.

Dijital arşivler ve içinde barındırdığı materyaller zengin, karmaşık ve kırılgandır. Onlar hızla gelişen teknoloji, modası geçmiş politikalar ve tüm dünyada arşiv sektörü bir beceri boşluğu tehdidi altındadır. Arşivlerdeki gerekli beceri ve kullanılacak araç eksikliği dijital arşivleri çeşitli risklerle tehdit etmektedir. Bu riskler; koruma riski, içerik ve bağlam riski, şeffaflık ve güven riski ile politika riskidir. Konu ile ilgili güncel çalışmalardan biri, İngiliz Milli Arşivi ve Warwick Üniversitesi ile arşiv alanında dijital koruma ile ilgili riskleri ölçen bir karar destek sistemi geliştirmek için iş birliğine gidilen çalışmadır. Bu iş birliği sayesinde dijital malzemeye yönelik riskleri yönetmek için bir araç geliştirilmiştir. Bu araç ise arşivcilere dijital koruma hakkında farklı düşünme yaklaşımları sağlamaktadır (Barons ve diğerleri, 2021).

Koruma ve dijital koruma ile ilgili birçok kurum, milli arşiv çalışmalar ve projeler yapmaktadır. Dijital koruma ile ilgili çok güzel çalışmaları olan ve birçok kurum, ülke vb. ile iş birliğinde bulunan “Dijital Koruma Koalisyonu-Digital Preservation Coalition

(DPC)⁹ bu konunun öncülerindendir. DPC'nin konu ile ilgili birçok çalışması, projesi, eğitimleri bulunmaktadır. Bu çalışmalara araştırmanın ikinci bölümünde ayrıntılı olarak yer verilmiştir.

2.1. Doğuştan Dijital Belgelerin Milli Arşive Transferi İlgili Yapılan Uluslararası Çalışmalar

Dijital belgelerin arşive transferi ve öncesinde yürütülen tüm bilgi yönetim aşamaları uluslararası alanda daha ileri seviyededir. Özellikle arşiv dünyasında başı çeken kurumlardan olan İngiliz Milli Arşivi bu konuda da birçok arşivden ileri seviyededir. Doğuştan dijital belgelerin bilgi yönetim süreçleri ile ilgili İngiliz Milli Arşivi'nin örnek alınacak çalışmaları bulunmaktadır.

Doğuştan dijital belgelerin transfer aşamaları denildiğinde akla değerlendirme, ayıklama, koruma, dijital süreklilik, hassasiyet incelemesi gibi süreçler gelmektedir. Konu ile ilgili yurt dışında yapılan çalışmalar daha çok strateji, rehber, politika gibi yazılı ve yasal dayanaklar ve yol gösterici metinler olarak karşımıza çıkmaktadır. Burada dikkat çeken önemli nokta yapılan çalışmaların öncelikle Milli Arşivler öncülüğünde yapıyor olmasıdır.

Bir eylemin devamlılığının sürdürülebilmesi ve sağlam temeller üzerine inşa edilebilmesi için öncelikle rehber, politika, yönetmelik, kanun gibi yazılı kurallara ihtiyaç vardır. Literatür incelendiğinde, Milli Arşivlerin yazılı kurallar eşliğinde oluşturulan doğuştan dijital belgelerin bilgi yönetim süreçleri ile ilgili karşımıza çıkan tablo aşağıda aktarılmıştır.

İngiltere'de İngiliz Milli Arşivi'nin¹⁰ doğuştan dijital belgelerin korunması ile ilgili bir koruma politikası, dijital süreklilik politikası ve rehberi bulunmaktadır. Aynı zamanda İngiliz Milli Arşivi dijital transfere başlamış ve transfer süreçlerine dâhil olan doğuştan dijital belgelerinden ayıklanmasından, değerlendirilmesi, hassasiyet incelemesi ve adımları ile ilgili çalışmaları bulunmaktadır. Tüm süreçlerle ilgili detayları ise kendi web sitelerinde açık erişim olarak yayımlamışlardır.

⁹Dijital Koruma Koalisyonu, İngiltere'de dijital kaynakların korunmasını ve uluslararası olarak küresel dijital bellek ve bilgi tabanını güvence altına almayı amaçlayan, İngiltere merkezli, kâr amacı gütmeyen bir limited şirkettir. Ayrıntılı bilgi için inceleyiniz. Erişim: <https://www.dpconline.org/>

¹⁰İngiliz Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <https://www.nationalarchives.gov.uk/>

ABD (Amerika Birleşik Devletleri)'deki NARA¹¹ (The National Archives and Records Administration) Milli Arşivi'nin elektronik belgelerin transferi için iki rehberi bulunmaktadır. Bu rehberlerde, elektronik belgelerin değerlendirilmesi, ayıklanması, hassasiyet incelemesi ve transfer süreci ile ilgili bilgilere yer verilmiştir. NARA dijital transfere 2022'den sonra başlayacaktır. NARA'nın dijital koruma politikası ve dijital stratejisi bulunmaktadır.

Avustralya Milli Arşivi¹²,nin dijital geçiş politikası, dijital süreklilik politikası, dijital koruma politikası bulunmaktadır. Aynı zamanda önlerindeki süreci görebilmek için bir stratejik planları bulunmaktadır. Avustralya Milli Arşivi bir dijital koruma politikasına sahiptir. Bununla birlikte Avusturya Milli Arşivi dijital transfer aşamasına geçmiş ve bu süreçten önce çalışma planlarını oluşturmuştur.

Fransa Milli Arşivi,¹³ Hollanda Milli Arşivi,¹⁴ Macaristan Milli Arşivi¹⁵ henüz dijital transfere başlamamışlardır fakat elektronik belgelerin uzun vadeli korunması ile ilgili çalışmalar yapmaktadırlar.

Yeni Zelanda Milli Arşivi¹⁶ dijital transfer sürecini başlatan arşivler arasında yer almaktadır. Doğuştan dijital belgelerin değerlendirilmesi, ayıklanması ve hassasiyet incelemesi ile ilgili çalışmaları bulunmaktadır.

İsviçre Milli Arşivi¹⁷ henüz dijital transfer aşamasına geçmemiştir fakat çalışmalarına devam etmektedirler. İlgili arşiv, bir veri koruma politikasına, dijital arşiv politikası ve arşiv kanuna sahiptir.

¹¹NARA Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <https://www.archives.gov/>

¹²Avustralya Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <https://www.naa.gov.au/>

¹³Fransa Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <http://www.archives-nationales.culture.gouv.fr/>

¹⁴Hollanda Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <https://www.nationaalarchief.nl/en>

¹⁵Macaristan Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <https://mnl.gov.hu/angol>

¹⁶Yeni Zelanda Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <https://archives.govt.nz/>

¹⁷İsviçre Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <https://www.bar.admin.ch/bar/de/home.html>

Estonya Milli Arşivi¹⁸ henüz dijital transfer sürecine başlamamıştır fakat arşivin bir arşiv kanunu bulunmaktadır. İlgili arşivin dijital arşiv çalışmaları bulunmakta ve çalışmalarına devam etmektedirler.

İrlanda Milli Arşivi¹⁹ henüz dijital transfer aşamasına gelmemiştir. Şu an Milli Arşivin bir dijital koruma politikası, dijital belgeler için bir çalışması bulunmamaktadır. Arşiv hali hazırda fiziksel arşiv transfer süreçleri ile ilgilenmektedir. Arşivin bir Arşiv Kanun'u ve arşiv yönetmeliği bulunmaktadır.

İskoçya Milli Arşivi²⁰ dijital koruma stratejisine sahiptir. Arşiv henüz dijital transfer aşamasına geçmemiştir ancak bir dijital transfer altyapısına sahiptir. Dijital sürekliliğe yönelik çalışmalarına önem verdikleri gözükmemektedir. Aynı zamanda İskoçya Milli Arşivi Glasgow Üniversitesi ile dijital belgelerin hassasiyet değerlendirmesi ile ilgili bir proje yürütmüşlerdir.

Danimarka Milli Arşivi²¹ dijital transfere başlayan arşivlerin arasındadır. Arşiv tüm süreçler için gerekli olan bir arşiv kanuna sahiptir.

Görüldüğü üzere yurtdışındaki birçok Milli Arşivin öncelikle bir “Arşiv Kanunu” bulunmaktadır. Arşivlerin birçoğu araştırma konumuz ile ilgili doğuştan dijital belgelerin bilgi yönetim süreçlerine dair kısımlar için genellikle bir politika, rehber, strateji belirlemişler ve temel dayanak oluşturmuşlardır. Böylelikle yapılan ve yapılacak olan çalışmaların daha sağlam temeller üzerine inşa edilmesi garantilenmiştir.

Dijital belgelerin değerlendirilmesi transfer sırasında değil daha önceden yani arşivleme sürecinde bazı unsurlara dikkat edilerek halledilmelidir. Hollier'e göre dijital transferin düzgün ilerlemesi için elektronik belgelerin arşivlenmesi sürecinde düşünülmesi gereken bazı hususlar şu şekildedir:

- Orjinallik. Elektronik belgenin güvenilir ve yasal olarak kabul edilebilir olmasını sağlayacak kurumsal ve teknik stratejiler nelerdir?

¹⁸Estonya Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <http://www.ra.ee/en/national-archives/about-us/>

¹⁹İrlanda Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <https://www.nationalarchives.ie/>

²⁰İskoçya Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <https://www.nrscotland.gov.uk/>

²¹Danimarka Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <https://www.sa.dk/en/>

- Ayıklama ve saklama süreci. Nasıl geliştirilecek ve uygulanacak?
 - Uzun vadeli korumaya değer belgelerin yeni sistemlere göç ettirilmesi. İhtiyaç duyulduğu sürece nasıl erişilebilir ve kullanılabilir kalacaklar?
 - Ortam ve formatların seçimi. Kuruluş genelinde çeşitli elektronik belge kategorileri için hangi standartlar kullanılmalıdır?
 - Üst veri. Üst veriler nasıl tanımlanacak ve kurumsal belgelerle bağlantılı kalması nasıl sağlanacak?
 - Personel için eğitim ve farkındalık yaratma. İyi belge yönetimi uygulamalarını desteklemek için hangi eğitim gereksinimleri ve destekleyici yönergeler gereklidir?
 - Kurumsal politikaya uygunluk. Kurumsal politikaya uygunluk nasıl izlenecek?
- (Hollier, 2001).

Dijital koruma yıllardır arşivler için bir sorun oluşturmıştır. Kullanıcılar için uzun süreli koruma ve erişim öncelik taşımış, bu bağlamda bu konu ile ilgili sürekli bir çözüm arayışına gidilmiştir. Fakat dijital çağın getirdiği değişimlerle birlikte artık odak noktası doğuştan dijital belgelerin üretimden itibaren değerlendirilmesi, ayıklanması, hassasiyet değerlendirmesi, arşive transferi gibi konuları beraberinde getirmektedir. Doğuştan dijital belgelerin değerlendirilmesi ile ilgili yapılan çalışmalardan birisi Wellcome Kütüphanesinin yapmış olduğu bir çalışmadır. Bu çalışmada kütüphane doğuştan dijital belgelerinin değerlendirilmesi ve hassasiyet değerlendirmesi üzerine çeşitli değerlendirme teknikleri kullanarak bir iş akışı yürütmüştür. Aynı zamanda iş süreçleri kolaylaştırmak adına DROID adlı bir program da kullanmışlar. Çalışma sonucunda değerlendirme ve hassasiyet değerlendirmesinin doğuştan dijital belgeler için kolay işlemler olmadığı fakat artık fiziksel belge transferinden uzaklaştığımızı, bu süreçlerin teknik boyutlarının birçok karışık iş akışına sahip olduğu ama yine de teknolojik imkânları kullanarak bu süreçleri ilerletmenin faydası olduğu bilgisine ulaşılmıştır (Sloyan, 2016).

Günümüzde büyük verinin savunucuları değerlendirme ve ayıklama yöntemlerinin eskimiş olduğunu savunmaktadırlar (Yeo, 2018, s. 45). Bunun sebebi artık dijital zorluk diye adlandırılan fizikselden sanala geçiş ve dijital belgelere fiziksel belgeler gibi müdahale etmenin yeterli olmamasıdır. Bu bağlamda dijital belgelerin bilgi yönetim süreçlerini kolaylaştırmak, sisteme oturtmak, işlerlik kazandırmak için teknolojik değişime ayak uydurmak ve çalışmalara öncelik vermek elzem gözükmektedir. Bunun için gerekli olan şey uygulamadaki ihtiyaçları belirleyip teknik ve yasal zemini

doldurarak bir sistem yapısı meydana getirmektir. Her yeni teknoloji dijital belgeler ve dijital arşivler için zorluklar doğurmakta ve bu değişim süreklilik arz etmektedir.

Dijital belgelerin transferi ile ilgili Özdemir'in bir çalışması bulunmaktadır. Çalışma; İngiltere'deki transfer konusundaki 30 yıldan 20 yıla indirilme değişikliği kapsamında dijital transfer süreçlerinin değerlendirilmesini ele almıştır. Çalışma kapsamında İngiltere'deki 23 kuruma anket uygulanmıştır. Hedef kitle olarak dijital belgelerin İngiltere Milli Arşivine en yüksek düzeyde transferine sahip olan kurumlar arasından seçilmiştir. Çalışmada analiz edilen unsurlar; değerlendirme, ayıklama, hassasiyet değerlendirmesi, belgelerin transfer sürecinde kabul edilen tarih unsurlarıdır. Araştırma esnasında anket yapılan kurumlardan sadece bir tanesi dijital belgelerini Milli Arşive aktarırken, çoğu kamu kuruluşunun doğuştan dijital belgeler için gerekli olan farklı düşünce yapısı, beceriler ve mevcut arşivleme süreçlerini hesaba katıp planlamadıkları bulgularına erişilmiştir (Özdemir, 2019, s. 224).

2.2. Doğuştan Dijital Belgelerin Bilgi Yönetim Süreçleri ile İlgili Türkiye'de Durum ve Yapılan Çalışmalar

Günümüzde Türkiye'de henüz doğuştan dijital belgelerin arşive transfer süreci başlamamıştır. Konu kapsamında resmi olarak bir belgenin dijital belge kabul edildiği tarih e-imza kanunu (2004) ile birlikte yürürlüğe girmiştir. Bununla birlikte 2008 yılında kurumlarda EBYS zorunlu hale gelmiştir. 2019 yılında güncellenen Devlet Arşiv Hizmetleri Hakkında Yönetmeliğe dayanarak son işlem tarihi üzerinden 20 yıl geçmiş ya da 15 yıl sonunda karara bağlanmış belgelerin arşive transferinin yapılması hakkındaki bilgiye göre ülkemizdeki dijital belgelerin bazıları için çoktan arşive transfer zamanı gelmiş ve geçmekte, bazıları için ise zaman yaklaşmaktadır. Bu zamanı günümüzden e-imza kanununun kabul edildiği tarihe kadar götürürsek bu süreyi 18 yıl olarak hesap etmek mümkündür. Kurumlarda EBYS'nin zorunlu hale getirilmesini baz aldığımızda ise 15 yılın tamamlandığını görmekteyiz. Ülkemizde henüz bir Milli Arşiv Politikası bulunmamaktadır. Bakanlar kurulunun imzalamış olduğu "Milli Arşiv Kanun Tasarısı" 07.04.2006 tarihinde TBMM Başkanlığı'na gönderilmiştir (Milli Arşiv Kanun Tasarısı, 2006). Sonrasında kanun tasarısı ile ilgili bir gelişme olmayıp halen Türkiye'nin bir Milli Arşiv Kanun'u bulunmamaktadır. Türkiye'de dijital belge üretimi 2000'li yılların başından itibaren olmasına rağmen bundan sonraki süreç ile ilgili eksik bir yol haritası mevcuttur. Konu ile ilgili bir yol haritasının ya da bir başka deyişle resmi bir politikanın olmayışı, bu konudaki çalışmaları da kısıtlamaktadır. Doğuştan dijital belgelerin süreçleri

ile ilgili bir yol haritası gereksinimi oldukça elzemdir. Türkiye’de yaygın olan ve işleyişini sürdüren çalışmalar elektronik belgelerin süreçleri ile ilgilidir ve bu bağlamda Türkiye’de EBYS²² çalışmaları yaygınlaşmış bulunmaktadır. Türkiye’de 2007 yılında TS 13298 Elektronik Belge Yönetimi Standardı yayımlanmıştır. Bundan sonraki süreçte Başbakanlık tarafından yayımlanan bir genelge ile tüm kamu kurum ve kuruluşlarında EBYS zorunlu tutulmuştur (Elektronik Belge Standartları Hakkında Genelge, 2008; Kandur, 2011, s. 6). Bu sayede her kurumda EBYS alt yapısı oluşturulmuştur. EBYS öncesi işleyen klasik arşiv sistemleri yerini EBYS ile birlikte elektronik belge yönetim süreçleri almıştır. Elektronik belgeler üretildiği tarihten itibaren standart dosya planı ve kendi üst verileri ile birlikte sistem içinde tanımlanır ve gerektiğinde oluşturulan özel kodlarla erişimi sağlanır (Dede ve Akbayır, 2017, s. 286). Kurumlarda EBYS’ye geçildikten sonraki süreçte hala eski sistemlere göre klasik arşivciliğin devam ettiği ve bunun sonucunda da bazı olumsuzlukların ortaya çıktığı gözlemlenmiştir. Bunlardan birisi standart dosya planına uyulmamasıdır. Kurumların birçoğunda kısa zaman önce oluşturulan bir belgeye erişilememesi ya da çok uzun zaman harcanarak belgenin bulunması bu duruma örnektir (Dede ve Akbayır, 2017, s. 288). Diğer bir sorun elektronik ortamda oluşturulan her belgenin bir nüshasının çıktısının alınarak dosyalanmasıdır. Bu durum yurtdışında da yaygın görülen bir unsurdur. Örneğin yapılan bir araştırmada İngiltere’deki Çalışma ve Emeklilik Bakanlığı’nın hala üretilen dijital belgelerin bir nüshasını fiziksel olarak da tuttukları gözlemlenmiştir (Özdemir, 2019, s. 231). Aynı zamanda elektronik ortamda oluşturulan tüm belgeler fiziksel ortamdaki belgeler gibi dosya bütünlüğü içinde olmalıdır (Dede ve Akbayır, 2017, s. 290). Fakat buradan “dijital belgelere de fiziksel belgelere yapılan muamele yapılabilir” algısı oluşmamalıdır. Bu görüş artık geçerliliğini yitirmiştir. Burada terimler arasındaki farkları terminolojik olarak belirtmek faydalı olacaktır. Arşiv Terminolojisi Sözlüğü’ne göre elektronik ve dijital genellikle eşanlamlı olarak kullanılır ancak elektronik analog ve dijital formatları içerir. NTSC ve PAL video ve AM ve FM radyo analog elektronik formatların örnekleridir. HDTV bir dijital video, XM bir dijital radyo formatıdır. Analog dijitalden farklıdır. Analog format örnekleri arasında fotoğraf baskıları, sinema filmi, erken ses ve video kaseti, fonograf kayıtları ve kâğıt üzerinde metin yer alır. Elektronik belgeler hem analog hem de dijital bilgi formatlarını kapsayabilir ancak terim esas olarak dijital

²²“İdarelerin faaliyetlerini yerine getirirken hazırladıkları ve faaliyetlerinin delili olabilecek e-Yazışma Teknik Rehberi’ne uygun belgelerin içerik, üst veri, format ve ilişkisel özelliklerini koruyan, belgelerin ait olduğu fonksiyon veya işlem için delil teşkil eden ve aidiyet zinciri içerisindeki yönetimini elektronik ortamda sağlayan sistem” (Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik, 2020).

bilgisayar sistemlerinde depolanan bilgileri ifade eder. Elektronik belgeler çoğunlukla elektronik formatta (doğuştan dijital) oluşturulan belgeleri ifade eder ancak bazen diğer formatlardaki (yeniden doğmuş dijital veya doğuştan analog) belge taramalarını tanımlamak için kullanılır. Elektronik belgeler genellikle fiziksel (kâğıt) belgelere benzer; mektuplar, e-posta, raporlar kelime işlem dosyaları ve diğer belgeler. Elektronik belgeler genellikle veritabanları ve coğrafi bilgi sistemleri gibi daha karmaşık biçimlere sahiptir. Doğuştan dijital bilgiler, dijitalleştirilmiş olanlardan farklıdır. Dijitalleştirilmiş belge taranmış (ve muhtemelen OCR kullanılarak karakter verilerine dönüştürülmüş) kâğıt üzerinde oluşturulan bir belgeyi tanımlar. Kelime işlemci kullanılarak oluşturulan bir belge doğuştan dijital olarak tanımlanabilir (Pierce-Moses, 2005).

Dijital bilgi ve belgeye doğası gereği farklı muamele yapılmalıdır. Burada kastedilen şey aslında örnek vermek gerekirse İngiliz Milli Arşivi'nin benimsediği yenilikçi dijital arşiv (disruptive digital archive) modeli yaklaşımıdır. Dijital ve fiziksel birbirinden farklıdır ve doğaları gereği benzer şekillerde işlenemezler. Fiziksel belgelerin oluşturduğu arşiv birinci nesil bir arşivdir fakat dijital belgelerin oluşturduğu arşiv ikinci nesil bir dijital arşivdir (*Digital Strategy*, 2017, s. 6).

Çoğu elektronik işlem Bilgi Yönetim Sistemleri üzerinden yapılmakta ve süreçler sistemden ileri gidememektedir. Bir bilgi yönetimi sistemi olarak EBYS'den sonraki süreçlere yönelik bir planlama yapılamamaktadır. Çok önemli bir başka husus ise EBYS'nin bir yönetim sistemi yerine bir arşiv olarak kullanılmasıdır. Dijital transfer konusunda kurumların önünde yol gösteren resmi bir politikanın olmayışı yapılacak olan çalışmaların önünü kapamaktadır. Aynı zamanda bu süreçler sadece dijital belgelerin arşive transferi için değil kurumsal, verimli ve etkin bir bilgi yönetim süreci için de gereklidir.

Özdemir yayımlanan bir çalışmada öncelikle her sürecin bilginin varlık olarak kabul edilmesi gerektiği ile başladığını vurgulamıştır (Özdemir, 2017, s. 49). Kurumlarda bilginin varlık olarak kabul edilmesi önemlidir. Bilgi varlığı; “tek bir birim olarak tanımlanabilen ve yönetilebilen, dolayısıyla anlaşılabilir, paylaşılabılır, korunabilir ve etkili biçimde kullanılabilir olan bilgi bütünüdür” (*What is an information asset?*, 2017, s. 1). Özdemir dijital belgelerin fiziksel belgelerden farklı olarak üretildiği andan itibaren yönetilmesi gerektiğini savunur. Eğer bu belgeler milli hafıza için değerli kabul edilip arşive transferi gerçekleştirilecekse üretildiği andan itibaren bilgi varlığı olarak kabul edilmelidirler aksi halde o bilginin sürdürülebilirliği imkânsız hale gelip milli hafıza da

zarar görecektir (Özdemir, 2017, s. 49). Konu ile ilgili bir diğer önemli nokta ise dijital süreklilik kısmıdır. Dijital süreklilik bir bilginin oluşturduğu andan itibaren düşünülmeli ve uygulanmalıdır. Çünkü dijital süreklilik kurumların faaliyetlerinin düzgün yönetiminde yardımcı olur. Dijital süreklilik iyi anlaşılmayıp yönetilmedikçe, belgelerin imhası zorlaşır, bilgi ve belgenin transferi sırasında sıkıntılar oluşur, belge formatları gerektiğinde açılmaz vb. sorunlarla kurumlardaki bilgi ve belge bütünlüğü olumsuz yönde etkilenir (Özdemir, 2017, s. 50). Tüm bu süreçlerin önemsenerek bilginin üretildiği andan itibaren gerçekleştirilmesi sonraki süreçlerin düzgün ilerlemesini ve zorlukların aşılmasını kolaylaştıracaktır.

Arısoy ve Özdemirci'nin elektronik belgelerin Milli Arşive transferi ile ilgili yaptığı bir çalışma bulunmaktadır. Çalışma kapsamında belirlenen 36 kurumdan 17'ine ulaşılmış, kurum ve kuruluşlara oluşturdukları elektronik belgelerin Milli arşive transfer süreci ile ilgili bir anket yapılmış ve konu ile ilgili kamu kurum ve kuruluşlarının bakış açısı irdelenmiştir. Ankete katılmayan bazı kurumlar henüz dijitalleştirme aşamasında olduklarını, e-arşivlerinin olmadığını, hala elektronik ortama geçemedikleri cevaplarını vermişlerdir. Çalışma sonucunda, kamu kurum ve kuruluşlarının büyük çoğunluğu elektronik belgelerin arşive transferi ile ilgili bir politika metni olmasını, ilgili işlemleri takip edecek yeterli personelin bulunması gerektiğini, elektronik belgelerin arşive transferinin ne zaman yapılacağını yetkili bir merci tarafından karar verilmesi ve kontrolünün yapılması, elektronik arşivlere erişiminin yetkili personelce sağlanması gerektiği kararları ortaya çıkmıştır (Arısoy ve Özdemirci, 2017). Yine Arısoy yapmış olduğu doktora tezi çalışmasında Türkiye'de elektronik belgelerin arşive transferindeki sürecin nasıl olması gerektiği, bu konuda yapılan çalışmaların yeterli olup olmadığı, transfer için ortak bir dosya formatı kullanılıp kullanılmadığı, tüm süreçlerde aktif rol oynayacak nitelikli personelin olup olmadığı, elektronik belgelerin arşivlenme sürecinde uzun süreli koruma ve erişim problemlerine nasıl çözüm bulunacağı ile ilgili sorulara cevap aramıştır. Türkiye'deki kamu kurum ve kuruluşlarından konu ile ilgili bilgi toplanmış ve değerlendirilmiştir. Çalışmaya göre Türkiye'de bir Milli Arşiv politikasının elzem olduğu ve bununla ilgili modellemelerin ayrıntılı olarak açıklandığı gözlemlenmiştir (Arısoy, 2018).

Türkiye'de kamuya açık belgelerin dijital transferi söz konusu olduğunda öncelikle çözülmesi gereken sorunlar şu şekildedir:

- Hükümet yetkilileri tarafından konunun anlaşılması önemlidir. Veri kaybının doğasının ciddiyeti anlaşılabilmesi ve bu nedenle transfer sırasında devletin dijital bilgilerinin yeterince korunamamasına yol açacaktır.
- Dijital çağda arşiv konularının daha iyi anlaşıldığı kapsamlı bir arşiv mevzuatı oluşturulmalıdır.
- Dijital belgelerin arşive transferi için arşiv düzeyinde bir teknolojik altyapı geliştirilmelidir.
- Diğer ülkelerde olduğu gibi bu süreçten geçen ve ilgili alanda görev alacak personele eğitim imkânı sağlanmalıdır (Özdemir, 2016, s. 124).



ÜÇÜNCÜ BÖLÜM

3. KURUMSAL BİLGİ YÖNETİMİ VE SÜREÇLERİ

Bilgi, yıllar boyunca çeşitli tanımları yapılmış ve üzerinde çalışılmış bir unsur olarak karşımıza çıkmaktadır. Kurumsal bilgi yönetiminden bahsedebilmek için öncelikle bilginin tanımına ve çerçevesine değinmek faydalı olacaktır. Bilgi üzerine yapılan çalışmalar incelendiğinde bilgi kavramının temelde dört ana unsura ayrıldığını görmekteyiz. Bunlar; veri (data), bilgi (information), bilgi (knowledge), bilgelik (wisdom)'tir. Bilginin kavramsal analizine aşağıda yer verilmiştir.



Şekil 1. Bilginin hiyerarşisi piramidi (Tecim, 2020, s. 48)

Veri (Data): “Olayları ve bulundukları durumları göstermek için kullanılan; belirli kurallara, yöntemlere göre düzenlenen; harfler, sayılar, şekiller grafikler ve benzeri sembollerdir”.

Bilgi (Information): “Herhangi bir fiziksel form dâhilinde hazırlanan verinin zihinsel olarak algılanmasıdır. Bu durum bilgi edinme sürecine imkân tanır”.

Bilgi (Knowledge): “Algılananın ötesinde zihinsel durumdur. Anlama ve hayatta karşılaşılan olaylarla anlayışın gelişmesi, deneyimlerin kaydedilmesidir. Bilgi (knowledge) aynı zamanda; kazanılmış deneyimlerin kitap, rapor gibi herhangi bir fiziksel forma dönüştürülmesine olanak tanır”.

Akıl (Wisdom): “Kültür veya toplum tarafından kabul edilen belirli kriter veya değerler çerçevesinde kararları-düşünceleri yansıtacak biçimde bilgi (knowledge)’nin uygulanmasıdır” (Debons, Horne ve Cronenweth, 1988, s. 8; Önal, 1993, s. 338-339).

Bilginin kavramsal tanımları dâhilinde kurumsal bilgi hakkında yapılmış tanımlamalar bulunmaktadır. Literatürde kurumsal bilgi tanımlamaları aşağıdaki şekilde belirtilmiştir.

Kurumsal bilgi, “Kurumun etkinliği, denetimi, yönetimi, geliştirilmesi vb. ile ilgili olarak üretilen, alınan, kullanılan ve bu nedenlerle özel bir nitelik kazanan her türlü malumat, fikir ve olgulardır” (Özdemirci, 2001, s. 2). Kurumsal bilgi, “kurum içinde üretilen veya kuruma dışarıdan gelen, o kurumla ilgili kayıtlı ya da kayıtsız her türlü bilgiyi ifade etmektedir. İnsanların kafasında olan, kurumsal faaliyetler sonucunda oluşmuş ve yazılı bir şekilde kaydedilmemiş kurumsal bilgi kapsamında değerlendirilmektedir” (Odabaş, 2003, s. 3). Yapılan tanımlamalar incelendiğinde, kurum ile ilgili yazılı olan ve olmayan, ayrıca deneyimlere dayalı olarak ta oluşturulabilen her türlü bilgi kurumsal bilgi olarak ifade edilebilir.

Bilgi yönetimi, bir kurumun amaç ve hedeflerine ulaşmada bilginin üretilme ve paylaşılma süreçlerini kontrol altına almak ve en iyi şekilde yerine getirmek için belirlenen süreçler dizisidir (Townley, 2001, s. 44). Başka bir tanıma bakacak olursak bilgi yönetimi, “Bir kurumun entelektüel kaynaklarının üretimini, tanımlanmasını, değerlendirilmesini, tutulmasını, geliştirilmesini ve dağıtımının belirli bir plan dâhilinde yürütülmesini sağlayan teori ve uygulamalardır” (Özdemirci, 2001, s. 179).

Kurumsal bilgi yönetimi; “bilginin sistematik ve bütünlük olarak üretilmesini, toplanmasını, geliştirilmesini, paylaşılmasını, kullanılmasını ve iş süreçlerine aktarılmasını sağlayarak kuruluş ve işletmenin başarısını artırma ve etkin yönetimi gerçekleştirme süreci” olarak tanımlanmıştır (Özdemirci ve Aydın, 2007, s. 170).

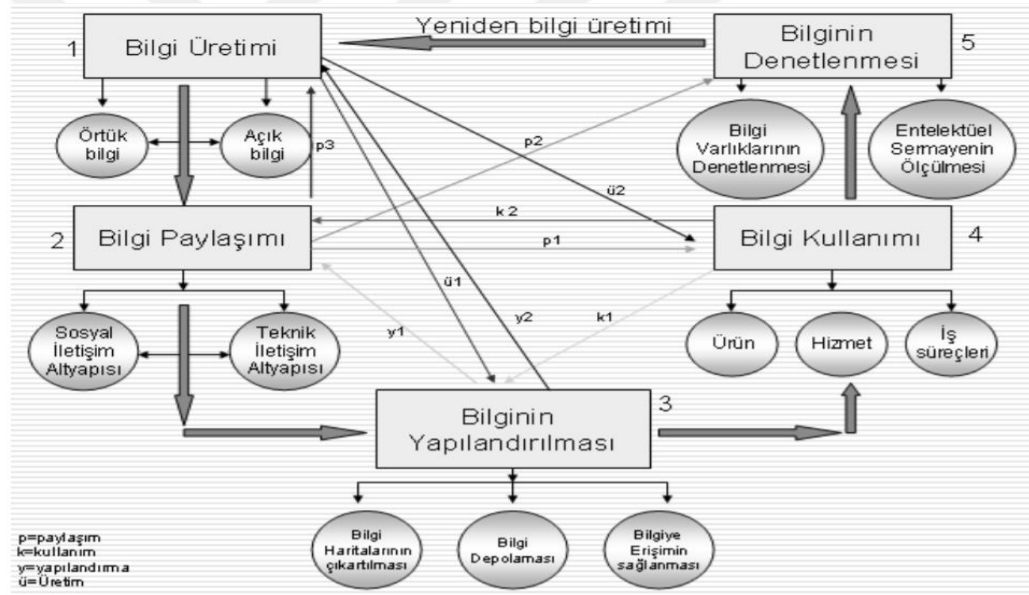
Kurumlarda bilginin üretilmesi, düzenlenmesi, sağlanması vb. süreçleri bilgi ve belge yönetimi uzmanlarının sorumluluğundadır. Kurumlardaki iş süreçlerinin temel ve yasal durumları belgelere dayanır (Külcü, 2018, s. 21).

Literatür çalışmaları incelendiğinde kurumsal bilgi yönetiminde bilginin öne çıkan iki farklı yönü dikkat çekmektedir. Bunlar açık ve örtük bilgidir. Açık bilgi; resim, doküman, söz gibi araçlarla kayıt altına alınarak ifade edilen bilgiyi temsil ederken, örtük bilgi ise sadece yazılı araçlarla kayıt altına alınan bilgiyi değil insanın deneyimleri ile

elde ettiği bilgiyi temsil etmektedir (Barutçugil, 2002, s. 62-63; Çakmak, 2011, s. 20). Başka bir deyişle açık bilgi herkesin kolaylıkla ulaşabildiği kayıtlı bilgi iken, örtük bilgi kurumlarda yapılan iş süreçlerindeki deneyimler sonucu oluşan, insanın zihnindeki bilgiyi temsil eder. Kurumsal bilgi yönetim süreçlerinde bu iki bilgi türü birbirlerinin yerini alarak dönüşüm sürecine girebilmektedir (Odabaş, 2003, s. 364; Townley, 2001, s. 46).

3.1. Kurumsal Bilgi Yönetimi Modelleri

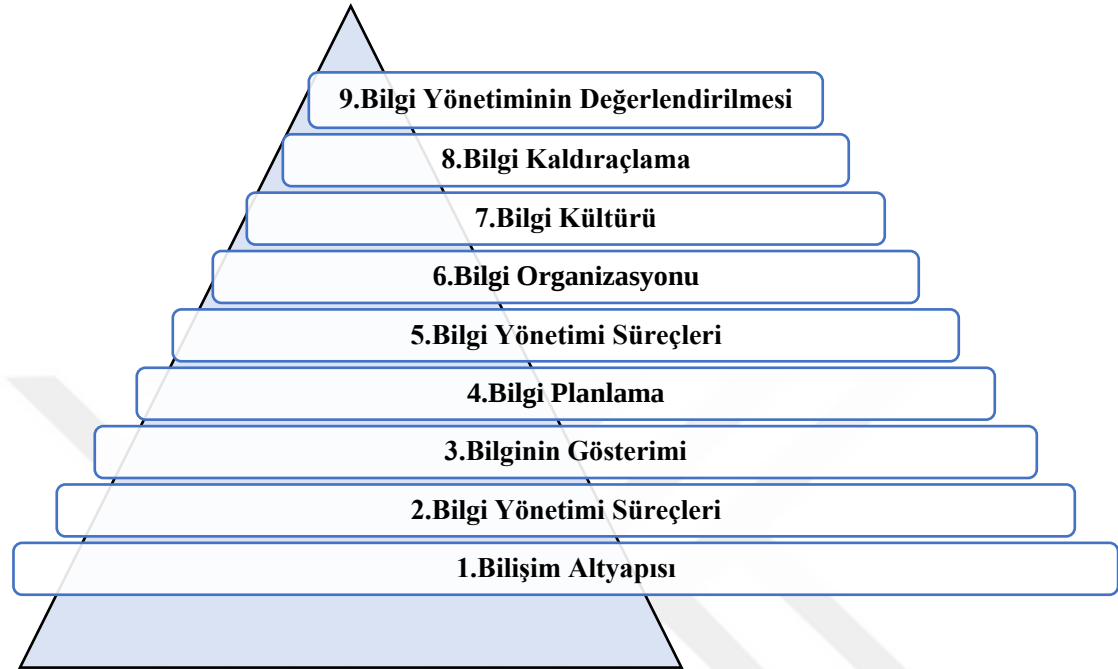
Literatürde bilgi yönetimi ile ilgili birçok araştırmacı tarafından yapılmış çok sayıda model bulunmaktadır. Modellerde bir ya da daha fazla unsurun ön plana çıkarıldığı gözlemlenmiştir. Çalışma kapsamında kurumsal bilgi yönetimi ile ilişkili modellere yer verilmiştir.



Şekil 2. Bilgi yönetimi süreçleri için yaşam döngüsü modeli (Sağsan, 2006)

Şekil 2' de yer alan model 2006 yılında Sağsan tarafından beş temel unsur üzerine inşa edilmiştir. Model, bilginin üretimi aşaması ile başlamaktadır. Bu aşamada kurumlarda bilginin üretim aşamasında odaklanılması gereken yerin bireylerin, grupların belirlenmesi hedeflenmiştir. Sonrasında belirlenen hedefin ürettiği bilginin örtük bilgi mi açık bilgi mi olduğu belirlenir. İkinci aşama modelin en önemli aşamalarından kabul edilen bilginin paylaşımı aşamasıdır. Bu aşama sosyal iletişim altyapısı ve teknik iletişim altyapısı olmak üzere iki şekilde gerçekleşir. Sonraki aşamada bilginin yapılandırılması süreçlerinin içine alan bilgi haritalarının çıkartılması, bilgi depolaması ve bilgi erişiminin

sağlanması süreçleri gerçekleşir. Dördüncü aşama ise kurum içinde üretilen, yapılandırılan ve paylaşılan bilginin kullanımına yöneliktir. Beşinci ve son aşama ise bilgi varlıklarının denetlenmesi ve entelektüel sermayenin ölçülmesi ile gerçekleşen bilginin denetlenmesi aşamasıdır (Sağsan, 2006, s. 30-38).



Şekil 3. Kurumsal bilgi yönetimi modeli (KBYM) (Arslankaya, 2017)

Kurumsal bilgi yönetimi modeli olarak 2017 yılından tasarlanan model, konu bağlamında literatürdeki en kapsamlı model olarak bilinmektedir (Çakmak, 2011, s. 23). Model toplam dokuz unsur üzerine inşa edilmiştir. İlk aşamada bilişim altyapısı ile başlayan model, sırayla bilgi yönetim süreçleri, bilginin gösterimi, bilgi planlama, bilgi yönetimi stratejileri, bilgi organizasyonu, bilgi kültürü, bilgi kaldıraçlama ve son olarak bilgi yönetiminin değerlendirilmesi katmanlarından oluşmaktadır. Bilişim altyapısı bölümünde internet, veri ambarı, belge yönetim sistemleri, yazılımlar vb. bilgi ve iletişim teknolojileri yer almaktadır. Modelin ikinci bölümü olan bilgi yönetim süreçlerinde bilginin yaratılması, edinilmesi, kaydedilmesi, transfer edilmesi aşamaları gerçekleşmektedir. Üçüncü aşamada bilginin bilgisayar tarafından yapısal olarak anlaşılmasının sağlanması, kurumsal olarak anlaşılmasının sağlanması ve serbest gösterim olarak işlemektedir. Dördüncü aşama olan bilginin planlanması aşamasında ise, kurumun amaç ve hedefleri doğrultusunda yapması gereken planlamalar, stratejiler yer almaktadır. Beşinci aşama olan bilgi yönetim stratejileri kısmında kurumun bilgi yönetimi ile ilgili stratejilerinin belirlendiği aşama yer alır. Diğer bir aşama ise bilginin organizasyonu, kurumun amaç ve hedefleri doğrultusunda ileriki süreçlerde

yapılacak olan işlerin belirlenerek gruplandırılması ve yetkili kişilere görev ve sorumluluklarının paylaştırılmasıdır. Yedinci aşama olan bilgi kültürü aşaması, kurum çalışanlarının bilgilerini sürekli yenilemeleri, kendilerini geliştirmeleri ve sahip olunan yeni bilgilerle kuruma yenilik katmaları olarak gerçekleşmektedir. Sekizinci aşama olan bilgi kaldıraçlama aşamasında, kurum içinde çalışan tüm personelin mümkün olduğunca aynı seviyeye taşınması hedeflenmektedir. Dokuzuncu ve son aşama olan bilgi yönetiminin değerlendirilmesi aşaması modelin en temel aşamalarından kabul edilmektedir. Çünkü kurumların bilgi yönetimlerinin değerlendirilmesi etkin bir bilgi yönetimini ifade etmektedir (Arslankaya, 2017, s. 109-177)

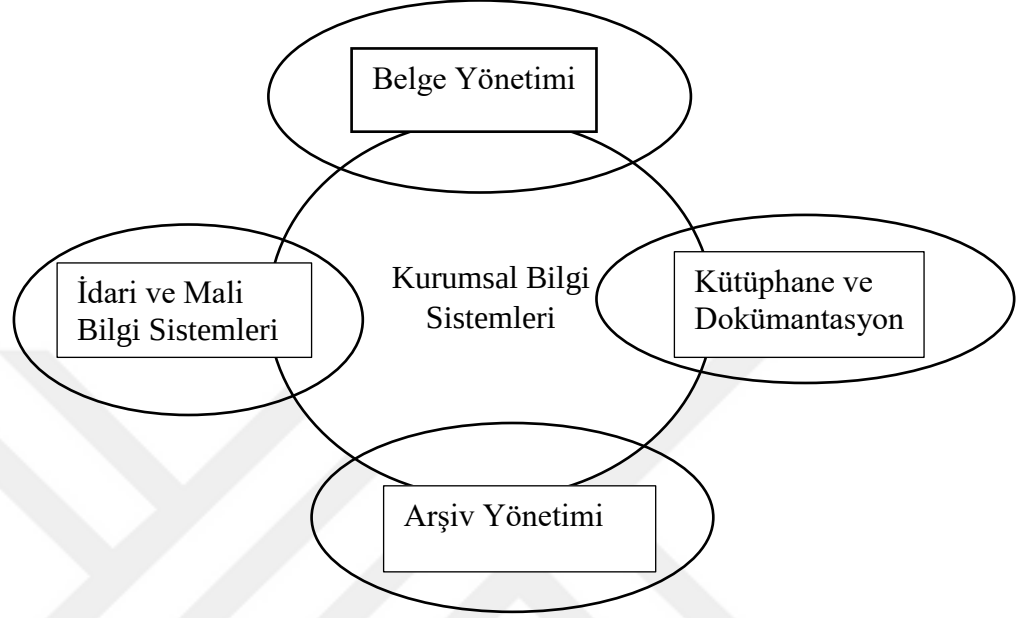
3.2. Yasal Düzenlemeler ve Standartlar Işığında Türkiye’deki Kurumsal Bilgi Yönetiminin Mevcut Durumu

Kurumlarda bilgi ve belge yönetim süreçlerinin verimli, doğru, düzenli ve hızlı yürütülebilmesi, iyi organize edilmiş ve standartlara bağlanmış bir kurumsal bilgi sisteminin oluşturulmasına bağlıdır (Özdemirci, 2001, s. 186). Bunun yanı sıra kurumlarda tüm iş süreçlerinin yazılı olarak belirlenmesi ve belirlenen iş süreçlerinde görev alacak personel ve görev tanımlarının oluşturulması bu kapsamda son derece önemlidir. Türkiye’deki kurumların, elektronik bilgi ve belge yönetimi uygulamalarında örnek alabilecekleri politika, yönetmelik gibi bilgi kaynağı oldukça sınırlıdır (Külcü, 2012, s. 45). Avrupa’da 1980’li yıllarda gündemde olan belge ve arşiv politikaları Türkiye’de uzun yıllarca varlığını gösterememiştir (Çiçek, 2020, s.379). Kurumlarda bilgi yönetim süreçleri belge yönetim süreçlerini de içine almaktadır. Belgeler kurumlarda bir bilgi niteliği taşımaktadır ve dolayısı ile belge yönetim süreçleri de bilgi yönetim süreçlerinin bir alt basamağı, hatta çoğu zaman birlikte yürütülen işlemler silsilesi olarak görülmektedir.

Kurumlarda sağlam bilgi yönetim süreçlerinin olması için aşağıdaki unsurların sağlanması gerekmektedir.

- “Kurum ve kuruluşlarda bir bilgi ağının kurulması,
- Kurum ve kuruluşlarda teknolojik ve elektronik ortamda haberleşme, yazışmalar, resmî belge işlemleri ve arşiv ilişkisi oluşturulması,
- Bilgi ve belgelerin güvenlik, gizlilik ve paylaşılabirlik sınırlarının belirlenmesi,
- Bilgi teknolojilerine ve bilgi güvenliğine ilişkin hukuki düzenlemelerin yapılması,
- Bilgi ve belge depolama konusunda standartların belirlenmesi,

- Elektronik ortamdaki belgelerin işlemlerde kullanımı ve yasal geçerlilikleri konusunda düzenlemeler yapılması,
- Bu alanlarda çalışacak nitelikli insan gücünün istihdamını sağlayacak yapının oluşturulması” (Özdemirci, 2001, s. 186).



Şekil 4. Kurumlarda bilgi yönetim sistemleri (Külcü, 2018, s. 48)

Yukarıdaki şekilde Külcü, son yıllarda bilgi yönetimindeki değişimin tablosunu gözler önüne sermeyi hedeflemiştir. Şekil 4’e baktığımızda kurumlarda bilgi yönetim süreçlerinde hiçbir alan birbirinden bağımsız değildir. Her birim birbiri ile ilişkilidir. Bu sebeple kurumsal bilgi yönetim süreçlerinin beraberinde kurumlarda belge yönetimi, idari ve mali bilgi sistemleri, arşiv yönetimi ve kütüphane yönetimi gelmektedir. Tüm süreçler birbiri ile bağlantılıdır.

Kurumlarda bilgi yönetimi, iş süreçleri ile bağlantılı bir şekilde hareket etmektedir. İş süreçleri üzerinde belirleyici rol oynayan etmenler ise yazılı politika, strateji gibi unsurlardır. Yazılı politikaların varlığı kurumlardaki iş süreçlerinin yapılandırılması ve düzgün işleminde önemli rol oynamaktadır. Bu kapsamda öncelikle konu kapsamında Türkiye’de var olan süreçler bir takım yasal düzenlemeler eşliğinde incelenmiştir.

Türkiye’de 2003 yılında Bilgi Edinme Hakkı Kanunu yayımlanmıştır. Kanunun amacı, “demokratik ve şeffaf yönetimin gereği olan eşitlik, tarafsızlık ve açıklık ilkelerine uygun olarak kişilerin bilgi edinme hakkını kullanmalarına ilişkin esas ve usulleri

düzenlemektir” (Bilgi Edinme Hakkı Kanunu, 2003). Kanunun kapsamı, “kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetlerinde” uygulanmasıdır. Bu bağlamda tüm kamu kurum ve kuruluşları, bireylerin bilgi edinme hakkı kapsamındaki taleplerini karşılamakla yükümlüdürler. Bilgi Edinme Hakkı Kanun’unda belirtilen “Kurum ve kuruluşlar, bu kanunda yer alan istisnalar dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idarî ve teknik tedbirleri almakla yükümlüdürler” ibaresi yer almaktadır. Bu kapsamda kurumlarda bilgi yönetim süreçleri aşağıdaki gibi işlerlik kazanmaktadır: istenilen bilgiyi kullanıcıya erişirme, ulusal ve uluslararası çıkarlar gözetilerek gizlilik kararı gereği verilemeyecek bilgi ve belgelerin belirlenmesi, istenilen bilgi eğer paylaşılamayacak ise yazılı olarak sebebinin açıklanması, şeffaflık, bilgiyi paylaşma süresi, hızı olarak değerlendirilebilir. Dolayısı ile Bilgi Edinme Hakkı Kanun’unun devreye girmesi ile birlikte özgürlük kavramı pekişerek bireyin özgürce bilgi edinme talebi yasalaşmıştır. Bu bağlamda hesap verilebilirlik kavramı da önem kazanmış ve kamu kurumları üzerindeki baskı artmıştır.

Kurumların, bireylerin bilgi edinme isteklerini karşılayabilmeleri için öncelikle faaliyetleri sırasında üretilen belgelerin yönetim süreçleri ile ilgili işlemleri en iyi şekilde yapmaları gerekmektedir (Özdemirci, 2004, s. 65). Eğer kurumlarda bilgi ve belge yönetim süreçleri düzgün işlerse bilgi edinme hakkı kanunu kapsamında da süreçler düzgün işler. Belgelerin üretimi, tasnifi, uzun vadeli korunması, dijital sürekliliği, değerlendirilmesi bu süreçlerden bazılarıdır.

Türkiye’de Bilgi Edinme Hakkı Kanunu ile ilgili yaşanan süreçlerin değerlendirildiği 2013 yılında yapılan bir çalıştayda, bilgi edinmenin bir sınırı olması gerektiği, devletin tamamen şeffaf olamayacağı ve gizliliğin de olması gerektiği dile getirilmiştir. Aynı zamanda kurumların şeffaf, hesap verebilir ve açık bir yönetim anlayışına sahip olması gerektiğinin de altı çizilmiştir. Vatandaşın bilgi isteme hakkına yönelik Bilgi Edinme Hakkı Kanun’u yapısına rağmen bazı kurumların “Bu bilgiyi ne amaçla istiyorsunuz?”, “Bu bilginin sizinle olan ilgisi belirlenememiştir.” gibi yanıtlarla yanlış değerlendirmeler yaparak dönüş sağladıkları belirtilmiştir. Bu durumun kanunumuzun “ilgililik şartı aramayan” ilkesine ters düştüğü görülmekte ve uygulamalarda daha çağdaş olma yoluna gidilmesi gerektiği belirtilmektedir. Yapılan çalıştayda, konu ile iki önemli sorun olduğu dile getirilmiştir. Bunlar; idareden kaynaklı ve talep sahibinden kaynaklı sorunlardır. İdareden kaynaklı sorunların başında yetkililerin

vatandaşlardan gelen taleplerine bilgi edinme hakkı kanunun istisna durumu kapsamında değerlendirme eğiliminde bulunmalarıdır. Bunun sebebinin ise gizlilik kavramının büyük oranda yetkililerinin sorumluluğuna bırakılmasından kaynaklı olduğu dile getirilmiştir. Talep sahibi ile ilgili sorunların başında ise vatandaşın kanun kapsamında bazı noktaları tam olarak anlamamaları gelmektedir. Gelen taleplerin %95'inin bilgi edinme hakkı ile ilgili olmadığı bilgisine yer verilmiştir (*Bilgi Edinme Hakkı Çalıştay Sonuç Raporları*, 2013).

2004 yılında Elektronik İmza Kanun'u yayımlanmıştır. Kanunun amacı, “elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir”. Kanunun 5. Madde'sinde “Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur” ibaresi yer almaktadır (Elektronik İmza Kanunu, 2004). e-İmza kanununda güvenli elektronik imza hükümleri, güvenli elektronik imza oluşturma ve doğrulama araçları, elektronik sertifika hizmet sağlayıcısı, nitelikli elektronik sertifika süreçleri yer almaktadır (Elektronik İmza Kanunu, 2004). Güvenilir e-imza, ıslak imza yerine geçmektedir. Bu sayede hukuki geçerliliği bulunmaktadır. Aynı zamanda güvenilir imzada veri bütünlüğünün sağlanarak izinsiz veride değişik yapılmasını engeller. Bunun yanı sıra bireylerin dijital ortamda yaptıkları işlemleri inkâr etmelerine izin vermez, bu sebeple doğruluğu kanıtlanabilir ve güvenilirdir.

e-İmza kullanımı elektronik belge yönetim sistemi uygulamaları ile birlikte kurumlarda yaygınlaşmaya başlamıştır (Özdemirci, 2019, s. 7). Kurumlarda iş süreçlerinin elektronik belgelerle yapılması imza süreçlerinin de e-İmza ile yürütülmesi gerekliliğini doğurmuştur. Güvenli e-İmza için nitelikli elektronik sertifika gereklidir. Uzun yıllar elektronik imza sektöründe hizmet sunan E-Güven şirketi tarafından yapılan araştırmaya göre kullanıcılar ıslak imza süreçlerinin gereksiz zaman kaybı ve maliyete yol açtığını bildirmişlerdir. Kullanıcılara göre e-İmza genel olarak “zorunluluk” sebebi ile kullanılmaktadır fakat faydaları da bulunmaktadır. E-imzanın birincil kullanım nedeni bazı kamu kurumlarında zorunlu olması sebebiyle öncelik kazanmaktadır. İkincil sebep ise zaman kaybını önlemek olarak belirtilmiştir. e-İmzanın en çok kullanıldığı alanlar kamu projeleri ve e-devlet uygulamaları olarak belirtilmiştir. e-İmza kullanmaya başlamadaki en önemli sebeplerin başında bazı kamu iş süreçlerinde zorunluluğun olması, UYAP sisteminin kullanılması, zaman kaybının önlenmesi ve yasal zorunluluk olması unsurları yer almaktadır. e-imza kullananların %90'ı bu kullanımdan memnun olduklarını belirtmişlerdir. e-imzanın en önemli yararları arasında sırayla onay işlemlerini

hızlandırması, ıslak imza ile aynı geçerliliğe sahip olması ve zaman tasarrufu gelmektedir (*E-imza Kullanım Alışkanlıkları Araştırması*, 2013).

Konu ile ilgili güncel gelişmelerden biri ise, 5070 sayılı elektronik imza kanuna 28 Ocak 2021 tarihinde yapılan düzenleme ile eklenen elektronik mühür (e-Mühür)'dür. e-Mühür "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve mühür sahibinin bilgilerini doğrulama amacıyla kullanılan elektronik veridir. Aynı zamanda, elektronik belgenin veya verinin mühür sahibi tarafından oluşturulduğunu, belgenin veya verinin kaynağını ve bütünlüğünü garanti eden delil kayıdır" (Elektronik İmza Kanunu, 2004). e-Mühür ile birlikte dijital ortamda kurumların kimlikleri yasal olarak ispatlanabilecektir. Bununla birlikte e-Mühür, tıpkı e-İmzanın ıslak imza ile aynı hukuki şartları sağlaması gibi fiziksel mühürle aynı hukuki özellikleri sağlamaktadır. Bu özellik kurumlar için önemli bir gelişmedir. Bunların dışında, e-İmza kişiseldir, e-Mühür ise kurumsaldır.

Türkiye'de elektronik belge yönetimi gelişmiş seviyededir. Birçok kurum ve kuruluş elektronik belge yönetim sistemine (EBYS)'ye geçmiştir ve çalışmalarını EBYS üzerinden yürütmektedir. 2017 yılı EBYS kullanımı, Devlet Arşivleri Genel Müdürlüğü'nün yapmış olduğu sunumda aşağıdaki gibi belirtilmiştir; üniversitelerin %36'sı, belediyelerin %42,5'i, bakanlıkların %89,8'i, diğer kamu kurum ve kuruluşların da %66,1'i EBYS kullanmaktadır (Türkiye Kamu Hastaneleri Kurumu, 2017; aktaran Arısoy, 2018, s. 74).

Ülkemizde standartlaşma çalışmaları ile ilgili yapılan öncü hareket 2003 yılında "e-dönüşüm Türkiye İcra Kurulu"nın oluşturulmasıdır. 2005 yılında ise Devlet Planlama Teşkilatı tarafından eylem planı yayımlanmıştır. E-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı'nda "Elektronik ortamlarda üretilecek, kayıt altına alınacak, başka birimlere ya da kurumlara iletilecek, saklanacak ya da gerektiğinde imha edilecek elektronik bilgi ve belgelerin kayıt, iletim, paylaşım, imha ve güvenlik açılarından tabi olacakları usul ve esaslar ile kurumlarda oluşturulacak elektronik kayıt sistemlerinin birbirleriyle uyumlu işlemesi ve etkin bir şekilde yönetilmesine ilişkin asgari standartların belirlenmesi hususlarında çalışmalar yapılacaktır" şeklinde bir hedef belirlenmiştir (*e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı*, 2005). Bu hedef sonrasında yine 2005 yılında "Elektronik Belge Yönetimi Sistem Kriterleri Referans Modeli (v.1.0)" yayımlanmış ve kullanıma hazır hale getirilmiştir. Belirtilen model geliştirilerek "Elektronik Belge Yönetimi Sistem Kriterleri Referans Modeli (v.2.0)" olarak 2006

yılında kullanıma sunulmuştur. Bundan sonraki süreçte bu model standartlaştırılarak ve Türk Standartları Enstitüsü (TSE) tarafından onaylanarak “TS 13298 -Elektronik Belge Yönetimi Standardı” haline getirilmiştir (Kandur, 2011, s. 6)

Kurumlardaki EBYS süreçleri 2000’li yıllarda başlamıştır. Öncelikle belge yönetimi alanında kabul görmüş ilk standart olan “ISO 15489 Uluslararası Belge Yönetim Standardı” TSE tarafından onaylanmış ve 2001’de yayımlanmıştır (ISO 15489-1, 2001). ISO 15489 standardı, bilgi ve belgenin üretiminden tasfiyesine kadar uzanan süreci kurumlar için tanımlayarak kolaylaştırmaktadır (Özdemirci, 2003, s. 10). ISO 15489 örnek alınarak TS 13298 Elektronik Belge Yönetimi Standardı hazırlanmıştır. Kurumlarda EBYS süreçlerinin yaygınlaşmasının en temel sebeplerinden biri 2007 yılında TS 13298 Elektronik Belge Yönetimi Standardı’nın yayımlanmış olmasıdır. Standartın yayımlanması sonrasında yayımlanan bir genelge ile kurumlarda kullanımı zorunlu hale getirilmiştir. Aynı zamanda kurumlarda EBYS’nin kullanımının yaygınlaştırılması için Devlet Arşivleri Genel Müdürlüğü önderliğinde çalışmalar yapılmıştır (Kandur, 2011, s. 6). Standart revize edilerek 2009 yılında tekrar yayımlanmıştır. TSE’nin 23 Ekim 2015 tarihli toplantısında standardın 2009 versiyonu tekrar düzenlenerek “Elektronik Belge ve Arşiv Yönetimi Standardı” olarak güncel halini almıştır (TS 13298, 2015). 2015 güncellenen versiyonunda belirgin fark “Elektronik Arşivleme Sistemi Referans Modeli (ELAS/RM)” adlı yeni bir bölümün eklenmiş olmasıdır. Bununla birlikte daha önceki 2009 standardında bulunan “üst veri elemanları” bölümü genişletilerek “üst veri yönetimi” adlı kapsamlı bir bölüm oluşturulmuştur. Yayımlanan standartların güncellenmesi, Türkiye’de konu ile ilgili çalışmaların yapıldığının, farkındalığın olduğunun göstergesidir.

Standartlaşma ile ilgili adımlardan bir diğeri 25 Mart 2005 tarihinde Resmî Gazete yayımlanan Standart Dosya Planı’dır. Standart Dosya Planının amacı, kamu kurum ve kuruluşlarının birbirinden bağımsız olarak yürüttükleri dosyalama süreçlerinin önüne geçmek ve standartlaşmayı sağlamaktır. Aksi halde kurumlar birbirinden bağımsız hareket etmekte, kurumlar arasında ortak bir iş süreci oluşamamakta ve kurum içinde üretilen bilgi ve belgeye erişim de zorlaşmaktadır. Standart Dosya Planı’nın kurumlarda uygulanması ile birlikte aşağıdaki unsurların gerçekleşmesi öngörülmüştür.

- Kurumlarda aynı konudaki belgelerin aynı numaralarla ifade edilmesi,
- Tüm kamu kurumlarında dosya numaraları standart olacağından doğru bilgi ve belgeye erişimin hızlı ve kolay olarak gerçekleşmesi,

- Kurumlar arasında etkili ve düzenli bir dosya ve haberleşme sistemi oluşturulması,
- Kurumlarda dosyalama süreçlerinin otomasyonu ve altyapısının sağlanması,
- Kurum içi ve dışı bilgi ve belge paylaşımının hızlı, kolay ve sistematik hale gelmesi,
- Kurumların dosyama süreçlerinde standartlaşma sağlanarak belgelerin arşivsel süreçlerinin düzgün ilerlemesinin sağlanması,
- Kurum içi ve dışı belge ve iş süreçlerinin daha hızlı ve kolay şekilde halledilebilmesi (*Standart Dosya Planı*, 2005).

Standart Dosya Planının Başbakanlık tarafından genelge ile yayımlanması ile birlikte kamu kurum ve kuruluşlarında uygulanması mecbur hale gelmiştir. Kamu kurum ve kuruluşları arasında dosyalama süreçlerinde iş birliği sağlanmasının önü açılmıştır. Dosya planları ile ilgili yapılan bir çalışmada, kurumlarda elektronik belgelerin çoğunun yanlış dosyalandığı anlaşılmıştır. Konu bağlamında standart dosya planları ile ilgili genelge gibi yasal dayanaklar oluşturulsa da uygulama tarafında eksiklikler bulunduğu belirtilmiştir (Çiçek, 2016).

2010 yılında Yüksek Öğretim Kurulu (YÖK) tarafından standart dosya planı geliştirilerek “Saklama Süreli Standart Dosya Planı” yayımlanmıştır. Saklama süreli standart dosya planının önemi aslında kamu kurumlarında belgenin yaşam döngüsü süresinde saklama sürelerini ve sonrasında milli arşive devredilip devredilmeyeceğinin de belirlenmesidir. Genel anlamda saklama planları, bir kurumun sahip olduğu belgeyi ne kadar süre ile saklaması gerektiğini, ne zaman imha edileceğini ve transfer ile ilgili bilgiler içeren kılavuzlardır. Saklama süreli standart dosya planı, belgelerin birim ve kurum arşivlerinde ne kadar süre saklanacağını ve tanımlanan saklama kodları ile birlikte belgelerin devlet arşivlerine gönderilip gönderilmeyeceğini, imha edilip edilmeyeceğini göstermektedir. Aynı zamanda belirlenen saklama süreleri belgenin işlemi bittikten sonra yani dosya kapandıktan sonraki süreyi temsil etmektedir (Saklama Süreli Standart Dosya Planı, 2017, s. 27).

İş birliği ile ilgili kamu kurum ve kuruluşlarında önemli bir başka gelişme ise Birlikte Çalışabilirlik Rehberi’dir. Birlikte Çalışabilirlik Rehberi ilk olarak 2005 yılında yayımlanmış sonrasında ise güncellenerek ikinci sürümü 2009 yılında yayımlanmıştır. Son olarak 2012 yılında rehber 2.1 sürümü ile yayımlanarak güncel halini almıştır. Birlikte Çalışabilirlik Rehberi e-Dönüşüm Türkiye Projesi kapsamında hayata

geçirilmiştir. Rehber, “başta kamu kurum ve kuruluşları olmak üzere, kamuya elektronik ortamda hizmet sunan tüm kuruluşlar arasında birlikte çalışılabilirliğin sağlanması ve bu çerçevede; yetki ve sorumluluklar, esas ve prensipler, yöntem ve kriterler ile teknik standartların belirlenmesine yöneliktir” (Birlikte Çalışılabilirlik Esasları Rehberi, 2012). Kamu kurum ve kuruluşlarında Birlikte Çalışılabilirlik Rehberi’ne uyulması zorunludur. Rehber teknik, kurumsal ve anlamsal olarak üç boyuta ayrılmıştır. Kamu kurum ve kuruluşları için bilgi sistemlerinde kullanılacak dosya formatları, e-imza formatları, resmi yazışmalarda kullanılacak standartlar, e-posta ve internet aktarım protokolleri, veri entegrasyonu, güvenlik standartları rehberde ayrıntılı olarak belirlenmiştir.

Türkiye’de Ankara’daki üniversitelerin EBYS’lerinin birlikte çalışılabilirliği ile ilgili yapılan bir araştırmada, kurumlarda bulunan EBYS’lerin kurumdaki diğer sistemlerle ve diğer kurumların sistemleri ile birlikte çalışmasının olumlu olduğu bulgusuna ulaşılmıştır. Ayrıca kurumlarda birlikte çalışılabilirliğe yönelik yapılan en yoğun çalışmalar kayıtlı elektronik posta (KEP) entegrasyonu üzerinedir (Dişli, 2019).

Türkiye’deki kurumsal bilgi yönetim süreçlerini ilgilendiren bir diğer gelişme ise TS ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi Standardı, 27001 Standardı ve Bilgi Güvenliği Yönetim Sistemi (BGYS)’dir. Standart 2013 yılında revizyona uğrayarak güncel halini almıştır. Bilgi güvenliği, kurum ve kuruluşların bilgi yönetim süreçlerinin sürekliliğinin sağlanması, doğabilecek tehditlere karşı önlem alınması ve kurum bilgisinin korunmasını hedefler. Kurumda var olan bilgi ister fiziksel ister dijital hangi biçimde olursa olsun yapısına uygun biçimde korunmalıdır (Yılmaz, 2016, s. 45). Kurumsal bilginin güvenliğinin sağlanabilmesi için gizlilik (confidentiality), bütünlük (integrity) ve kullanılabilirlik (availability) ilkelerine göre hareket edilmelidir. Gizlilik, bilginin yetkili kişilerin elinde bulunması anlamına gelmektedir. Bütünlük, bilginin sorumlu olmayan kişiler tarafından değiştirilmesi, bütünlüğünün bozulmasına karşı alınan önlemlerdir. Kullanılabilirlik, bilginin istenildiği zaman kullanılabilme durumudur. Kurumların bilgi güvenlikleri ve iş süreçlerindeki sorunları sadece kendi aldıkları teknik önlemlerle halledebilmeleri mümkün gözükmemektedir. Bu kapsamda devreye Bilgi Güvenlik Yönetim Sistemleri (BGYS) girmektedir. ISO 27001 BGYS’nin kurum ve kuruluşlara kattığı yararlar aşağıda belirtilmiştir.

- “Doğru, güvenilir ve geçerli bilgiler sağlar.
- Fazladan iş yükü ve gereksiz zaman kaybının önüne geçer.
- Riskleri minimize eder.

- İş sürekliliği sağlar.
- Bilgi varlıklarının gizliliğinin korunmasını sağlar.
- Kuruluş genelinde, bilgi sistemleri ve zayıflıkların nasıl korunacağı konusundaki farkındalığı artırır.
- Bilginin ve metotlarının doğruluğunun ve bütünlüğünün korunması, içeriğinin değişmemesi sağlanır.
- Yasal tarafların zorunlu kıldığı kriterler sağlanmış olur.
- Bilgi varlıklarına erişim korunur.
- Kurumsal saygınlık korunur.
- Rekabet avantajı sağlar” (CTR Uluslararası Belgelendirme ve Denetim, 2021).

BGYS'nin kurumlarda hayat bulması için PUKÖ (Planla – Uygula – Kontrol et – Önlem al) modeli kullanılmaktadır. PUKÖ modeli süreçleri bir döngü halinde durmaksızın devam etmelidir. Model kurumun iş süreçlerinin planlaması, planladığı faaliyetleri hayata geçirmesi, süreci kontrol etmesi ve gerekli durumlar için önlem alması şeklinde gerçekleşmektedir (*Bilgi Güvenliği Politikaları Kılavuzu*, 2014, s. 12). ISO 27001 'e göre üst yönetim onaylı bilgi güvenliği politikaları oluşturulmalı, yayımlanmalı ve kurum personeli yayımlanan politikaya göre hareket etmelidir. Aynı zamanda bazı kurum ve kuruluşlarda²³ ISO 27001 belgesi almak zorunlu hale getirilmiştir. Türkiye’de ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı ile ilişki bulunan bir kanun bulunmaktadır. İlgili kanun, 2006 yılından yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu’dur. Kanun’un amacı, “..., kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir” (Kişisel Verilerin Korunması Kanunu, 2016). Kişisel bilgiler kurumların güvenliğini sağlamakla yükümlü olduğu bilgi varlıklarıdır. Bu kapsamda ISO 27001 standardı ile bağlantılıdır. Kişisel veriler hassas verilerdir ve kişinin rızası olmadan işlenemez, bir yere aktarılamaz. Kişisel verilerden sorumlu ve verilerle ilgili tüm süreçleri yürütecek kişi veri sorumlusudur. 2010 yılında 5982 sayılı Kanunla yapılan değişiklikle “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp

²³Ayrıntılı bilgi için ayr. bkz <https://belgelendirme.ctr.com.tr/iso-27001.html>

kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir” maddesi eklenerek anayasada kişisel verilerin korunması hakkına ilişkin durum açıkça belirtilmiştir (*Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular. KVKK Yayınları, Ankara, 2018, s. 12*). Bu kapsamda da tüm kurum ve kuruluşlar, anayasada belirtilen hüküm ve Kişisel Verileri Koruma Kanunu gereğince kişisel bilgileri korumakla yükümlü tutulmuşlardır. Kanunun yayımlanmasından sonra kişisel verileri koruma ile ilgili yönetmelikler yayımlanmıştır. Kanun’da belirtilen Kişisel Verileri Koruma Kurulu oluşturulmuştur. Kanun kapsamında özel ya da kamu kurumu fark etmeksizin yasal yükümlülükler uymayanlara para ve hapis cezası gibi belirli yaptırımlar uygulanacağı belirtilmiştir. Bu bağlamda kurumların konu ile ilgili süreçlerini belirleme, politikalarını oluşturma, önlemlerini alma, bilişim altyapısını oluşturma, kurumdan bir veri sorumlusu yetkilendirme gibi zorunlulukları doğmuştur. Aynı zamanda kurumlardaki kişisel verilerin korunmasına ilişkin süreçler Devlet Denetleme Kurulu (DDK) tarafından da denetlenmektedir.

Üniversite kütüphanelerinde kişisel verilerin korunması konusuna yönelik uygulamaları ve durumlarını ortaya çıkarmak amaçlı yapılan bir çalışmada, Ankara’daki üniversite kütüphanelerine bir anket uygulanmıştır. Çalışmada, çoğu kütüphanelerde kişisel verilerin sahiplerinden onay alınmadan toplandığı ve süreçlere dâhil edildiği görülmüştür. Üniversite kütüphanelerinde kullanıcıların onayı alınmadan sahip olunan kişisel verilerin işlenmesi, kaydedilmesi, saklaması süreçlerinde eksiklik olduğu bilgisine ulaşılmıştır (Şişkin ve Çakmak, 2020).

30 Ekim 2019 tarihinde Cumhurbaşkanlığı Devlet Arşiv Daire Başkanlığı tarafından “2020-2024 Dönemi Stratejik Planı” yayımlanmıştır. Yayımlanan stratejik planın misyonu “Devlet ve toplum hafızasını barındıran arşiv belgelerini arşivcilik standartları ve gelişen teknolojiler çerçevesinde tespit etmek, derlemek, korumak ve araştırmaya açmak suretiyle kamuoyuna güvenilir, kaliteli ve hızlı erişilebilen arşiv hizmetlerini sunmak ve kamu belge yönetimini etkinleştirmektir” şeklindedir 2020-2024 Dönemi Stratejik Planı’nın vizyonu ise; “Ülkemiz arşivlerinin tek merkezden yönetimini sağlamak ve dünyada arşivcilik alanında referans bir kuruluş olmak” şeklinde belirtilmiştir (2020-2024 Dönemi Stratejik Planı, 2019). Stratejik planda kurumun dört yıllık süre içerisinde gerçekleştirmeyi planladığı amaçlar, hedefler bu doğrultuda gelecek

süreçlerde yapılacak çalışmalar ve gereksinimler belirtilmiştir. Konumuz dâhilinde stratejik planda geçen amaç ve hedef bulunmaktadır.

Amaç; “Kamu kuruluşları ile iş birliği içinde kamuda belge yönetiminin etkinleştirilmesi ve arşivcilik anlayışının geliştirilmesi” şeklindedir. Bu amaca yönelik belirlenen hedefler içerisinde ise; “Devlet Arşiv Ağı ve Devlet Arşivi Veri Merkezi kurulmak suretiyle arşiv belgelerinin tek bir sistem üzerinden kolay ve hızlı erişimi sağlanacaktır” maddesi yer almaktadır (2020-2024 Dönemi Stratejik Planı, 2019, s. 6).

Stratejik planın teknoloji ve bilişim altyapısı analizi kısmında “11 sayılı Cumhurbaşkanlığı Kararnamesi ile Başkanlığa verilen yeni görevlerle birlikte bilişim hizmetlerinde yeni bir yapılanmaya gidilmesi kaçınılmaz bir hale gelmiştir. Bu kapsamda Devlet Arşiv Ağı ve Devlet Arşivi Veri Merkezi’nin kurulması amacıyla çalışmalar başlatılmıştır. Yükümlü kurumlarla belge transferini sağlamak amacıyla ağ altyapısında ihtiyaç duyulan güncellemeler yapılarak gerekli donanımlar temin edilmeye başlanmıştır. Bunun yanında kurumların elektronik ortamda devredeceği belgeleri depolamak amacıyla mevcut depolama ünitesinin kapasitesinin artırılmasına yönelik çalışmalar başlatılmıştır” ibaresi yer almaktadır (2020-2024 Dönemi Stratejik Planı, 2019, s. 35).

Devlet Arşivleri Başkanlığı tarafından yayımlanan 2020 yılı faaliyet raporunda “Bütünleşik Arşiv Yönetim Sistemi Projesi Arşiv belgelerinin tespiti, Başkanlığımıza transferi, depolanması ve tasnif edilerek araştırma hizmetine sunulması, yükümlü kurum ve kuruluşların yürütmüş olduğu arşiv hizmet ve faaliyetlerinin değerlendirilmesi, belgelerin tanımlanmasına yönelik kavramsal dizin oluşturulması, Devlet Arşiv Ağı ve Devlet Arşivi Veri Merkezinin oluşturulması, birimler ve faaliyetler arası ilişki ve iş akışlarının tanımlanması ve akabinde birçok modül ve arayüzden oluşacak kapsamlı bir otomasyon sistemi kurulmasına yönelik 24.09.2019 tarihinde Makam Oluru ile BAYS Projesi başlatılmıştır. 22.09.2020’de Savunma Sanayii Başkanlığı ile protokol imzalanarak çalışmalara başlanmıştır” ibaresi yer almaktadır (2020 Yılı Faaliyet Raporu, 2020, s.49). Raporda geçen bu bilgiler dijital belgelerin arşive transferi için oldukça önemli bir adımdır.

Kamu kurum ve kuruluşlarının bilgi yönetim süreçlerini ilgilendiren önemli diğer bir yasal dayanak ise ilk olarak 16.05.1988 tarihli 19816 sayılı Resmî Gazete’de yayımlandıktan sonra 18.10.2019 tarihli 30922 sayılı Resmî Gazete’de güncellenerek yayımlanan Devlet Arşiv Hizmetleri Hakkında Yönetmelik’tir. Yönetmeliğin amacı

“Kamu kurum ve kuruluşlarının iş ve işlemleri sonucunda oluşan belgelerin; düzenlenmesine, gerekli şartlar altında korunmalarının teminine, herhangi bir sebepten dolayı kaybının engellenmesine, Devletin, gerçek ve tüzel kişilerin ve bilimin hizmetinde değerlendirilmelerine, kurum ve kuruluşlar ile şahıslar elinde bulunan arşiv belgeleri ve ileride arşiv belgesi haline gelecek arşivlik belgelerin tespit edilmesine, saklanmasına gerek görülmeyen belgelerin ayıklanmasına, imhasına ve arşiv belgelerinin Devlet Arşivleri Başkanlığına devrine ilişkin usul ve esasları düzenlemektir.” (Devlet Arşiv Hizmetleri Hakkında Yönetmelik, 2019). Yönetmelik güncellendikten sonra değişen en önemli noktalar, belgelerin arşive transferi süresinin değişmesi ve arşive transferde basılı belgelerin yanı sıra dijital belgelerin de yer almasıdır. Belgelerin arşive devri “...en son işlem tarihi üzerinden otuz yıl geçmiş veya üzerinden on beş yıl geçtikten sonra kesin sonuca bağlanmış olup her türlü yazılı evrak, defter, resim, plân, harita, proje, mühür, damga, fotoğraf, film, ses ve görüntü bandı, baskı ve benzeri belgeleri ve malzemeyi..” ibaresi şeklinde yer alırken yönetmeliğin 2019 yılı güncellenmiş halinde “Son işlem tarihi üzerinden yirmi yıl geçmiş veya on beş yıl geçtikten sonra kesin sonuca bağlanmış bulunan ve günlük iş akışı içinde işlevi bulunmayan, varsa tâbi olduğu diğer mevzuatlar ile saklama planlarındaki saklama sürelerini tamamlayan, üretim biçimleri, donanım ortamları ne şekilde olursa olsun geleceğe, tarihi, siyasi, sosyal, kültürel, hukuki, idari, askeri, iktisadi, dini, ilmi, edebi, estetik, biyografik, jeneolojik ve teknik herhangi bir değer olarak intikal etmesi gereken ve bir bilgiyi içeren yazılmış, çizilmiş, resmedilmiş, görüntülü, sesli veya elektronik ortamlarda üretilmiş belgeyi” ibaresi yer almaktadır. Görüldüğü üzere yönetmelikte belgelerin arşive transfer süresi otuz yıldan yirmi yıla düşürülmüş ve bunun yanında yönetmeliğe elektronik ortamda üretilen belgelerin de arşive transfer olacağı maddesi eklenmiştir. Transfer kuralının değişime uğraması kurumlar ve kullanıcılar için olumlu bir gelişmedir. Burada üzerinde durulması gereken konulardan biri ise arşive devredilen belgelerin otuz yaşına gelene kadar kapalı kalacak olmasıdır. Devlet Arşivleri Başkanlığı’nın sitesinde belgelerin ne zaman erişileceği hakkında “Tasnif işlemleri tamamlanan ve en son işlem tarihi üzerinden 30 yıl geçen belgeler araştırmaya açılır. Personel sicil dosyaları ve şahıs dosyaları en son işlem tarihi üzerinden 101 yıl geçtikten sonra araştırmaya açılır” ifadesi yer almaktadır (T. C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı, t.y.). Bu durum doğuştan dijital belgeler için bir zaman sonra belirli riskler taşıyacaktır. Örneğin dijital belgelerin okunamaması, kullanılamaz hale gelmesi vb. Bunun yanı sıra dijital belgelerin 30 yıl kapalı şekilde arşivde yer alması bilgi edinme hakkı kanununa ne kadar uygun ve ne kadar şeffaf bir

durumdur? Tüm belgeler 30 yaşına kadar hassas veri olarak mı kabul edilmektedir? Bunun yanı sıra bir belge 1990 yılında hassas sayılmazken 1999 yılında hassas sayılabilir ya da tam tersi, bu duruma o dönemin koşulları önderlik edecektir.

1988 yılında yayımlanan Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanun'a göre arşive belgelerini devredecek kurumlar "...genel ve katma bütçeli dairelerle (saklama, ayıklama ve imha işlemleri kendi mevzuatına tabi olmak kaydıyla Cumhurbaşkanlığı, Türkiye Büyük Millet Meclisi, Genelkurmay Başkanlığı, Milli Savunma Bakanlığı, İçişleri Bakanlığı, (Ek ibare: 1/2/2000 - 4516/1 md.) Dışişleri Bakanlığı ve Millî İstihbarat Teşkilâtı hariç) mahalli idareler, üniversiteler ve bunlara bağlı sabit ve döner sermayeli kuruluşlar, kamu iktisadi teşebbüsleri, özel kanunlarla kurulan kamu bankaları ve teşekkülleri..." olarak belirtilmiştir. (Muhafazasına Lüzum Kalmayan..., 1988). Bu madde 2018 yılında yayımlanan Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi'nde "Bu Cumhurbaşkanlığı Kararnamesi, Türkiye Büyük Millet Meclisi ve Millî İstihbarat Teşkilatı Başkanlığı hariç olmak üzere 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununa ekli cetvellerde yer alan kamu idarelerini, Genelkurmay Başkanlığını, Kuvvet Komutanlıklarını, mahalli idareler (köyler hariç) ve bunların bağlı kuruluşlarını, kamu tüzel kişiliğini haiz diğer kurum, kuruluş, enstitü, teşebbüs, teşekkül, birlik, fon gibi adlarla kurulmuş olan bütün kamu kurum ve kuruluşlarını, kamu kurumu niteliğindeki meslek kuruluşlarını, vergi muafiyeti tanınan vakıfları ve kamu yararına çalışan dernekleri kapsar" şeklinde belirtilmiştir (T. C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı..., 2018) ve 2019 yılında yayımlanan Devlet Arşiv Hizmetleri Hakkında Yönetmelik'te de referans olarak kullanılmıştır. Görüldüğü üzere Türkiye Büyük Millet Meclisi ve Millî İstihbarat Teşkilâtı Başkanlığı haricindeki daha önce belgelerini arşive transferden muaf tutulan kurumlar yeni düzenleme ile arşive transfer işlemlerinden sorumlu olacaklardır. Bu konuda düzenlemeler olması olumlu gelişmelerdendir fakat konu ile ilgili politikaların eksikliği söz konusudur. Literatürde incelenen çalışmalara bakıldığında akademisyenlerin yıllardır bir arşiv kanunun olması gerektiği yönündeki çalışmalar bulunmaktadır. Hali hazırda bir arşiv kanunumuz yoktur. Bunun yanı sıra Cumhurbaşkanlığı Devlet Arşivleri tarafından yayımlanan dijital belgelerin arşive transferi konusunda yazılı bir politika belgesi ya da yol haritası bulunmamaktadır (Özdemir Şahin, 2020, s. 10).

DÖRDÜNCÜ BÖLÜM

4. DOĞUŞTAN DİJİTAL BELGE VE BİLGİ YÖNETİM SÜREÇLERİ

Günümüzde sürekli değişen ve boyut atlayan bir teknoloji yapısına bağlı olarak birçok kavramı salt tanımlarla sınırlandırmak artık yeterli gelmemektedir. Buna rağmen çalışmaların düzgün bir temele oturması için birtakım tanımlarda bulunmak yerinde olacaktır.

Doğuştan dijital belge (born-digital record); dijital formatta oluşturulmuş belgelerdir (What are born-digital records?, 2020). Bu tür belgeler aynı zamanda dijital belge olarak da adlandırılmaktadır. Dijital belgelere örnek verecek olursak; veri setleri, veritabanları, mailler, metin tabanlı belgeler, sunumlar vb. Daha önce de belirttiğimiz gibi dijital belge sayısallaştırılmış belgeden farklıdır. Sayısallaştırılmış belge daha önce fiziksel ortamda üretilip sonrasında çeşitli yöntemlerle elektronik ortama aktarılırken, dijital belge dijital ortamda oluşturulan verilerden meydana gelmektedir.

Dijital belge çoğu yerde elektronik belge olarak da ifade edilmektedir. Buna göre TS 13298 standardında elektronik belge “Kurumsal aktivitelerin yerine getirilmesi sırasında üretilen ya da alınan; kurumsal kimlik doğrulama sistemleri, elektronik veya mobil imza sistemleri ile imzalanmış her türlü kayıtlı belgeyi ifade eder” şeklinde tanımlanmıştır (TS 13298, 2015, s. 47).

Dijital belgeyi diğer belgelerden ayıran özellikler aşağıda belirtilmiştir.

- Belgelerin ortamı,
- Belgelerin içeriği,
- Belgelerin fiziksel formu,
- Belgelerin işlevi,
- Belgelerin arşivsel değeri,
- Yasal ve idari koşullar (Duranti, 2001, s. 4; Külcü, 2018, s. 168).

Bu noktalar dışında belgeye şekil veren üç ana unsur bulunmaktadır. Bunlar “fonksiyon”, “hukuk” ve “idari işlem”dir. Fonksiyon, kurum içinde yapılacak işler. Örnek olarak üniversitedeki personel özlük işi ya da belediyedeki imar işi gibi. Hukuk, “fonksiyonun yasal çerçevede nasıl gerçekleştiğini açıklamaktadır”. İdari işlem ise,

hukuk kurallarının öngördüğü uygulamalar olarak tanımlanmaktadır (Çiçek, 2015, s. 41-43).

4.1. Doğuştan Dijital Belgelerin Milli Arşive Transfer Aşamaları

4.1.1. Dijital Değerlendirme (Appraisal)

Amerikan Arşivciler Derneği sözlüğünde değerlendirmenin tanımları yapılmıştır. Konu ile ilgili iki tanımı vermek yerinde olacaktır. Bunlar;

1. Yeterli değere sahip, arşive girecek materyallerin belirlenme süreci,
2. Yasal gerekliliklere dayanarak mevcut ve potansiyel faydalara göre saklanacak belgelerin zamanının belirlenmesi süreci, olarak ifade edilmiştir (Pierce-Moses, 2005).

Sözlükte değerlendirme tanımlamalarının altında yer alan nota göre ise, arşivsel bağlamda değerlendirme; belgelerin ve materyallerin kalıcı değere sahip olup olmadığının belirlenmesi süreci olarak ifade edilmiştir (Pierce-Moses, 2005).

Değerlendirme, süreçleri devam eden değerli belgeleri değere sahip olmayanlardan ayırma işlemidir (*What is appraisal?*, 2013, s. 3).

Birçok araştırmacı değerlendirmenin zamanlaması sorununu tartışmıştır. Neredeyse hepsinin vardığı sonuç; “değerlendirme, belgeleri üreten sistemlerin ömrünün başlarında yapılmalıdır” şeklinde olmuştur (*Appraisal task force report*, [t.y.], s. 3). Dijital belgelerin arşive transferi düşünüldüğünde bir değerlendirme sürecinden geçmesi elzemdir. Dijital belgelerin değerlendirilmesi belge oluşturulduğu andan itibaren yaşam döngüsü içinde yapılmalı ve arşive transfer süreci beklenmemeli ve bu bağlamda kurum ve belge yöneticileri tarafından transfere hazır hale getirilmelidir. Dijital belgelerin değerlendirme süreci fiziksel belgelerden farklıdır ve belgelerin yapısı gereği farklı olmak zorundadır.

Dijital değerlendirme fiziksel değerlendirmeden teori olarak farklı olmamakla birlikte bu işlemin farklı bir süreç olarak görülme eğilimi de bulunmaktadır. Belge yöneticilerinin dijital değerlendirme ile ilgili gerekliliği ve geçerliliği kapsamında soru işaretleri bulunmaktadır. Uygulamacılar dijital değerlendirme ile birlikte dijital belge miktarında artış, depolama maliyetlerinde ise azalma olacağını ve dijital belgelerin fiziksel arşivlerdeki gibi depolama baskısına maruz kalmayacağını ve daha iyi korunabileceğini düşünmektedirler (Slovan, 2016, s. 22). Fakat artan dijital belge miktarı

depolamadaki alan sıkıntısını çözmemekte aksine kullanıcı beklentileri değişmekte ve sürekli artış ve erişim isteği artmaktadır.

Literatürde belgeler için farklı değerlendirme çerçeveleri bulunmaktadır. Bunlar;

Makro değerlendirme: Makro değerlendirmede tek tek belgeleri incelemekten ziyade yüksek seviyede belge grupları ile çalışılır. Belgelerin içerik ve bilgi değerleri yerine işlev ve işleyiş yapısı dikkate alınır.

İşlevsel değerlendirme: Bir işlev sonucu oluşan belgelerin saklanması ve işlevsel analizini içeren bir makro değerlendirme alt kümesidir. İşlevsel değerlendirmenin içinde bir teknik değerlendirme süreci de bulunmaktadır. Teknik değerlendirme, istenmeyen dosya formatlarını ve birden fazla nüsha belgeleri belirleme sürecinden oluşmaktadır.

Mikro değerlendirme: Her bir belgenin ayrı ayrı değerlendirildiği çok ayrıntılı bir süreçtir.

Aşağıdan yukarıya değerlendirme: Klasör ve dosya başlıklarının doğru olup olmadığını değerlendiren geniş bir sınıflandırma sistemidir (Sloyan, 2016, s.23).

Değerlendirme süreci; kurumun işleyişi, yapısı, seçim kriterleri, koruma faktörleri, teknik hususlar gibi bir dizi unsurlarla bağlantılı olarak belirlenip ilerlemektedir.

Değerlendirme kendi içinde teknik değerlendirme ve entelektüel değerlendirme olarak ikiye ayrılır. Entelektüel değerlendirme şunlarla ilgilidir: bir nesnenin içeriği ve esas olarak provenans, içerik, özgünlük ve güvenilirlik, düzen ve bütünlük ve içsel değer ile ilgilidir. Teknik değerlendirme, bir nesnenin formatıyla ilgilidir ve bunu sürdürmek için teknik becerimiz olması gereklidir. Hem entelektüel hem de teknik değerlendirme otomatikleştirilebilir ancak her ikisi de çok farklı amaçlara hizmet eder. Biri arşivin özgünlüğü ve güvenilirliği ile ilgilenirken diğeri ise gelecekte arşivde kullanılabilme özelliği ile ilgilenir. Değerlendirmeyi devam eden bir süreç olarak düşünmenin de faydalı olduğu görülmüştür (Harvey ve Thompson, 2010, s.316). Bu sebeple tüm süreçlerin en başına gelecek olduğumuzda bir belgenin üretim/oluşturma süreci çok önemlidir. Çünkü belge oluşturulurken önemsenen unsurlar (özgünlük, güvenilirlik, birlikte çalışılabilirlik, tekrar kullanılabilirlik, tanımla ve onayla kolaylığı, gizlilik, bütünlük) ve format yapısı belgenin sonraki süreçlerini (değerlendirme, ayıklama, transfer) de etkilemektedir.

Belge yönetiminde değerlendirme sürekli bir iyileştirme döngüsüne sahiptir. Değerlendirme sürecinin sonuçları, çeşitli alanlarda fayda sağlamak için kullanılabilir. Örneğin; yasal uygunluk, risk yönetimi, bilgi güvenliği, gizliliğin korunması, bilgilerin yeniden kullanımı veya arşiv belgelerinin korunması gibi. Ayrıca hangi belgelerin/bilgilerin kullanılabileceğini belirlemek için bir araç olarak kullanılabilir (ISO 21496, 2018, s. 2).

4.1.1.1. Değerlendirme Kriterleri

Değerlendirme rastgele yapılan ya da yapılacak olan bir işlem değildir. Değerlendirme yaparken bazı unsurları göz önüne almak gereklidir. Değerlendirmenin birtakım kriterleri bulunmaktadır. Bu kriterler şu şekilde açıklanabilir.

- Değerlendirmenin ilk ve en önemli kriteri misyon uyumudur. Kurumun koruma politikası gereği var olan belgenin kurumun misyonu ile uyuşup uyuşmadığı bilgisi önemlidir.
- İkinci en önemli değerlendirme kriteri dijital belgelerin değeridir. Arşiv yönetimi teorileri, belgelerin değerlerini birincil ve ikincil değerler olarak sınıflandırır. Birincil değerler idari, mali ve hukuki değerler olarak belirlenirken ikincil değerler ise kullanıcı için değeri ifade etmektedir.
- Üçüncü değerlendirme kriteri maliyettir. Aynı içeriğin birden çok sürümünü seçmek belirleyici faktör haline gelebilmektedir.
- Dördüncü değerlendirme kriteri ise fizibilitedir. Korumanın fizibilitesi genellikle koruyucunun teknik kapasitesi tarafından belirlenmektedir (Niu, 2014, s. 71-73).

4.1.1.2. Değerlendirmenin Faydaları

Değerlendirme bilgi ve belge yönetiminin bir bileşenidir. Değerlendirme sürecini erken başlatmak, belge yönetim süreçlerini de olumlu yönde etkilemektedir (*Appraisal process*, 2020). Belgeleri değerlendirmenin birtakım faydaları bulunmaktadır. Bu faydaları şu şekilde sıralamak mümkündür:

- Kurumlar, acil ve sürekli iş ihtiyaçları için yüksek riskli ve/veya yüksek değerli her bilgiyi ve belgelerini tanımlayabilir ve yönetebilirler.
- Kurumlar, kaynaklarını verimli bir şekilde yönetebilirler çünkü uzun süre saklanması gereken belgelerin depolama maliyetleri ortadan kalkabilir, belgeler göç ettirilebilir ve dahası.

- Kurumlar, bilgileri ve belgelerini kolayca bulabilir, alabilir ve kullanabilirler.
- Kurumlar, kalıcı koruma için hangi bilgi ve belgelerin arşiv değeri olduğunu anlayabilirler (*Appraisal process*, 2020).

4.1.2. Dijital Seçim/ Ayıklama (Selection)

Dijital belgelerin değerlendirilmesinden sonraki aşama ayıklama aşamasıdır. Ayıklama; arşiv değeri olan ve korunması gereken bilgi ve belgelerin belirlenmesidir (*Best practice guide to appraising and selecting records for The National Archives*, 2013, s. 15). Belgeleri ayıklama süreci öncelikle hangi belgelerin kuruma toplumsal ve tarihsel olarak değer kattığı hangilerinin katmadığına odaklanma sürecidir.

Uzmanlar ve uygulamacıların bir kısmı değerlendirme süreci gibi ayıklama sürecinin de fiziksel ve dijital ayıklama arasında çok fark olmadığını belirtse de bir kısmı da bu uygulamada farklı süreçler gerektiği görüşündedirler. İçinde bulunduğumuz teknolojik dönüşüm sürecinde öğrendiğimiz şeylerden biri şudur ki; dijitalin doğası farklıdır ve fiziksel belgelere yapılan muamele dijital belgelere yapılamaz.

Fiziksel ayıklama sürecinde belgelerin arşive transfer için manuel olarak ayıklama yapılabilir ve belgelerin değerine bakılabilir. Fakat doğuştan dijital belgeleri tek tek el ile ayıklamamız artan belge miktarı ve teknolojik anlamda pek mümkün gözükmemektedir. Bu sebeple dijital ayıklama sürecinde gelişen teknolojinin olanaklarından faydalanmak kurumların işlerini oldukça kolaylaştıracaktır.

Önceki bölümlerde kısaca belirttiğimiz gibi dijital ayıklama için şu an doğuştan dijital belgeleri ayıklamaya başlamış olan kurumlar birtakım programlardan yardım almaktadırlar. Dijital ayıklama için uluslararası platformlarda kullanıldığı bilinen programlara DROID, PRONOM ve JHOVE örnek gösterilebilir. Bu ve benzer programlar ve/veya yazılımlar sayesinde kurumlarda bulunan farklı formatlardaki belgeleri, fazla kopya belgeleri, hatalı belgeleri, mevcut belgelerin tarihleri, boyutları gibi bilgilere kolayca ulaşp ayıklama işlemini daha kısa sürede ve standart bir şekilde yapmak mümkündür.

Sağlam bir seçim/ayıklama süreci geliştirmek için öncelikle dijital içeriği edineceğimiz yolları anlamak son derece önemlidir. Ardından, dijital içerikle ilgili onu seçip seçmeme kararını etkileyebilecek hem yasal hem de teknik konuları göz önünde

bulundurmak gerekmektedir (Novice to Know-How: Digital Preservation Skills for Beginners- Selecting Digital Content, 2020).

Yasal konular aşağıdakilerle ilgili hususlardır:

- Mülkiyet,
- Fikri mülkiyet hakları,
- Gizlilik ve hassas veriler,
- İçerik sorumluluğu.

Seçim/ayıklama için dikkate alınması gerekebilecek teknik konular ise şunları içerir:

- Virüsler ve kötü amaçlı yazılımlar,
- Depolama ortamı
- Biçimler,
- İçerik hacmi,
- Belgeler ve üst veriler (Novice to Know-How: Digital Preservation Skills for Beginners- Selecting Digital Content, 2020).

4.1.3. Hassasiyet Değerlendirmesi (Sensitivity Review)

Hassasiyet değerlendirme; hangi belgelerin erişime kapatılması gerektiği, hangilerinin erişime açılarak Milli Arşivlere aktarılması gerektiğinin kararının verilmesi aşamasıdır (*Step 3: Sensitivity review*, 2019).

Ülkemizde bulunan Bilgi Edinme Hakkı Kanun'unun amacı; “demokratik ve şeffaf yönetimin gereği olan eşitlik, tarafsızlık ve açıklık ilkelerine uygun olarak kişilerin bilgi edinme hakkını kullanmalarına ilişkin esas ve usulleri düzenlemektir” (Bilgi Edinme Hakkı Kanunu, 2003). Yurtdışındaki bilgi edinme hakkı yasaları gereği demokratik ve açıklık ilkeleri de öne çıkmıştır. Bu kanunlarla birlikte herkes eşit derece bilgi edinme özgürlüğüne sahiptir. Toplum, kanunlar ile birlikte devlet bünyesinde bulunan bütün belgelere erişim hakkı isteyebilmektedir. Buradaki sınır Bilgi Edinme Hakkı Kanun'u Madde 9'da “İstenen bilgi veya belgelerde, gizlilik dereceli veya açıklanması yasaklanan bilgiler ile açıklanabilir nitelikte olanlar birlikte bulunuyor ve bunlar birbirlerinden ayrılabilirse, söz konusu bilgi veya belge, gizlilik dereceli veya açıklanması yasaklanan bilgiler çıkarıldıktan sonra başvuranın bilgisine sunulur. Ayırma gerekçesi başvurana

yazılı olarak bildirilir” şeklinde açıkça belirtilmiştir (Bilgi Edinme Hakkı Kanunu, 2003). Bu madde yakinen belgelerin hassasiyet değerlendirmesi işlemi ile ilgilidir.

En az doksan ülke, kamu belgelerinin halka ücretsiz olarak sunulması veya açılması gerektiğini belirten bilgi edinme özgürlüğü yasalarını uygulamaktadır. Ancak, birçok kamu belgesi, kişisel veya gizli bilgiler gibi hassas bilgiler içermektedir. Bu nedenle, herhangi bir hassas bilgiyi tanımlamak ve korumak için önce halka açılan tüm kamu belgeleri gözden geçirilmelidir. Tarihsel olarak, duyarlılık incelemesi tamamen manuel bir süreç olmuştur. Bununla birlikte, e-posta gibi doğuştan dijital belgelerin benimsenmesiyle, yalnızca insanlar için duyarlılık incelemesi pratik değildir ve insan duyarlılığı gözden geçirenlere yardımcı olacak yeni teknolojilere ihtiyaç vardır (McDonald, Macdonald ve Ounis, 2019a).

Hassasiyet değerlendirmesi işlemi doğuştan dijital belgelerdeki en sıkıntılı ve zor süreçlerin başında gelmektedir. Bunun sebebi, doğuştan dijital belgeleri bazı uygulama ve yazılımlarla değerlendirme ve ayıklama bir şekilde mümkündür. Fakat doğuştan dijital belgelerin hassasiyet değerlendirmesi süreci düşünüldüğünde bu süreç fiziksel süreçten çok daha farklıdır. Fiziksel süreçte belgelerin hassas içeriğe sahip olup olmadığı belgeleri manuel olarak tek tek inceleyip gözden geçirme olanağı olması bakımından ve hata yapma (yani hassas belgeleri erişime açma) olanağı daha az olduğundan bu işlem dijital hassasiyet değerlendirmesi ile kıyaslandığında daha kolaydır.

Dijital kamu belgelerinin hassasiyetle incelenmesine yardımcı olacak teknolojilere duyulan ihtiyaç, İngiltere ve ABD de dâhil olmak üzere birçok ülkede kabul edilmiştir. Ancak bu tür teknolojiler adalet (fairness), hesap verebilirlik (accountability), gizlilik (confidentiality), şeffaflık (transparency) ve güvenlik (safety) “FACTS” ilkelerine uymalarını sağlamak zorunda kalacaklardır. Örneğin, duyarlılık sınıflandırmasının belirli gruplara karşı adil olmayan bir şekilde ayrımcılık yapmamasını sağlamak için yöntemler geliştirmek adaleti, bilgi yayımlamaktan sorumlu devlet dairelerinin veya diğer kamu kurumlarının belgeleri halka açmayı ya da açmamayı seçerken verdikleri kararlardan yasal olarak sorumlu tutulması hesap verebilirliği, hassas bilgileri denetim geçirenlerin görevi icabı gizli bilgiye erişmesi ve yanlışlıkla ya da bilerek dış dünyayla hassas bilginin paylaşılması gizliliği, demokratik kamu kurumlarının kendi içlerinde açık olma prensibi şeffaflığı, hassasiyet inceleme süreci hatasız olmaması ve bazı hassas belgelerin yanlışlıkla serbest kalması sebebiyle teknolojinin kötü amaçlarla kullanılması güvenliği temsil etmektedir. Teknoloji destekli hassasiyet incelemesine olan

talep önümüzdeki yıllarda artmaya devam edecek ve FACTS ilkeleri, teknolojinin başarısının ayrılmaz bir parçası olacaktır (McDonald, Macdonald ve Ounis, 2019a).

Hassasiyet değerlendirmesinde bir risk kategorisi belirlenirken aşağıdaki unsurlar dikkate alınır:

- Materyalin yaşı,
- Materyalin tanımlanabilir olup olmadığı,
- Yaşayan bireylerin varlığı,
- Katalog ne kadar kapsamlı ve ayrıntılı?
- Gizli tutulacağına dair bir bilgi mevcut mu?
- Bilgi nasıl yapılandırılmış (örneğin alfabetik olarak)? (Sloyan, 2016, s. 31).

Kamu belgelerinin halk tarafından bilgi edinme hakkı kanunu kapsamında hassas içeriğe sahip belgeler hariç erişme hakları bulunmaktadır. Bu erişimi sağlamak için öncelikle belgelerin hassasiyet denetiminden geçmesi gerekmektedir. Çünkü bir belgenin hassasiyet değerlendirmesi yapılmadan erişime açılması devlet, kişi gibi unsurların kişisel bilgilerine, devlet özel işlerine erişme imkânı sağlamakta ve bu da ileride olumsuz sonuçlar doğurabilmektedir.

Birçok kamu belgesi, kamuya açıklanmadan muaf olan hassas bilgiler içerir. Bilgi Edinme Hakkı Kanun'u aracılığıyla, örneğin kişisel bilgilerin bu kapsamda ulusal güvenlik sorunları veya ülkenin uluslararası ilişkilerine zarar vermesi muhtemeldir. Bu nedenle, kamuya açıklanması düşünülen tüm kamu belgelerinin ilk önce manuel olarak hassasiyeti gözden geçirilmelidir. Dijital olarak doğan belgelerin hacmi, e-postalar gibi gözden geçirilecek olanlar, kâğıt belgelerden çok daha fazladır. Tüm bu sebeplerden ötürü, dijital hassasiyet incelemesine yardımcı olacak yeni teknolojilere duyulan ihtiyaç uzun süredir farkında olunan bir konudur (McDonald, Macdonald ve Ounis, 2020).

Kamuya sunulan tüm devlet belgeleri, hassas bilgilerin tanımlanması ve korunması için önce manuel olarak incelenmelidir. Bununla birlikte, dijital olarak doğmuş belgelerin yardımsız manuel duyarlılık incelemesi oluşturulan belgelerin hacmi nedeniyle pratik değildir. Bu nedenle, teknoloji destekli bir inceleme dijital belgeler için hem gerekli hem de kaçınılmazdır (McDonald, Macdonald ve Ounis, 2019b).

4.1.4. Uygulamada Dijital Değerlendirme, Dijital Ayıklama ve Hassasiyet Değerlendirmesi

Kurumlarda dijital belgelerin bilgi yönetim süreçleri EBYS üzerinden ilerlemektedir. Belgenin üretimi, üst verilerinin oluşturulması, ilgili konusu bakımından dosyasına kaldırılması süreçleri EBYS içerisinde yapılmaktadır. Bu bölümde aşağıdaki sorulara yanıt aranmaya çalışılmıştır.

- İleride doğuştan dijital belgelerin arşive transferi sürecine karar verildiğinde kurumlar EBYS sürecini nasıl yürütecekler?
- Kurumların dijital belgelerin arşive transferi sürecinde karşılaşacağı zorluklar neler olacak?
- Kurumlar uygulamada dijital belgelerin değerlendirme, ayıklama ve hassasiyet değerlendirme süreçlerini nasıl gerçekleştirecekler?

Dijital belgelerin değerlendirilmesi ve ayıklanması dijital çağda artık birlikte ele alınan süreçler olarak değerlendirilebilir. Teoride bu süreçleri ayrı ayrı ele alsak ta uygulamada birbiriyle iç içe giren süreçlerin olduğunu belirtmekte fayda vardır. Uygulama sürecini örneklerle anlatmak daha açıklayıcı ve anlaşılır olacaktır. Öncelikle konu ile ilgili yasal denetleyici bir politika, strateji, rehber olması ve süreçlerin burada belirlenen adımlara göre ilerlemesi son derece önemlidir.

Dijital değerlendirme belgenin ömrünün başında, üretilirken yapılmalıdır. Böylelikle hangi belgenin değerli olduğu, saklanıp saklanmaması gerektiği ya da ayıklanması gerektiği sürecine daha sağlıklı karar verilebilecektir. Sonrasında ise ayıklama işlemleri ile devam edilecektir. Bu bölümde bahsedilen süreçler fiziksel belgelerin değil dijital belgelerin süreçleri ile ilgilidir ve manuel bir yaklaşımdan bahsedilmemektedir. Bunun yanı sıra uygulamada bahsedilen bu süreçlerin hepsi kurum özelinde düşünülmelidir. Belgelerin içerikleri, değerlendirme süreçleri hassas olup olmadıkları kurumun yapısı ile yakından ilgilidir.

Öncelikle yapılan literatür taramaları ve teorik yaklaşımlar ve incelemeler sonucu elde edilen verilere göre EBYS içerisinde ya da bir veritabanında belgelerin dijital değerlendirme/ayıklama işlemleri şu şekilde yapılabilmektedir.

Değerlendirme ve ayıklama yapabilmenin adımı ilgili verinin tanınması ve iyi anlaşılmasından geçmektedir. O belge yığınının önemini bilme, üst verilerini inceleme, içerik, özgünlük ve güvenilirlik, düzen ve bütünlük ve içsel değerine ait bilgi sahibi olma

ve karar verme son derece önemlidir. Bu kısımlar değerlendirme sürecinde daha önceki bölümlerde belirtilen entelektüel değerlendirme aşamasına girmektedir. Sonrasında ise teknik değerlendirme süreci gelmektedir. Bu süreç ise belgelerin format yapısı ve sürdürülebilirliği ile ilgilidir ve teknolojik bir altyapı gerektirmektedir.

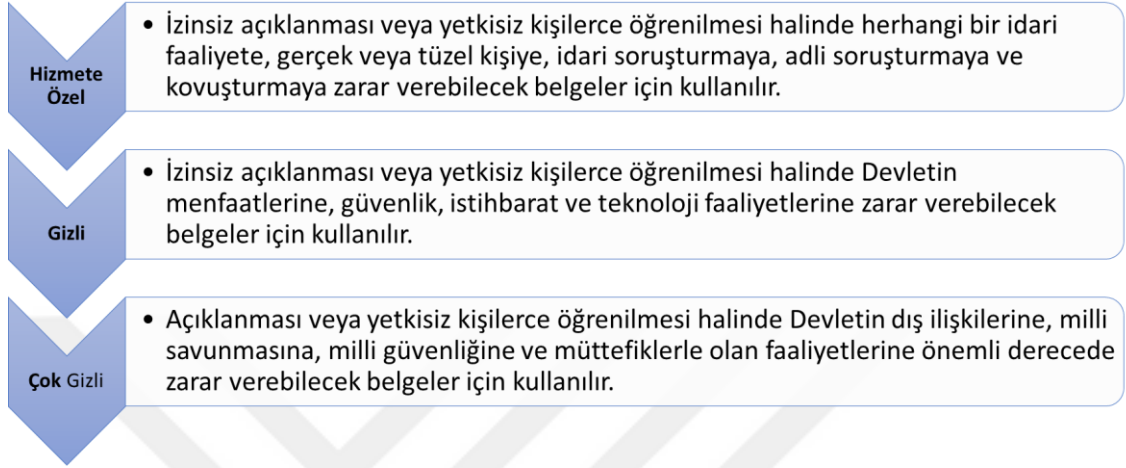
Bir EBYS içerisindeki binlerce belgenin değerlendirmesi ve ayıklama süreçleri için bilinen ve uluslararası platformlarda kullanılan DROID, PRONOM ve JHOVE gibi programları kullanmak gereklidir. Bu programlar yerine kurumun kendi ürettiği ya da ülkede kullanılan ve örnek olarak Devlet Arşivleri tarafından belirlenmiş, aynı amaca hizmet eden bir programdan da yararlanabilir. Bu programlar kullanılarak binlerce belgenin fazla kopyaları, bilgi varlık kayıtları, yaşı, yapısı, önemli olaylar, formatları, hatalı ya da eksik bir veri gibi unsurlar belirlenebilmektedir. Manuel süreçlerle uğraşana dek bu süreçler teknolojinin yardımıyla çok daha kısa sürede halledilebilmektedir.

Gizlilik Dereceleri	AÇIKLAMA
Hizmete Özel	ÇOK GİZLİ, GİZLİ ve ÖZEL gizlilik dereceleriyle korunması gerekmeyen ve fakat bilmesi gerekenlerden başkasının bilmesine lüzum görülmeyen mesaj ve doküman
Özel	Müsaadesiz açıklandığı takdirde milletimizin menfaat ve prestijini haleldar edecek veya bir şahsın zarar görmesini mucip olacak veya yabancı bir devlete fayda telkin edecek mahiyette olan mesaj ve doküman
Gizli	Müsaadesiz açıklandığı takdirde, milli güvenliğimizi, prestij ve menfaatlerimizi ciddi suretle haleldar edecek ve diğer yandan, yabancı bir devlete geniş faydalar temin edecek mahiyette olan mesaj ve doküman
Çok Gizli	Müsaadesiz açıklandığı takdirde, milli menfaatlerimize hayati bakımdan son derece büyük zarar verecek olan ve güvenlik bakımından olağanüstü önemi haiz mesaj ve doküman

Şekil 5. Gizlilik dereceleri ve açıklamaları tablosu (Resmî Yazışmalarda..., (2020))

Cumhurbaşkanlığı Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'e ilişkin kılavuz hazırlamış ve kılavuza göre yönetmelikte belirtilmeyen ayrıntılara yer verilmiştir. Şekil 5 ilgili kılavuzdan alınmıştır. Şekil 5'e göre EBYS içerisinde gizlilik dereceleri "hizmete özel, özel, gizli ve çok gizli" olmak üzere dört

gruba ayrılmaktadır. Konu kapsamında 26 Nisan 2022 tarihinde “Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik” yayımlanmıştır ve bu yönetmeliğe göre gizlilik derecelerindeki “özel” derecesi yaygın kullanılmadığı için kaldırılmış ve dereceler “hizmete özel, gizli ve çok gizli,” olmak üzere üçe ayrılmıştır (Gizlilik Dereceli Belgelerde Uygulanacak...,2022).



Şekil 6. Belgelerin Gizlilik dereceleri

Dijital belgelerin hassasiyet süreçleri ise değerlendirme ve ayıklama süreçlerinden daha karmaşık ve zordur. Örnek olarak EBYS içerisindeki üst veri alanları bakımından süreci inceleyelim.

Tablo 1. Örnek bir EBYS üst veri alanı

Belge Üst Verisi	
Belge No	140012547
Belge Tarihi	03.02.2022
Dosya kodu	010.07.02.01.01
Konu	Görevlendirme
Üretildiği yer	Personel Şube Müdürlüğü
Üreten Kişi	Emine Cengiz
Belge Türü	-
Gizlilik Derecesi	Tasnif Dışı
İvedilik Derecesi	Normal

Tablo 1’de görülen bilgiler canlı bir EBYS içerisinden alanlar değiştirilerek oluşturulmuştur. Bu tabloda dikkat çekilmek istenen nokta EBYS içerisinde bir dijital belgenin gizlilik derecesi üst veri alanının “tasnif dışı” olarak belirtilmesidir. “İlgili mevzuatta “Tasnif Dışı” ibaresi gizlilik derecesi olarak belirtilmemektedir. Tasnif dışı ibaresi için Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik Kılavuz’unda “Tasnif Dışı” olarak adlandırılan belge, herhangi bir gizlilik derecesi

taşımamaktadır. Bu sebeple belgede gizlilik derecesi bulunmadığından belge üzerine ve belge üst verilerine bu ifadenin yazımına gerek duyulmamaktadır” ibaresi yer almaktadır (2020, s.71). EBYS’ler incelendiğinde ağırlıklı olarak gizlilik derecesi alanında tasnif dışı olarak ifadenin geçtiği görülmektedir (Tablo 1). Oysaki tasnif dışı yukarıda da belirttiğimiz üzere bir gizlilik derecesi değildir. Burada kurumların ve kurumlarda çalışan personellerin konu ile ilgili farkındalıklarının eksik olduğu anlaşılmaktadır.

Tablo 2. Canlı bir EBYS içinden alınan “Gizlilik Derecesi” alanı örneği

Gizlilik Derecesi
KEP,
KEP,
KEP,
NULL
ÇOK GİZLİ
NULL
Kurum İçi Gelen Evrak,
NULL
KEP,
Kurum İçi Gelen Evrak,
NULL
Kurum İçi Gelen Evrak,
Kurum İçi Gelen Evrak,
GİZLİ
Kurum İçi Gelen Evrak,
NULL
NULL
Kurum İçi Gelen Evrak,
Kurum İçi Gelen Evrak,
NULL
Kurum İçi Gelen Evrak,
Kurum İçi Gelen Evrak,
Kurum İçi Giden Evrak,
Kurum İçi Gelen Evrak,
NULL

Tablo 2’de farklı bir canlı EBYS içerisinden alınan gizlilik derecesi üst veri alanı gösterilmektedir. Tablo 2’ye göre EBYS içerisinde dijital belgelerin gizlilik durumları “KEP, Kurum içi gelen evrak, Kurum içi giden evrak, gizli ve çok gizli” olarak kullanılmaktadır. Kurum içi gelen ve giden evrak, KEP alanları birer gizlilik derecesi değildir. Burada da yine kurumlardaki farkındalık konusu dikkat çekiyor. NULL alanı ise bu üst veri alanının boş olduğunu yani bilgisinin girilmediğini gösteriyor. Düzgün tasnif işlerinin yapılması için bu üst veri alanının boş bırakılmaması gerekmektedir. Bu sebeple EBYS’lerde bu alanın girişinin zorunlu tutulması gerekmektedir.

EBYS içerisinde hassasiyet denetimi yapılacağı zaman geldiğinde bu işlemin nasıl yapılacağı oldukça önemlidir. Hassasiyet değerlendirmesi işleminin etkili bir şekilde yapılabilmesi için EBYS içerisinde dijital belgelerin üst veri alanlarının da düzgün girilmesi gerekmektedir. Birkaç farklı EBYS örneğini incelediğimizde karşımıza çıkan sorunlardan bir tanesi de ilgili belgenin bir kişisel bilgi içeriyorsa bu kişisel bilginin belirtilmemesidir. Kişisel bilginin belirtilmemesine ek olarak neye göre hangi kanunun hangi maddesine göre kişisel bilgi sayıldığına yönelik bir alanın da olmaması başka bir sorun olarak karşımıza çıkmaktadır. Çünkü hassasiyet değerlendirmesi sadece bir belgenin hassas olup olmadığı ile ilgili değil aynı zamanda bağlamı ile de ilgilidir. Yıllar sonra özel bir konuda bir anahtar kelime verilip kurumda hassas bilgi bulunup bulunmadığına bakılmak istendiğinde bu bilgiler hayati öneme sahip olacaktır. Genel olarak dijital belgelerin hassasiyet değerlendirmesi süreci için EBYS içerisinde aşağıdaki unsurlara dikkat edilmesi gerekmektedir.

- “Gizlilik derecesi” üst veri alanının boş bırakılmaması, zorunlu tutulması,
- Gizlilik derecesi ve gerekçesinin belgenin üretim aşamasında girilmesinin zorunlu olması gerektiği,
- Gizlilik dereceli üst veri alanının yönetmeliğe uygun alanlara göre girişinin yapılması,
- Bir belgenin eğer gizli, çok gizli ya da hizmete özel olduğu belirtiliyorsa sistem içerisinde ek bir üst veri alanı oluşturulması ve bu belgenin neye dayanarak (Bilgi edinme hakkı kanunu, kişisel verileri koruma kanunu vb. kanun maddesi) gizli olduğu belirtilmesi,
- Gizli, çok gizli ya da hizmete özel olduğu belirtilen belge için ek bir üst veri alanında anahtar kelime, ya da ortak alanlar için kod alanı (örneğin tc kimlik numarası ise bunun için 01 kodu belirlenebilir),
- EBYS içerisinde hassas belgeleri kolay bulabilmek için akıllı arama çubuğu (anahtar kelime taraması filtre alanı) olması,

Yukarıda belirtilen maddeler uzun vadede arşive transfer konusu için önemli olmasının yanı sıra etkin kurumsal bilgi yönetimi için de gereklidir.

4.1.5. Transferi Planlama

Bu aşama dijital belgelerin kurum arşivlerinden Milli Arşive transferinin planlanması, gerekli koşullarının sağlanması süreçlerinden oluşmaktadır. Bu aşamada

dijital belgelerle ilgili teknik süreçler planlanıp gerçekleştirilmelidir. Bu aşamada hem belgeler hem de üst verilerin aktarılması sağlanmalıdır. Kurumlar ve Milli Arşiv arasında ilgili protokoller yapılır. Kurum ve Milli Arşiv arasında transferin yapılacağı tarih ve zaman aralığı belirlenmeli, bu görevde bulunacak kurumlardaki sorumlular belirlenmelidir. Dijital belgelerin transfer işlemi tamamlandıktan sonra aktarımı yapılan belgeler kurumda bir süre daha saklanmaya ve korunmaya devam edilmeli ve Milli Arşiv ile irtibat halinde olunmalıdır.

4.1.6. Kontrol Aşaması ve Erişim

Bu aşama dijital belgelerin Milli Arşive teslim edildikten sonraki kontrol süreçleri içermektedir. Bu aşamada Milli Arşivde bulunan konu ile ilgili birimdeki personele önemli görevler düşmektedir. İlgili ekip tarafından dijital belgeler ve üst veriler teslim alındıktan sonra öncelikle virüs taramasından geçirilir. İlgili kontroller sağlanır, dosyalarda bir sorun var ise kurumlarla irtibata geçilir. Dosyalar bir dizi teknik işlemlerden geçirilip sağlaması yapıldıktan sonra esas sisteme alınır. Tüm süreçler tamamlandıktan sonra araştırmacılar için belgelerin erişimi Milli Arşiv web sayfası ya da ilgili bir yazılımla sağlanır.

4.2. Dijital Süreklilik (Digital Continuity)

Dijital süreklilik, dijital bilgileri ihtiyaç duyduğunuz şekilde, ihtiyaç duyduğunuz kadar kullanabilme yeteneğidir (*Understanding Digital Continuity*, 2017, s. 4; *What is Digital Continuity?*, 2019). Dijital sürekliliği sağlamak için etkin bir şekilde çalışmak gerekir aksi halde bilgiler kolayca kullanılamaz hale gelebilir. Dijital süreklilik, bilgilerin eksiksiz, erişebilir ve bu sebeple iş ihtiyaçları için kullanılabilir olmasını sağlamakla ilgilidir. Bilgiler kullanılabilir durumda ise;

- İhtiyaç halinde bulunabilir,
- İhtiyaç duyulduğunda açılabilir,
- İhtiyaç duyulduğunda bilgi ile çalışılabilir,
- Bilginin ne olduğu ve ne hakkında olduğu anlaşılabilir,
- Sunulan içeriğe güvenilebilir (*What is Digital Continuity?*, 2019).

4.2.1. Dijital Sürekliliğin Önemi

Dijital sürekliliği yönetmek kurumsal iş sürecinde ihtiyaç duyulan bilgileri korur. Bu durum hesap verebilir, yasal, etkili ve verimli çalışmayı sağlar. Ayrıca dijital

sürekliliğin iyi yönetilmesi, kurumun itibarını korumasına, bilinçli kararlar almasına, maliyetleri azaltmasına ve daha iyi kamu hizmeti sunmasına yardımcı olur. Dijital süreklilik düzgün yönetilemezse bilgi kaybına sebep olur ve bu durum kurumlar için ciddi sonuçlara yol açabilir (*What is Digital Continuity?*, 2019).

Dijital süreklilik iyi yönetilemezse yüzleşecek olduğumuz olumsuz sonuçlara verilecek örnekler şu şekildedir:

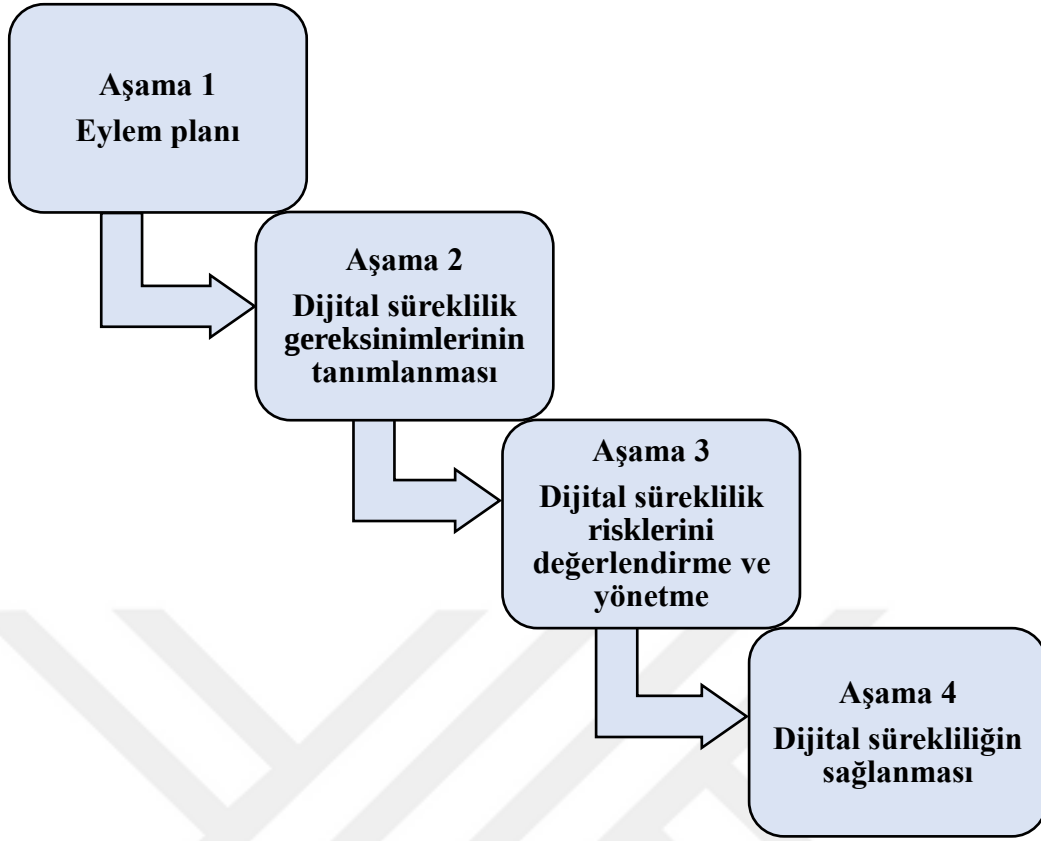
- “Çeşitli formatlarda oluşturulmuş belgeleri açmak ve kullanmak istediğimizde donanım ve yazılımın desteklememesi,
 - bir adli soruşturma için ilgili bilginin bulunamaması,
 - yeni teknolojiler kullanılmaya başlandığında, eski sistemden yeni sisteme veri göçünün gerçekleştirilememesi,
 - üst veri eksikliğinden ötürü çeşitli destek ödeneklerinin sağlanamaması,
 - bir projede gerekli olan çoklu ortamlı belgelerin sürdürebilir dosya formatlarında olmadıklarından dolayı bilginin yeni dosya formatlarına transfer edilmesi için harcama yapılması,
 - Çok önce yaşanmış ciddi bir virüs salgını tekrar ortaya çıktığında, konu ile ilgili belgelerin bulunamaması ya da veri tabanında bulunan bilgilerin görüntülenememesi vb.”
- (*Understanding Digital Continuity*, 2017, s. 5; Özdemir ve Cengiz, 2019, s. 276).

4.2.2. Dijital Sürekliliğin Sağlanması ve Yönetilmesi

Dijital sürekliliğin sağlanması ve yönetilmesi bilgi varlıklarına bağlıdır. Bilgi varlığı; “varlığın verimli bir şekilde anlaşılması, paylaşılabilmesi, korunması ve kullanılabilmesi için tek bir birim olarak tanımlanan ve yönetilen bilgi yığınıdır” (Özdemir ve Cengiz, 2019, s. 276; *What is an information asset?* , 2017). Kurumlar ister büyük ister küçük olsun sahip oldukları bilgileri anlamadıysa bilgi varlığını tam olarak koruyamaz ve kullanamazlar. Var olan her bir dosyayı, veri tabanını ya da herhangi bir bilgi kırıntısını bilgi varlığı olarak kabul etmek de doğru değildir. Örneğin kurumun sahip olduğu EBYS’deki tüm bilgileri bir bilgi varlığı olarak kabul edilebilir ancak içeriği yönetmek zor olabilir. Yine kurumun tüm finansal verileri tek bir bilgi kaynağı olarak kabul edilebilir. Küçük bir kurumun sahip olduğu veri tabanı bir bilgi varlığı iken büyük bir kurumda bu veri tabanları daha fazla bilgi varlığı olarak kabul edilebilir. Kurumsal faaliyetlere göre bilgi varlıkları gruplanıp, yönetilmelidir (*What is an information asset?*, 2017).

Hem şimdi hem de gelecekte kurumsal ihtiyaçlarını karşılamada bilgi varlıklarının teknolojik ve bilgi yönetimi süreçlerinin yönetimi kurumun bilgilerinin dijital sürekliliğini korumaya yardımcı olur. Zamanı geldiğinde kurum hangi bilgilere sahip olduğunu, ne hakkında olduğunu, nerede olduğunu, gelecekte nasıl kullanmak istediğini biliyor olacaktır. Kurumun sahip olduğu teknoloji ve bilgi yönetim süreci değişen gereksinimlerle başa çıkabilmeyi ve bilgiyi kullanabilmeyi sağlayacaktır. Dijital sürekliliğin sağlanması bilgi varlıkları, teknik hizmet ve ortam ve kurumsal ihtiyaçlarla bağlantılıdır. Dijital süreklilik aynı zamanda bir risk yönetimidir. Değişimi yönetmek dijital sürekliliği yönetmektir. Değişiklikler etkili bir şekilde yönetilmezse, kullanılamayacak bilgi varlıkları ve teknoloji meydana gelir. Bu durum en iyi ihtimalle verimsizlik, en kötü ihtimalle ise ihtiyaç duyulan bilgilerin kaybolmasına neden olacaktır. Düşünülmesi gereken sadece değişiklikler ve onlara uyum sağlamak değil aynı zamanda gelecekteki değişim için hazırlıksız olma riskidir. Örneğin gelecek beş yıl içinde bilgileri nasıl kullanmak isteyeceğini kurum düşünmelidir. Kurumun bu zaman içinde ihtiyaçları değişecek mi? Donanım ve yazılımın yaşam döngüsü planlandı mı? Bu ve benzer konularla ilgili planlamalar yapıldı mı? Personelin bu konuda bilgileri ne durumda? Bu ve benzer sorulara cevap verebilmek, hazırlıklı olmak bir risk yönetimi sürecini doğurur (*What is an information asset?*, 2017, s. 10).

İngiliz Milli Arşivi'nin kurumlarda dijital sürekliliğin yönetilmesi için oluşturduğu model dört aşamadan oluşmaktadır:



Şekil 7. Dijital süreklilik modeli (Managing Digital Continuity, 2017, s. 6)

Birinci aşama olan eylem planı sürecinde, kurum, hedeflerini, kiminle çalışması gerektiğini ve kurum genelinde dijital sürekliliği nasıl yönetmesi gerektiğini belirler ve farklı disiplinlerden bir çalışma ekibi oluşturur. Ekibin içinde bilgi yönetimi, hukuk, insan kaynakları, bilişim, stratejik geliştirme ve ilgili alanlardan disiplinler olabilir. Ekibin düzgün bir süreç yönetebilmesi için başına üst yönetimden kıdemli risk sorumlusu atanır. Tüm süreçlerin sağlıklı ilerlemesi risk değerlendirmelerinin planlı yapılmasına bağlıdır. İkinci aşama dijital süreklilik gereksinimlerinin tanımlanmasıdır. Bu aşama bilgi varlıklarını iyi tanımak, varlıkların kurumsal değerini bilmek, nasıl kullanıldıklarını zamanla kullanımının nasıl değişeceğini bilmek ile ilgilidir. Üçüncü aşama dijital süreklilik risklerini değerlendirme ve yönetmedir. Bu aşama dijital sürekliliği kaybetmeme adına bilgi varlıklarının risk yönetimi ile ilgilidir. Kuruma uygun yönetim ve risk yönetimi yapı planlarını oluşturmak, ne tür tedbirler alınacağını belirlemek, bu iş için bir ekip oluşturmak ve ekipte kimlerin olacağını belirlemek ile ilgilidir. Dördüncü ve son aşama dijital sürekliliğin sağlanması aşamasıdır. Bu aşama kurumun bilgilerinin kullanılabilirliğini korumak adına süreçler ve stratejiler oluşturmak ile ilgilidir. Kurumun dijital süreklilik süreçleri stratejik planlarda ve politikalarda yer almalı ve bu sürecin bilgi

yönetimi ile bağlantılı olduğu benimsenmeli ve bu konuda gerekli eğitici, yönlendirici adımlar atılmalıdır (*Managing Digital Continuity*, 2017, s. 6-17).

4.2.3. Bilgi Varlıkları

Bilgi varlığı; “varlığın verimli bir şekilde anlaşılması, paylaşılabilmesi, korunması ve kullanılabilmesi için tek bir birim olarak tanımlanan ve yönetilen bilgi yığıdır” (Özdemir ve Cengiz, 2019, s. 276; *What is an information asset?* , 2017, s. 1).

Bir şeyin bilgi varlığı olup olmadığını anlamak için aşağıdaki sorulara cevap vermesi beklenir.

- “Bilginin kuruma bir değeri var mıdır?
- Bilgi ne kadar yararlı?
- Bilgiyi yeniden edinmenin kuruma bir maliyeti var mıdır?
- İstek üzerine bilgi yeniden üretilemezse kuruma yasal, itibarsal ve finansal olarak yansımaları olur mu?
- Bilgiye kolayca erişilemezse bu durumun operasyonel verimlilik üzerinde etkisi olur mu?
- Bilgiye sahip olamamanın sonuçları olur mu?
- Bilgiyle ilişkili bir risk var mı?
- Bilgiyi kaybetme riski var mı?
- Bilginin doğru olmama riski var mı?
- Birisinin onu kurcalamaya çalışması riskli bir durum mu?
- Bilgi gurubunun sahip olduğu belirli bir içerik var mı?
- Bilgilerin tamamı birbirleri ile bağlam açısından ilişkili mi?
- Bilgi yönetilebilir bir yaşam döngüsüne sahip mi?
- Bilgiler aynı kurallara göre mi imha edilecek? (*What is an information asset?*, 2017, s. 1).

Kurumlarda bilginin varlık olarak kabul edilmesi kurumsal bilgi süreçlerinin de düzgün işlemesine katkı sağlayacaktır. Bu sürecin düzgün işleyebilmesinin bir başka ayağı da her kurumun bir belge yönetim politikasına sahip olması gerekliliğidir.

Kurumların sahip oldukları bilgiyi öncelikle bir varlık olarak görmeleri bu sürecin düzgün ilerlemesi için önemlidir. Aksi taktirde o kurumdaki bilginin sürekliliğinin sağlanması mümkün olamayacaktır. Bu sebeple de kurumlarda bilgi varlık

envanterlerinin olması gerekir. Bilgi varlık envanterleri sayesinde eğer kurumda bir bilgi güvenlik olayı meydana gelirse, bilgilerin bütünlüğü, erişilebilirliği ve gizliliği korunacaktır (Özdemir, 2017, s. 49). Özellikle dijital çağda kurumlarda karşılaşılan dijital zorluklara karşı bilgi varlıklarının belirlenmesi ve düzgün şekilde yönetilmesinin önemi dikkat çekmektedir (Aydın ve Saydam, 2019, s. 4).

ISO 27000 bir standartlar serisidir. İçerisinde ISO 27001, 27002, 27003 gibi birden fazla standart içerir. ISO 27001, Bilgi Güvenliği Yönetim Sistemi Standardı olarak geçmektedir. Bilgi Güvenliği Yönetim Sistemini kurum ve kuruluşlarda uygulamak için aşağıdaki 11 adıma uymak gerekir.

- Bilgi güvenliği politikası: Kurum ve kuruluşlarda üst yönetimin onayladığı bir bilgi güvenliği politikası olmalıdır.
- Bilgi güvenliği organizasyonu: Kurum içindeki bilgilere erişimin güvenliğinin sağlanması gerekir.
- Bilgi varlıklarının yönetimi: Kurum, kuruluş şirket vb. bilgi varlıklarının envanterinin oluşturulması gerekmektedir.
- İnsan kaynakları güvenliği: Personelin görev ve sorumlulukları belirlenmedi ve ona uygun hareket etmesi sağlanmalıdır.
- Fiziksel ve çevresel güvenlik: Her türlü fiziksel ve çevresel riske karşı önlemlerin alınması gereklidir.
- İletişim ve işletme yönetimi: Bilgi işlem süreci ile ilgili yazılı prosedürler olmalı ve uygulanmalıdır.
- Erişim kontrolü: Erişim denetimi politikası oluşturulmalı ve politikada herkesin erişim için sahip olacağı haklar açıkça belirtilmelidir.
- Bilgi sistemlerinin geliştirilmesi: Bilgi sistemleri geliştirilmeli, güncellenmeli ve güvenlik riskleri belirlenmelidir.
- Olayların yönetimi: Bilgi güvenliği süreçlerinde gerçekleşen tüm olaylar raporlanmalıdır.
- İş sürekliliği yönetimi: İş sürekliliği ile ilgili süreçlerin belirlenmesi ve geliştirilmesi sayesinde kurumun bilgi varlıkları ve iş süreçleri risklerine karşı tedbirli olunması sağlanmış olur.
- Uygunluk: Kurumdaki bilgi sisteminin tüm yasal gereksinim ve süreçleri açık şekilde belirlenmeli ve belgelenmelidir (Şen, 2013).

Tüm bunların yanında kurumun bilgi yönetim süreçlerinin düzgün işlemesi, sürdürülebilirliğinin olması için öncelikle sahip olduğu bilgi varlıklarının farkında olması gerekmektedir. Bilgi varlıklarının envanteri oluşturma, oluşabilecek riskleri belirleme ve bilgi varlıklarını koruma odaklı çalışmalar yapılması kurumlar için hayati önem taşımaktadır. ISO 27001 standardı kuralları gereği de birçok kurum bilgi varlığı envanteri çıkarma sürecini başlatıp gerekli işlemleri yapmaktadır. Bu süreçlerin daha iyi anlaşılması adına aşağıda örnek bir bilgi varlık envanteri tablosu oluşturulmuştur.

Varlık Numarası	Varlık Adı	Lokasyon/ Dosya Yolu	Varlık Sahibi/Sorumlu	Hacim	Kişisel Veri	Erişim	Paylaşım	Format	Saklama süresi	Riskler	Anahtar Kelimeler
1	Kütüphane kullanıcı bilgileri	Yordam Sistemi http://katalog.marmara.edu.tr/yordambt/yordam.php	Kütüphane personeli	600 bin dosya	Kişisel veri	Sorumlu personel	Sorumlu personel	Pdf, jpg, xlm	Sürelili 5 yıl	Hassas bilgi	Var
2	Personel maaş bilgileri	Personel Yönetim Sistemi http://bys.marmara.edu.tr/v2/	Rektörlük Personel İşleri Birimi	80 bin dosya	Kişisel veri	Sorumlu personel	Sorumlu personel	Pdf, jpg, xlm	Sürelili 10 yıl	Hassas bilgi	Var
3	Proje ihale dosyası	EBYS http://bilgi.islem.marmara.edu.tr/ebys.php	Bilgi İşlem Daire Başkanlığı	120 bin dosya	Hassas veri	Sorumlu personel	Sorumlu personel	Pdf, jpg, xlm	Sürelili 10 yıl	Hassas bilgi	Var

Şekil 8. Varlık envanteri örneği

Yukarıdaki bilgi varlık kaydı İngiliz Milli Arşivi ve ISO 27001 bilgi varlık kaydı örnekleri baz alınarak oluşturulmuştur. Bir kurum, kuruluş, şirket bünyesinde var olan her türlü fiziksel ve dijital varlıkların envanterini tutmalıdır. Şekil 8’deki başlıkları inceleyecek olursak, varlık adı kurumun bünyesinde var olan varlığın ismini ifade eder. Konum bilgisi, mevcut varlığın kurum bünyesinde bir bilgi sisteminde mi, fiziksel bir alanda mı, elektronik bir bağlantı içinde mi olduğunu gösteren uzantıdır. Varlık sahibi, varlıktan sorumlu birimi, kişileri; hacim bilgisi varlığın boyutunu, kişisel veri olup olmadığı, varlığın hassas bir veri olup olmadığını; erişim, varlığın kimler tarafından erişilebilir olduğunu; paylaşım kısmında kimlerin yetkili olduğu; saklama süresi varlığın

kurumda ne kadar tutulacağını; riskler kısmında varlık için bulunan bir riskin olup olmadığı ve anahtar kelimeler varlığın bir anahtar kelimeye sahip olup olmadığını belirtmektedir. Böylelikle kurumda varlıklar ve varlıklara ait bilgiler üst veriler tanımlanarak daha yönetebilir bir duruma gelecektir. Varlık envanterinin iki aşaması bulunmaktadır. Öncelikle varlıklar belirleme sonrasında da varlıkların değerini belirleme kısmıdır ve bu sayede risk analizi gerçekleştirilebilmektedir. Her bir bilgi varlığı için riskler belirlenip, risk puanlamaları verilir. Risklerin derecesi yüksek, orta, düşük olarak ve gizlilik, bütünlük ve erişilebilirlik ilkeleri temel alınarak derecelendirilir ve çıkan puanlar toplanıp her bilgi varlığı için toplam risk değeri bulunur. İncelemeler sonucu görülmüştür ki; birçok kurum, kuruluş, şirket ISO 27001 standardı gereği bilgi varlık envanteri oluşturmakta, risk değerlendirmeleri yapmakta ve yetkili birimlerce denetimlerden geçmektedirler. Yine bu kapsamda birçok kuruma bilgi güvenliği sertifikası zorunlu hale getirilmiştir. Kanunen yaptırımlar olduğunda ve denetimler yapıldığında görmekteyiz ki kurumlar bu yaptırımlara uymaktadırlar.

4.3. Belge Yönetimi Süreçlerinde Politikalar ve Önemi

Politika, bir kurumun elindeki en önemli güçlerden biridir. Bir kurum ya da kuruluşun iş süreçleri, bilgi ve belge işleyişleri ve tüm işlemlerin sürekliliğini sağlama politikalarıyla var olabilmektedir. Politikaların kurum ve kuruluşlarda önemi oldukça büyüktür. Politikalar sayesinde, iş süreçleri aksamaz, belirli standart ve istikrarla devam eder. Politikaların eksikliği ise süreçlerin düzgün ilerlememesine yol açmaktadır. Man'e (2010) göre politika, kuruluşun amaç ve faaliyetlerinin analizi, belirlenmesi, hangi belgelerin oluşturulması ve tutulması gerektiği ve belgelerin ne kadar uzun süre saklanması gerektiğinin belirlenmesi unsurlarını içermelidir.

Konu bağlamında literatür incelendiğinde bilgi yönetimi politikaları ve belge yönetimi politikalarının karıştırıldığını ve bazen birbirleri yerine geçtiğini görmekteyiz. Türkiye örneğinden yola çıktığımızda kurumlarda belge yönetimi politikası yerine daha çok bilgi yönetimi politikaları bulunmaktadır ve bu iki unsur birbirleri ile karıştırılmaktadır. Bilgi yönetimi politikası içerik yönetimi ele alan daha kurumsal ve stratejik bir yapıya sahiptir. Belge yönetimi politikası ise daha çok arşivsel süreçlerle ilgilenmektedir.

Ulusal ve uluslararası literatür incelendiğinde, bilgi bilim ve arşivcilik alanında genel anlamda politika oluşturma ile ilgili sorunların var olduğuna ulaşılmıştır. Üniversite, bakanlık, belediye gibi her organizasyonun dijital sürekliliğin de sağlanması

adına bilgi yönetimi politikası ve belge yönetimi politikasına sahip olması son derece önemlidir. Aslında dijital belgelerin tüm süreçleri ile ilgili politikaların, yasal dayanakların olması son derece önemli görülmektedir. Bu durum belgelerin oluşturulma sürecinden başlayarak milli arşive transfer sürecine kadar olan tüm alanlarda geçerlidir. Bir devletin, milli arşiv kanunu ve bu kapsamda oluşturulmuş süreçlerle ilgili politikaları, yönetmelikleri kısaca yasal dayanaklarının olması çok büyük bir gerekliliktir. Bu koşulların sağlanamadığı zamanlarda ise kurumlarda işleyen belge yönetim süreçleri aksamaya ve eksiliklerle devam etmeye mecburdur.

TSE 13298'e göre "Arşiv kurumları ve kurumsal arşivler öncelikle ne tür malzemeleri transfer edeceklerini ve hangi hizmet koşullarında kullanıma açacaklarını belirten bir kurum politikası geliştirmelidir. 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" (2015, s. 42). Burada bahsi geçen kurum politikaları belge yönetim politikalarını da içermektedir.

Belge yönetiminin en önemli bileşeni, sorumlulukları belirli kişilere atamaktır. Belirli bir politikayı kimin resmi olarak onayladığını izlemek basittir, ancak politikanın çeşitli yönlerinden kimin uzun vadeli sorumluluğa sahip olduğunu belirlemek daha önemlidir. Bir kurumdaki çalışan kişiler zamanla değiştiği için, oluşturulan politikalarda isimler değil roller belirlemelidir. Kurumların bir politikayı uygulama şekli zamanla değişecektir, çünkü hem teknoloji hem de iş ihtiyaçları sürekli olarak gelişmektedir, ancak politikanın kendisi nispeten istikrarlıdır (Garland, 2019). Belge yönetimi politikası bir kurumda belgelerin etkin yönetilebilmesi için mihenk taşı olarak kabul edilir. Ayrıca belge yönetimi politikası belgelerin yönetilmesinde rol ve sorumlulukları belirler (Ipinge ve Nengomasha, 2018, s. 384).

Çiçek, kurumlarda yürütülen belge süreçlerine dair bir dokümanın, yönergenin bulunması ile bir belge yönetim politikasının bulunmasının aynı anlama gelmediğini, belge yönetimi politikasının olmayışının aynı zamanda kurumda belgeler için etkili bir dokümanın bulunmaması anlamına geldiğini belirtmiştir (2020, s. 394). Tüm kurum ve kuruluşlar, belge yönetimi için resmi olarak kabul edilmiş bir politikaya sahip olmalıdır. Politikanın amacı, gerekli olduğu sürece iş işlevlerini ve faaliyetlerini destekleyebilen gerçek, güvenilir ve kullanılabilir belgelerin oluşturulması ve yönetimi olmalıdır. Politika, en yüksek karar alma düzeyinde benimsenmeli ve onaylanmalı ve kuruluş genelinde ilan edilmelidir (Shepherd and Yeo, 2003). Politikalar kurum tarafından

zorunlu olarak uygulanması ve personel tarafından da uyulması gereken yasal dayanaklardır. Bir kurumda politikanın eksik oluşu süreçlerin standartlaşmadan uzak olarak yürütülmesi anlamına gelir. Bu da uygulamada işleyişin aksamasına sebep olacaktır. Ayrıca belge yönetim politikası ile kurumsallaşma da sağlanır (Solhan, 2015, s. 51).

Kurumlarda belge yönetim politikasının varlığı ve uygulanması EBYS'yi ve personelin iş süreçlerini olumlu yönde etkileyen unsurların başında gelmektedir (Yalçınkaya ve Saydam, 2018). Kurumlarda belge yönetimi politikasının var olması kurumun hizmetlerini düzgün bir biçimde yürütebilmesi için başlı başına yeterli bir unsur değildir. Bu unsurun tamamlanmasında personelin çok önemli bir rolü bulunmaktadır. İlgili personel tüm süreçlere hâkim belge yöneticisi olmalıdır. Bu kapsamda belge yöneticilerinin görev ve sorumluluklarının açıklandığı bir yasal dayanak oldukça önemli bir yere sahiptir. Konu kapsamında 2020 yılında ulusal meslek standartları yayımlanmıştır. Yayımlanan ulusal meslek standardında meslek tanımlamaları ve meslek profilleri belirlenmiştir. Meslek profilleri içerisinde belge yöneticisinin tanımı, görevleri ve bu görevlere bağlı olarak başarımlar ölçütleri, mesleki bilgi ve uygulama becerileri titizlikle belirlenmiştir (Ulusal Meslek Standartlarına Dair Tebliğ, 2020).

Belge yönetimi tarihi, mali, idari ve hukuki değere sahip kurumsal belgelerin tanımlanmasını, saklanması ve korunmasını ve gerekli olmayan belgelerin belirlenen politikaya uygun olarak ayıklanmasını sağlar. Belge yönetimi politikası, kurum ve kuruluşlarda mevcut belgelerin daha etkin yönetimini gerçekleştirir. Aynı zamanda bir belge yönetimi politikasının olması kurumsal hesap verebilirlik ve bilgiye zamanında erişim sağlar. Politikanın varlığı, alınacak eylemleri ve kararları kolaylaştırmak için bir kılavuz işlevi görür. Bu bağlamda elektronik belge yönetimi faaliyetleri, organizasyonu yönlendirmek ve uygulanan işlevlerin etkinliğini tespit etmek için açık, kapsamlı, anlaşılır bir politika ile yönlendirilmelidir.

4.3.1. Belge Yönetimi Politika Türleri ve Başlıkları

Belge yönetimi politikası bir kurumun işleyişinin sağlam temeller üzerinde oturmasına destek olur. Tüm kurum ve kuruluşlar, belge yönetimi için resmî olarak kabul edilmiş bir politikaya sahip olmalıdır. Türkiye'deki kamu kurum ve kuruluşlarında bu konudaki eksiklik somut deliller üzerine inşa etmeye çalışılmıştır. Bu kapsamda otorite kabul edilen İngiltere'deki bakanlıkların belge yönetim politikaları incelenerek örnek bir

belge yönetimi politikasının içerik yapısı oluşturulmaya çalışılmıştır. Bunların yanı sıra, belge yönetimi politikalarının kurumsal şeffaflık ve etkili yönetim açısından önemi vurgulanmaya çalışılarak, İngiltere’deki kamu kurumlarının belge yönetimi politikaları örneğinde, Türkiye’de nasıl ve neden uygulanması gerektiği ele alınıp literatüre katkı sağlanması amaçlanmıştır. Türkiye’deki bakanlıklar, üniversiteler ve belediyelerin web sayfaları taranmış ve incelenmiştir. Öncelikle incelemeler sırasında Türkiye’de belge yönetimi politikasından çok kurumlarda bilgi yönetimi politikası ve bilgi güvenliği politikası ya da dokümanlarına erişilmiştir. Bu sonuca erişilmesinin sebebinin kurumların ISO 27001 kapsamında bilgi güvenliği denetimlerine tabi tutulmasından kaynaklı olduğu düşünülmektedir.

Türkiye’de üniversiteler içerisinde Ankara Üniversitesi’nin “Belge Yönetimi ve Arşiv Sistemi Politikası” isimli bir belge yönetim politikasına sahip olduğu görülmektedir. Politika metni on bölümden ve üç sayfadan oluşmaktadır. Politika içeriğinde giriş, kapsam, belge yönetimi ve arşiv sisteminin amaçları, kurumsal sorumluluklar, personel, önemli belgeler, eğitim başlıklarından oluşmaktadır. Başlık içeriklerinde kısaca genel açıklamalar yapılmıştır. İnceleme sonunda politikanın ayrıntılı bir metne dayanmadığı görülmektedir (Ankara Üniversitesi Belge Yönetimi ve Arşiv Sistemi, 2009).

İncelenen bakanlıkların, belediyelerin ve üniversitelerin büyük çoğunluğunun bir belge yönetimi politikasına sahip olmadığı sonucuna varılmıştır. Çalışmada incelenen ve bulunan sonuçlar yayımlanan belge yönetimi politikalarına aittir. Kurumların yayımlanmayan, kendi içlerinde yürüttükleri politikaları olabileceğinin az da olsa göz önünde bulundurulması gerekmektedir. Bu değerlendirme, anket sürecinde bilgi profesyonellerinden alınan cevaplardan elde edilmiştir. Bunun üzerine arşivcilik alanında öncü çalışmaları olan İngiliz Milli Arşivi’nin ve İngiliz kamu kurum ve kuruluşlarının belge yönetimi politikaları incelenmiştir. İngiliz kamu belge yönetimi politikası uygulamalarının yaygın olması nedeniyle, çalışma kapsamında buradaki kamu kurum ve kuruluşlarına yer verilmiştir. Bu uygulamaların yaygın olma sebebi 1950’li yıllardan beri yürürlükte olan Arşivcilik Kanunu (Public Records Act) ve 2000’li yıllarda yasallaşan Bilgi Edinme Özgürlüğü Kanunu’nun (Freedom of Information Act) kurumlara iyi belge yönetimi uygulamalarını zorunlu kılmasıdır. Bir kurumun bir belge yönetimi politikasına sahip olması, belge yönetimin etkin bir şekilde gerçekleştirildiğinin göstergesi olabilir.

Araştırma kapsamında İngiltere’de belge yönetimi politikasına sahip olan kurumların “İngiliz Milli Arşivi (The National Archives)²⁴, İngiltere Adalet Bakanlığı (Ministry of Justice)²⁵, İngiltere Galler Hükümeti (The Welsh Government)²⁶, Metropolitan Polis Teşkilatı (Metropolitan Police Service)²⁷, İngiltere Savunma Bakanlığı (Ministry of Defence)²⁸, İngiltere Ulaştırma Bakanlığı (Department for Transport)²⁹, İngiltere Çevre, Gıda ve Köy İşleri Bakanlığı (Department for Environment, Food and Rural Affairs)³⁰, İngiltere Çalışma ve Emeklilik Bakanlığı (Department for Work and Pensions)³¹, İngiltere Topluluklar ve Yerel Yönetimler Bakanlığı (Department for Communities and Local Government)³², Sağlık ve Sosyal Güvenlik Bakanlığı (Department of Health and Social Care)³³, Başsavcılık Ofisi (Attorney General's Office)³⁴, Ulusal Ölçüm ve Düzenleme Ofisi (National Measurement and Regulation Office)³⁵, Şirketler Sicil Ofisi (Companies House)³⁶” politikaları incelenmiştir.

²⁴Records management policy, İngiliz Milli Arşivi (The National Archives), <https://cdn.nationalarchives.gov.uk/documents/information-management/rm-code-guide3.pdf>

²⁵Records information management policy, İngiltere Adalet Bakanlığı (Ministry of Justice), <https://www.gov.uk/government/publications/records-information-management-policy-psi-042018-pi-022018>

²⁶Welsh Government Information Management and Governance Policy, İngiltere Galler Hükümeti (The Welsh Government), <https://gov.wales/sites/default/files/publications/2018-10/information-management-and-governance-policy.pdf>

²⁷Records management policy, Metropolitan Polis Teşkilatı (Metropolitan Police Service), <https://www.met.police.uk/SysSiteAssets/foi-media/metropolitan-police/policies/strategy--governance---mps-records-management-policy---compliance--guidance>

²⁸Defence Records Management Policy and Procedures, İngiltere Savunma Bakanlığı (Ministry of Defence), https://data.parliament.uk/DepositedPapers/Files/DEP2014-1256/JSP_441_Version_4.3-FINAL-U%5B1%5D.pdf

²⁹Records Management Policy, İngiltere Ulaştırma Bakanlığı (Department for Transport), <https://www.transportation.gov/digitalstrategy/policyarchive/Records-Management>

³⁰Information Management Assessment, İngiltere Çevre, Gıda ve Köy İşleri Bakanlığı (Department for Environment, Food and Rural Affairs), <https://cdn.nationalarchives.gov.uk/documents/information-management/defra-ima-report.pdf>

³¹Information Management Policy, İngiltere Çalışma ve Emeklilik Bakanlığı (Department for Work and Pensions), <https://www.gov.uk/government/publications/dwp-information-management-policies/dwp-information-management-policy>

³²MHCLG: records and information management policy, İngiltere Topluluklar ve Yerel Yönetimler Bakanlığı (Department for Communities and Local Government), <https://www.gov.uk/government/publications/mhclg-records-and-information-management-policy>

³³Records management: code of practice for health and social care, Sağlık ve Sosyal Güvenlik Bakanlığı (Department of Health and Social Care), <https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care>

³⁴Records Management Policy, Başsavcılık Ofisi (Attorney General's Office), <https://www.gov.uk/government/publications/records-management-policy>

³⁵Electronic records management policy, Ulusal Ölçüm ve Düzenleme Ofisi (National Measurement and Regulation Office), <https://www.gov.uk/government/publications/electronic-records-management-policy>

³⁶Records Management Policy, Şirketler Sicil Ofisi (Companies House), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/317573/Companies_House_Records_Management_Policy_-_Online_version.pdf

Belge yönetimi politikaları içerik incelemeleri sonucu türlerine göre temel içeriğe sahip belge yönetimi politikaları ve ayrıntılı içeriğe sahip belge yönetimi politikaları olmak üzere iki gruba ayrılmıştır. İncelenen belge yönetim politikaları içerik ve başlık olarak derlenerek iki gruba ayrılmıştır. Aşağıda belge yönetimi politikalarının türlerine göre başlıkları ve açıklamaları tablo ile gösterilmiştir.

Tablo 3. Temel içeriğe sahip belge yönetimi politika başlıkları

Temel İçeriğe Sahip Belge Yönetimi Politika Başlıkları	
1.	Politika başlığı
2.	Giriş
3.	Kapsam
4.	Belge yönetimi politikasının amacı
5.	Saklama
6.	İmha
7.	Koruma
8.	Denetim ve uygunluk

İncelenen politikalardan temel içeriğe sahip belge yönetimi politikalarının başlıkları düzenlenip Tablo 3'te gösterilmiştir. Tablo 3'te belirtilen temel içeriğe sahip belge yönetimi politikası başlık içerikleri şu şekildedir: Politika başlığı kurumun oluşturduğu politikaya verilen ismi, giriş kısmı politikanın içeriği hakkında bilgiyi, kapsam kısmı politikanın kimleri ve neleri kapsadığını, belge yönetimi politikasının amacı başlığı kurum genelinde politikanın neleri amaçladığı, saklama başlığı hangi belgelerin nasıl, nerede, ne kadar saklanacağı bilgisini, imha başlığı hangi belgelerin neden, nasıl ve ne zaman imha edilmesi gerektiği bilgisini, koruma başlığı belgelerin hangi ortamda, nasıl, hangi yöntemlerle korunması gerektiği bilgisini, denetim ve uygunluk başlığı ise politikanın yasal mevzuatlara uygunluk ve denetim bilgilerini ifade etmektedir. Tablo 3'teki belge yönetimi politika başlıkları, Tablo 4 ile karşılaştırıldığında daha yüzeysel kalmaktadır. Belge yönetim politikasında olması gereken roller ve sorumluluklar, elektronik belge yönetim sistemi ve süreç, dijital belgeler için saklama, ayıklama, üst veri standardına uygunluk, koruma, hassas belgelerin süreçleri, eğitim gibi birçok unsurun Tablo 3 içerisinde yer almadığı görülmektedir. Temel içeriğe sahip belge yönetim politikalarının genel anlamda dijital belgeler yerine fiziksel belgeler için yapılandırılmış olduğu görülmektedir.

Görüldüğü üzere temel içeriğe sahip politikalarda, başlıklarında çok fazla ayrıntıya yer verilmeden, temel başlıklar halinde içerik sunulmuştur.

Tablo 4. Ayrıntılı içeriğe sahip belge yönetimi politika başlıkları

Ayrıntılı İçeriğe Sahip Belge Yönetimi Politika Başlıkları	
1.	Politika başlığı
2.	Giriş
3.	Kapsam
4.	Belge yönetimi politikasının amacı ve kapsamı
5.	Temel mevzuat
6.	Terimler ve tanımlar
7.	Belge yönetimi nedir?
8.	Belge yönetimi neden gereklidir?
9.	Roller ve sorumluluklar
10.	Kamu belgelerinin tanımlanması
11.	Arşive uygun materyal türünün belirlenmesi
12.	Dosya planı
13.	Elektronik belgelere erişim
14.	Elektronik belge yönetim sistemi ve süreç
15.	Fiziksel ve dijital belgeler için saklama politikası
16.	Ayıklama politikası
17.	İmha politikası
18.	Fiziksel ve dijital belgelerin milli arşive transferi
19.	Üst veri standardına uygunluk
20.	Hesap verebilirlik ve şeffaflık
21.	Bütünlük
22.	Kullanılabilirlik
23.	Koruma
24.	Hassas belgelerin süreçleri
25.	Eğitim ve farkındalık
26.	Yönetim ve gözden geçirme
27.	Ortak oluşumlar, birimler ve sorumluluklar

Tablo 4'te incelenen ayrıntılı içeriğe sahip belge yönetimi politikalarının başlıkları derlenip bir tabloda toplanmıştır. Tablo 4'teki ayrıntılı içeriğe sahip belge yönetimi politikasının başlıklarının içerik değerlendirmesi aşağıda yer almaktadır.

Öncelikle ayrıntılı bir belge yönetimi politikası politika ismi ile başlamaktadır. Belge yönetimi politikasına bir giriş yapıldıktan sonra kapsam kısmında politikanın hangi belge türlerini, formatlarını içerdiği, belge yönetimi politikasının amacı ve kapsamı belirtilmektedir. Belge yönetiminin neyi ifade ettiği ve neden gerekli olduğu ve kurumlarda belirlenen ekibin rol ve sorumluluklarının neler olduğuna dair kısımlar bulunmaktadır. Kurumlarda belgelerin tanımlanması, arşive uygun materyalin

değerlendirme süreçleri, dosya planlarının oluşturulması, fiziksel ve dijital belgelere erişim süreçleri, elektronik belge yönetim sistemi ve süreçleri belge yönetimi politikasının içerdiği diğer kısımlardandır. Bunların yanında tüm belgeler için saklama, ayıklama, imha kurallarının belirlenmesi, belgelerin transfer süreçleri, yapılacak işlemler, gerekli üst veri standartlarının belirlenmesi ve bunlara uygunluk, süreç içerisinde belgelerde hesap verebilirlik, şeffaflık, bütünlük, kullanılabilirlik ve koruma ilkelerine uygunluk ile ilgili kısımların belirlenmesi ayrıntılı içeriğe sahip belge yönetimi politikasında var olan unsurlardır. Hassas içeriğe sahip belgelerin nasıl yönetileceği, kurum arşivine transferi ve tüm belgelerin milli arşive transfer süreçleri diğer unsurlardandır. Politikada, belge yönetimi ve politika kapsamında personele eğitim ve farkındalık çalışmaları hakkında bilgiler bulunmaktadır. Son olarak kurum içi ve dışı birimlerin konu kapsamında sorumlulukları ve politikanın sürekliliğinin sağlanabilmesi adına yönetim ve gözden geçirme süreçleri politika belgesinde yer alan unsurlardır. Ayrıntılı içeriğe sahip belge yönetim politika başlıkları incelendiğinde, tablo 3'te temel içeriğe sahip politika başlıklarına göre personele daha yol gösterici özellikleri bulunan politikalar olarak görülmektedir. Bu politikaların bir belgenin doğuşundan milli arşive transferine kadar olan sürece ait bilgileri daha ayrıntılı bir biçimde içerisinde barındırması sebebiyle hem personele hem de kuruma büyük katkılar sağlayacağı düşünülmektedir. Belge yönetimi politikaları ile ilgili yapılan kapsamlı bir çalışmada ilgili konu ayrıntılı bir şekilde çalışılmıştır. Çalışmada Türkiye'deki kamu kurum ve kuruluşlarının belge yönetimi politikaları hakkında mevcut durumu ortaya çıkarılmış, aynı zamanda otorite kabul edilen kurumların belge yönetim politikaları incelenerek örnek bir belge yönetimi politikasının içerik yapısı oluşturulmuştur (Cengiz Mater ve Özdemir Şahin, 2022).

4.4. Dijital Koruma (Digital Preservation)

Dijital koruma, dijital bir nesneyi gerektiği kadar uzun bir süre özgün bir biçimde ve kullanıcılar için erişilebilir halde tutma işlemidir (Brown, 2013, s. 3). Diğer bir tanıma bakacak olursak dijital koruma; dijital materyallere erişimi sürdürmek için medya başarısızlığı veya teknolojik değişim sınırlarının ötesinde gereken tüm eylemleri ifade eder (*What is digital preservation?*, 2008).

Dijital korumayı tüm yönleri ile yapmak için kurumların dijital koruma politikasına sahip olması gerekmektedir. Bu sayede gereksinimler ve uygulanacak adımlar belirlenir, çözümler geliştirilebilir.

Dijital korumanın kalbi dijital nesnedir. Dijital nesnelerin beş temel özelliği bulunmaktadır:

- Dijital nesneler donanıma ve yazılıma bağlıdır.
- Veri nesneleri anlamlaştırılarak bilgi nesnesi haline getirilir.
- Dijital korumanın son odağı bilgi nesnesidir.
- Birden çok veri nesnesi aynı bilgi nesnesini temsil edebilir.
- Aynı veri nesnesi birden fazla yerde bulunabilir (*Digital Preservation for Community Archives*, 2018).

Dijital çağda sürekli değişimin meydana getirdiği etkilerle birlikte kurumlar ve eylemleri evrim geçirmektedir. Toplum, interneti hızlı arama için eskiye oranla daha fazla kullanır hale gelmiştir. Google en yaygın kullanılan arama motorlarından biridir. Arama motorlarından her yıl aranan bilgi miktarı bir önceki yıla göre artış göstermektedir. Bu büyük değişiklikler sürecinde dijital materyali, nesneyi, bilgiyi korumak, saklamak önemli bir unsur haline gelmiştir. Ayrıca dijital koruma dijital dünyada karmaşık ve zordur.

TS 13298 standardına göre “Elektronik arşiv malzemelerinin uzun süreli veya sürekli korunması için seçilen dosya formatları ile arşiv malzemesinin saklandığı depolama ünitelerinin güncel teknolojilerle erişilebilir ve okunabilir olması” gerekmektedir (TS 13298, 2015, s. 44). Dosya formatları dijital belgeler için oldukça önemlidir. Teknolojiye bağlı olarak dosya formatları çok sık değişmektedir ve bu durumda öncesinde oluşturulan bazı dosyaların açılmaması, kullanılamaması anlamına gelmektedir. Bu bağlamda kurumlarda kullanılan dijital belge oluşturulan sistemlerde, eskiyen formatların otomatik olarak güncellenen formatlara çevrilmesi gerekmektedir. Bunun dışında ileride kurum arşivlerinden milli arşive dijital belgelerin transferi sırasında milli arşivin kabul ettiği geçerli belirli format yapıları olmalıdır. Bu bilgiler kurumlarla paylaşılmalı, bilgi yönetim sistemlerine entegre edilmeli ve kurumlar transfer edilecek format yapısı açısından hazır hale gelmelidir. Tüm bunların yanı sıra dijital belgelerin üst veri alanları da önemli bir konu teşkil etmektedir. Üst verilerle ilgili derinlemesine araştırma yapan Yalçınkaya doktora tezinde “Elektronik ortamda üretilen belgelerin teknolojik gelişmeler karşısında içerik ve bağlam açısından sürdürülebilir olması, standart bir üst veriye dayandırılması ile doğru orantılıdır. Standart üst veri belgelerin uzun süreli arşivlenmesinde belgeyi anlamlı kılar ve gelecek nesiller için bilgi ve belgelerin

kullanabilir, anlaşılabilir olmasını sağlar” şeklinde belirtmiştir (2014). Üst veri alanları belgelerin tanımlayıcı alanları olarak ifade edilebilir. Dijital belge üst veri arşive transfer sürecinde oldukça önem taşımaktadır. Belgelerin üst verileri, kullanılan bilgi sistemlerinde otomatik olarak tanımlanmalı ve bir standart sağlanmalıdır. Üst veri için bir kısıtlama olmamalı fakat tamamen belgeyi oluşturulan kişiye üst veri oluşturma sorumluluğu bırakılmamalıdır. İleride belgenin milli arşive transferi sırasında üst verilerde de bir standart sağlanmalıdır.

İngiliz Milli Arşivi ilk zamanlarda transfer işlemlerinde tüm formatları kabul etmeyip belirli format yapılarını kabul ediyordu. Belirlenen formatlar daha uzun süre dayanıyordu. Son dönemlerde ise faaliyetlerini bu alanda geliştirerek, ayırım yapmaksızın tüm formatları kabul etmektedirler. Format konusunda artık sınır koymayıp her türlü format kabul edilmekte ve riskler üzerinde çalışılmaktadır. Tüm formatlarda arşive daha az ve sık transfer yöntemini uygulamaktadırlar (Sheridan, 2021).

Koruma çalışmaları kapsamında bu zamana kadar dünyanın birçok yerinde yedekleme, yenileme, donanım ve yazılımın korunması, standartlara uyum, öykünme, göç, ortak sanal ağlar oluşturma gibi çözümlere gidilmiştir (MacKenzie, 2000; Smith, 1999, Çakmak, 2016, s. 29).

Dijital belgelerin korunması dünyanın her yerinde henüz çözümü net olmayan bir durumdur. Fakat bu zamana kadar yapılan çalışmalar göstermiştir ki eğer aşağıdaki unsurlara belge yaşam döngüsü sürecinde dikkat edilirse bu konuda yaşanacak sıkıntıların biraz da olsa önüne geçilmiş ve koruma sağlanmış olacaktır.

Dijital belgelerin uzun vadede korunması ve erişilebilirliğinin sağlanabilmesi için;

- Depolama ortamlarının sürekliliği sağlanmalı,
- Dijital süreklilik tüm kurum bünyesinde önemsenmeli ve uygulanmalı,
- Kurumda bilgi varlık envanteri oluşturulmalı ve sorumlular belirlenmeli,
- Konu kapsamında politika, strateji, rehber vb. oluşturulmalı,
- Bir risk planlaması yapılmalı,
- Uygun veri formatları kullanılmalı,
- Standartlara uygun üst veri oluşturulmalı,
- Konu kapsamında düzenli aralıklarla eğitimler verilmeli

ve benzeri unsurlara dikkat edilmelidir.

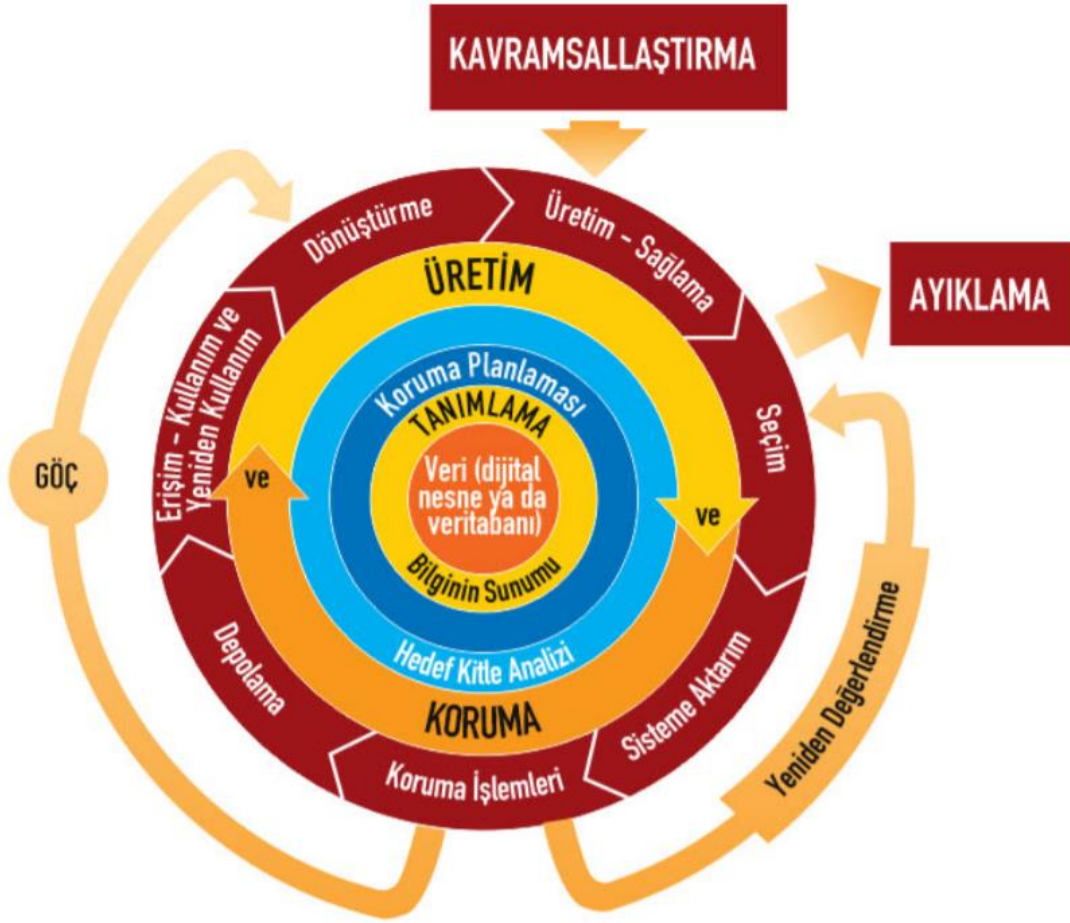
4.4.1. Dijital Korumanın Önemi

Öncelikle bilginin korunabilmesi için varlık olarak kabul edilmesi gerekir. Varlık olarak kabul edilen bilgi, dijital bilgi, her yerdedir. Dijital bilgi hayatımızın her alanında rol oynar. Dijital bilgi; hem iş hem sosyal hayatımızdaki iletişimde, alışveriş yapma, paramızı yönetme, sağlık hizmetlerine erişme ve kendimizi eğitme şeklimizde, kamu kurum ve kuruluşların çalışmalarını yürütmede oldukça önemli bir yere sahiptir. Bu nedenle, dijital bilgilere erişebilmek, kullanabilmek ve yeniden kullanabilmek çok önemlidir. Google ve Facebook gibi bazı şirketler için bilgi, ticaret yaptıkları ana maldır. Ancak dijital bilgiye erişme ve kullanma yeteneğini sürdürmek, daha geleneksel analog kaynaklara kıyasla çok farklı zorluklar sunar. Örneğin, el yazısı bir belgeniz, basılı bir kitabınız veya kâğıt üzerinde bir çiziminiz varsa, çevresel şartlar sağlandığı sürece, onu daha sonraki bir tarihte saklayabileceğiniz ve yeniden kullanabileceğiniz konusunda bir güvene sahip olacaksınız. Analog eşyalar genellikle oldukça sağlamdır ve hatta bir dolaba konulup unutulmanın zararsız ihmaline bile dayanır. Kötü bir küf salgını yaşamadığımız sürece, büyük olasılıkla yıllar sonra bir belgenin yazıldığı dili konuştuğunuz sürece okuyup kullanabileceksiniz. Ancak dijital bilgileri korurken karşılaşılan zorluklara karşı genellikle daha acil ve proaktif adımların atılmasını gerektirir. Yeniden yazılabilir bir CD'ye kaydedilmiş bir metin belgesini örnek olarak kullanalım. Bu belgeye erişebilmek ve bu belgeyi kullanabilmek için öncelikle CD sürücüsü olan bir bilgisayara sahip olmalıyız ve bu bilgisayarda, belgeyi açmanıza ve ekranda doğru şekilde görüntülemenize izin verecek uyumlu bir yazılıma ihtiyacımız var. Ancak bilgisayar donanımı sürekli olarak modası geçmiş ve yükseltip değiştirilme döngüsü içindedir. Bu örnekle ilgili olarak, kendi dizüstü bilgisayarınızda artık bir CD sürücüsü var mı? Ve yazılımın yeni sürümleri düzenli olarak yayımlanmaktadır. Eski dosyalarla uyumlu olduğuna güvenebilir miyiz? Depolama ortamının kendisi şaşırtıcı derecede kırılgandır ve bilgileri kaydetmek için kullanılan boya hızla bozulabildiğinden veri kaybına karşı hassastırlar. En fazla birkaç yıl ona güvenebiliriz (Novice to Know-How: Digital Preservation Skills for Beginners-Why is Digital Preservation Important?, 2020).

4.4.2. Dijital Koruma Modelleri

Dijital koruma için bu zamana kadar oluşturulmuş bazı ana modeller bulunmaktadır. Bu modellere aşağıda yer verilmiştir.

Dijital koruma ile ilgili alan yazında kabul gören bir model Digital Curation Center tarafından geliştirilen Dijital K rasyon Ya am D ng s  Modeli olan  ekil 9'daki modeldir.

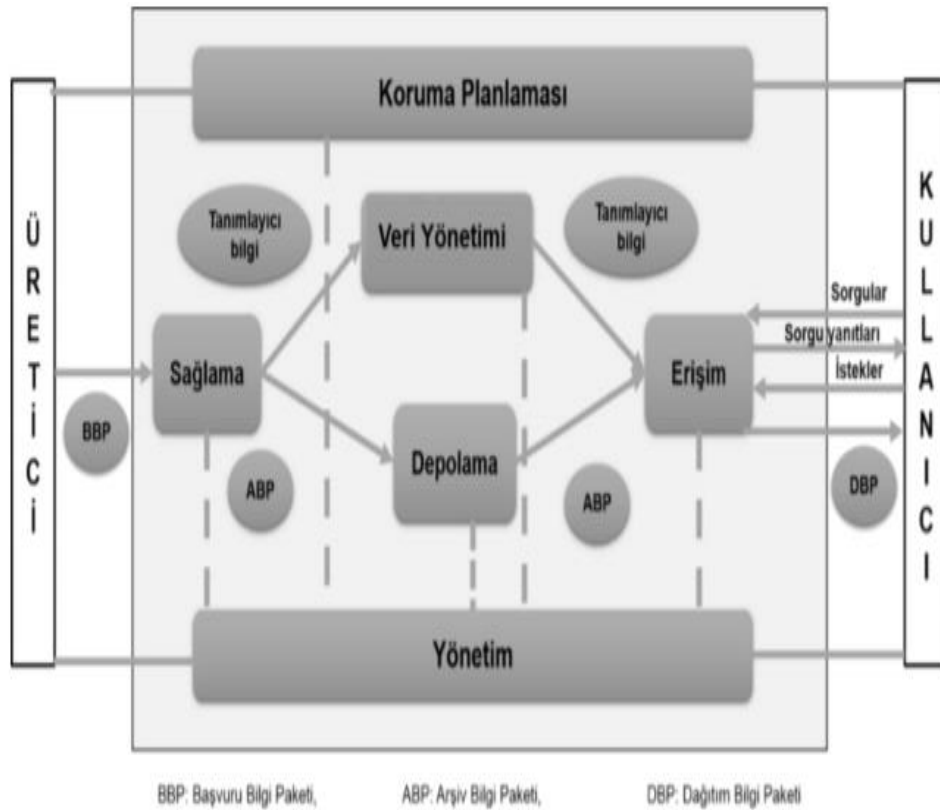


 ekil 9. DCC Dijital k rasyon ya am d ng s  modeli (Higgins, 2008, s. 136;  ztemiz ve  zel, 2019, s. 1211).

Dijital materyallerin s rekliliėini saėlamak i in ya am d ng s  y netimi gereklidir. Model incelendiėinde g ze  arpan  zellik s re lerin iki farklı ardışık d ng  şeklinde birbirini takip etmesidir. İlk olarak dijital nesnenin ya da bir ba ka deyi le verinin sunumu ve tanımlanması a amaları ger ekle tirilmektedir. Sonrasında ise hedef kitle analizi ile birlikte koruma planlamalarının yapılma a amaları gelmektedir. Model dijital nesnelerin korunması ve  retim odaklı bir dizi k rasyon i lemleri ile son bulmaktadır. Bu baėlamda bu i lemlerle diėer ardışık d ng  ile birlikte paralel olarak i leyi  g steren dijital nesnelerin kavramsalla tırılması sonrasında ise  retim ve se im ve nesnelerin ar ive aktarılması s reci birbirini takip etmektedir. Bu i lemlerin ardından sisteme aktarılan dijital nesnelerin koruma i lemleri devam etmekte, depolama ve eri im ve yeniden kullanım s re leri d n  t rme a aması ile son bulmaktadır. Bu i lemler

sırasında sisteme aktarılmayacak olan dijital nesnelerin ayıklanması, göç ettirilmesi aşamaları da paralel bir şekilde işleyiş göstermektedir.

Dijital koruma çalışmalarına örnek bir model Açık Arşiv Bilgi Sistemi Referans Modeli 2003 yılında ISO 14721 standardına dönüştürülüp resmi olarak yayımlanmıştır. Sonrasında bu model 2012 yılında güncellenerek son şeklini almıştır. 2014 yılında ise Açık Arşiv Bilgi Sistemi Referans Modeli Rehberi yayımlanmıştır. Model uzun vadede bilgiyi koruma üzerine odaklıdır. İlgili modele Şekil 10'da görsel olarak yer verilmiştir.



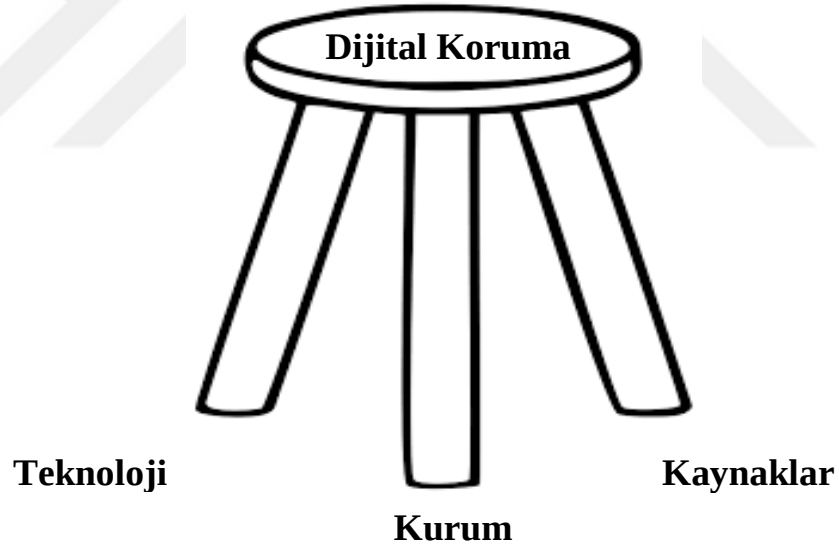
Şekil 10. Açık arşiv bilgi sistemi referans modeli (Çakmak, 2016, s. 30; Reference Model For An Open Archival Information System (OAIS), 2012, s. 41).

Açık Arşiv Bilgi Sistemi Referans Modeli'nin altı temel bileşenini şu şekilde açıklamak mümkündür:

- Sağlama (Ingest): Üretici yolu ile elde edilen bilginin kabulü ve hazırlanması süreci ve kabul edilecek bilgilerin arşivde saklanmasına hazırlanma ile ilgilidir.
- Depolama (Archival Storage): Arşiv sisteminin uzun süreli depolama ve bakımı yöneten kısmıdır. Daha özel olarak, arşivlenen içeriğin uygun depolama biçiminde bulunması ve korunmuş bilgiyi içeren bit akışlarının uzun süre boyunca tam ve okunabilir kalmasını içeren bölümdür.

- Veri Yönetimi (Data Management): Arşiv varlıklarını tanımlamaya ve belgelemeye yarayan bölümdür.
- Koruma Planlaması (Preservation Planning): Koruma planlaması, OAIS'in koruma stratejisinin yanı sıra OAIS'deki gelişen koşullara yanıt olarak bu stratejide uygun revizyonların önerildiği ortamdır. Sürekli değişen ve gelişen teknoloji ortamında verileri koruma ve riskleri öngören bölümdür.
- Erişim (Access): Sistem içindeki bilgiyi kullanıcı ile buluşturmaya yarayan uygulamalardan oluşur.
- Yönetim (Administration): Yönetim bileşeni, OAIS'in günlük operasyonlarını ve ayrıca diğer beş üst düzey OAIS işlevsel biriminin faaliyetlerini koordine etmekle görevlidir (Lavoie, 2014, s. 12-13).

Dijital koruma için bir diğer model ise DPM (Digital Preservation Model) “Three-Legged Stool/Üç Ayaklı Tabure” olarak literatürde yer alan modeldir. İlgili modele Şekil 11’de görsel olarak yer verilmiştir.



Şekil 11. Dijital koruma modeli: Beş aşamalı ve üç ayaklı tabure (Digital Preservation Management Workshop 2003; Kenney ve McGovern, 2003).

Modelde üç ayaklı unsur bulunmaktadır. Her bir unsurun alt aşamaları vardır. Bu unsurlar: kurum, kaynaklar ve teknoloji’dir. Her unsur dijital korumanın başarılı bir şekilde gerçekleşmesi için ele alınması gereken bir dizi sorunu ve etkinliği temsil etmektedir.

Kurum

- Politika
- Strateji
- Prosedürler
- Riskler ve faydalar
- Personel

Kaynaklar

- İş planlaması
- Maliyetler
- Finansman
- Sürdürülebilirlik
- Personel becerileri

Teknoloji

- Depolama ve yedekleme
- Depo sistemleri
- Araçlar
- Güvenlik

Bu unsurlar dışında modelin beş aşaması bulunmaktadır.

1. Onaylamak: Dijital korumanın yerel bir endişe olduğunu anlamak,
2. Eylem: Dijital koruma projelerini başlatmak,
3. Birleştirme: Projelerden programlara ayırma;
4. Kurumsallaştırma: Daha geniş çevreyi dâhil etme,
5. Dışsallaştırmak: Kurumlar arası iş birliğini ve bağımlılığı benimsemek (Kenney ve McGovern, 2003).

4.4.3. Dijital Korumanın Riskleri ve Zorlukları

Daha önceki bölümlerde de belirttiğimiz üzere dijital korumanın henüz bulunmuş kesin bir çözümü yoktur. Kurumlar kendilerine özgü koruma stratejileri geliştirmekte ya da bu konuda zorluk çekip kendine çözüm önerisi getiren kuruluşlarla iş birliğine gitmektedir. Bu bağlamda hala çözilemeyen ve gelecek yıllarda dijital koruma ile ilgili

endişeler, zorluklar bizleri beklemektedir. Dijital içeriklerin çoğu kaybolma riski altındadır, çünkü yönetim ve koruma için çok az sağlam güvenli altyapı bulunmaktadır.

Ulusal Dijital Bilgi Altyapısı ve Koruma Programı/National Digital Information Infrastructure and Preservation (NDIIPP)'na göre dijital koruma ile ilgili birtakım tehditler, riskler bulunmaktadır ve bu riskler dört grup altında incelenmiştir. Bunlar;

Teknolojik Riskler

- Yazılım ve donanımı güncel tutmak ve korumak zor olabilir.
- İçerik biçimleri karmaşık ve kırılgan olabilir.
- Yaşam döngüsü yönetimi riskleri, veri göçü ve dosya bozulması gibi nedenlerle içeriği kullanılmaz hale getirebilir.

Yasal ve Politik Riskler

- Telif hakkı yasaları kütüphanelerin kopya oluşturma ve saklama hakları konusunda net değildir.
- Gizlilik talepleri içeriğin toplanmasını ve belgelenmesini yasaklayabilir.
- Düzenlemeleri içerik sahiplerini tarihsel olarak değerli belgeleri imha etmeye teşvik edebilir.
- Kanunlar, dijital içeriğin korunmasında kamu değerini tanınamamaktadır.

İçerik Riskleri

- Hacim veya verinin karmaşıklık kapsamlı bir şekilde içerik toplamayı zorlaştırır.
- İçeriğin yetersiz tanımlanması kullanımını ve keşfedilmesini zorlaştırır.

Yönetimsel Riskler

- Bilgi oluşturmada yetersiz kaynaklar içerik kaybına neden olabilir.
- Dijital içeriği korumak için yetki ve sorumluluk unsurları genellikle bu tür içeriğin talepleriyle uyumlu değildir.
- Yetersiz vasıflı personel rutin en iyi uygulamaları bile önleyebilir (NDIIPP, 2011, s. 12).

Harvey ve Weatherbur dijital korumanın zorluklarını dört ana gruba ve on altı maddeye ayırmıştır.

- Dijital koruma için standartlar geliştirmek ve onların kullanımını teşvik etmek,

- Yeni içerik oluşturmak,
- İşbirliğini artırmak ve paydaşları dijital koruma programlarına dâhil etmek,
- Dijital koruma ile ilgili politika geliştirme,
- Yasal hakların dijital korumayı engellememesini sağlamak,
- Erişimi korumak için dijital materyallerin özelliklerini belirlemek,
- Dijital korumayı kurumsal faaliyetlere entegre etme,
- Küçük ölçekte de olsa kurumların şimdi harekete geçmesi,
- Korunmuş dijital materyale erişimin sağlanması,
- Korunmuş dijitalin özgünlüğünü ve bütünlüğünü sürdürmek,
- Koruma için daha iyi maliyet modeli geliştirmek,
- Dijital koruma için fon sağlama,
- Dijital koruma hakkında farkındalığı artırmak,
- Dijital koruma için gerekli becerileri geliştirme,
- Dijital korumayı otomatikleştirme,
- Büyük ve artan miktarlarda değişen dijital malzeme ile başa çıkmak (Harvey ve Weatherburn, 2018, s. 200-201).

Dijital koruma için belirtilen on altı zorluğun yanında dört temel zorluk daha bulunmaktadır. Bu zorluklar bu zamana kadar bahsedilen tüm zorluklar içinde en zorlarıdır. Bunlar;

1. Dijital korumayı yönetmek, özellikle de dijital korumayı ana operasyonlara entegre etmek,
2. Yeterli maliyet olmadan dijital korumayı finanse etmek,
3. Dijital korumayı yürütmek, özellikle gerekli becerileri tanımlamak, gelecekte de kullanılabilir olmalarını sağlamak,
4. Dijital korumayı hem büyük sistemlere hem de en küçük kurumlara ölçeklenebilir şekilde uygun hale getirmek

(Harvey ve Weatherburn, 2018, s. 202).

Dijital bilginin değeri olduğunu, fırsatlar yarattığını ve kişisel ve çalışma hayatımızın birçok yönü için gerekli olduğunu biliyoruz. Ancak dijital bilgilere erişim, doğru donanım, yazılım altyapısı ve bunları sürdürme ve kullanma becerisine sahip kişiler gerektirir. Teknoloji ve kadrolardaki personel değişir, bu da kullanımın önünde engeller yaratır. Dolayısıyla, dijital bilginin yaratabileceği fırsatlardan yararlanmaya devam etmek

istiyorsak onu korumak ve muhafaza etmek için aktif adımlar atmalıyız (Novice to Know-How: Digital Preservation Skills for Beginners-Why is Digital Preservation Important?, 2020).

4.4.4. Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmeliğin Dijital Süreklilik ve Uzun Vadeli Koruma Açısından İncelenmesi

Resmi yazışma usul ve esasları 1991 yılında bir genelge ile belirlenmiş, ardından 2004 ve 2015 yıllarında ilgili yönetmelikler yayımlanarak içerik genişletilmiştir. Teknolojinin değişmesi ve gelişmesi ile birlikte EBYS’lerde ihtiyaçlar değişime uğramış ve bu kapsamda 2020 yılında yönetmelik yenilenmiş ve yönetmeliğe dayanak olarak da bir kılavuz hazırlanmıştır.

Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmeliğin amacı; “güvenli elektronik imza kullanılarak elektronik ortamda veya el yazısıyla atılan imza ile fiziksel ortamda yapılan resmî yazışmalara ilişkin kuralları belirlemek, bilgi veya belge alışverişini, hızlı ve güvenli bir biçimde yürütmek ve uygulama birliğini sağlamaktır” (Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik, 2020).

Yönetmeliğe dayanan kılavuza göre yönetmelikte yapılan değişiklikler şu şekildedir:

- “Resmî yazışma süreçlerinin elektronik ortamda yürütülmesi asli unsur haline getirilmesi,
- Belgelerin elektronik ortamda tek nüsha oluşturulması,
- Sayı bölümünde belgenin hazırlanma sürecinin belirtilmesi,
- Doğrulama kodu ve kare kod kullanımı,
- Kişiyeye özel belgelere ilişkin düzenleme,
- Kılavuz ile yönetmelik hükümlerinin detaylandırılması,
- Belge içerisinde logo kullanımı,
- Arşiv imzası,
- Yurt dışı temsilciliklerince oluşturulacak belgelere ilişkin örneklendirmeler,
- Yabancı dilde oluşturulan belgelere ilişkin düzenleme,
- Kılavuzda “Metin İçeriği Hazırlama” ve “Gizlilik” hakkında detaylı bilgilendirme” (Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik Kılavuzu, 2020, s. 5).

Yeni güncelleme ile birlikte, resmi yazışma süreçlerinin artık elektronik ortamda yürütülmesi asli unsur olarak kabul edilmesi dijital süreklilik ile bağlantılıdır. Çünkü dijital süreklilik (digital continuity) kavramı, doğrudan elektronik ortamda işlenen ve saklanan bilginin korunmasıyla ilgilidir. Elektronik ortamda üretilen bilgilerin dijital süreklilik bağlamında bakıldığında kullanılabilir durumda olması ulusal belleğin korunmasına ve bilgi yönetiminin doğru bir şekilde uygulanmasına katkı sağlar (Özdemir ve Cengiz, 2019, s. 273).

Yönetmelikte “Gizlilik” hakkında detaylı bilgilendirme” ileride öne çıkacak dijital belgelerin hassasiyet değerlendirmesi açısından oldukça önemli bulunmaktadır.

Belgelerin elektronik ortamda tek nüsha oluşturulması yeniliği, fazla nüshaların oluşmasını engeller ve böylelikle doğuştan dijital belgelerin değerlendirilmesi ve ayıklanması aşamalarında kolaylık oluşur. Keza Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik Kılavuz’unda bu durum aşağıdaki kazanımları sağladığı belirtilmiştir:

- “Sistem performansının artması, uygulamanın ve imza süreçlerinin hızlanması
- Veri boyutunun küçülmesiyle veri saklama ve yedekleme ünitesi maliyetlerinde tasarruf sağlanması” (2020, s. 7).

4.4.5. Dijital Koruma İçin Faydalı Çalışmalar, Araçlar ve Sistemler

Dijital koruma için büyük önem taşıyan, çeşitli kurumlar ya da yazılım geliştiriciler tarafından uygulamada yaşanan dosya formatlarından kaynaklı sorunları gidermek amacıyla tasarlanan/geliştirilen bir takım araç ve sistemler bulunmaktadır. Bu araçlar ve sistemler dijital korumaya fayda sağlamaktadır. Bu bölümde dijital koruma bağlamında önemli bir yere sahip olan Açık Koruma Vakfı ve çalışmalarından bahsedilmiştir. Buna ek olarak farklı kurumlar tarafından geliştirilen dijital korumaya fayda sağlayan sistemlere aşağıda detaylı olarak yer verilmiştir.

Açık Koruma Vakfı ve Çalışmaları - Open Preservation Foundation (OPF)

OPF, AB tarafından finanse edilen ve Gezegenler adı verilen araştırma ve geliştirme projesinin sonuçlarını sürdürmek üzere 2010 yılında kurulmuştur. Tütünün ilk kuruluşlarından biri olan vakfın hedefi; projenin dijital korumayı geliştirmeye yönelik işbirlikçi ve pratik yaklaşımını geliştirmektir. 2014 yılında OPF, büyüyen bir alandaki evrimi ve alaka düzeyini yansıtmak için adını Açık Gezegenler Vakfı'ndan Açık Koruma

Vakfı'na deęiřtirdi. OPF, dñnyanın dñrt bir yanından gelen dijital koruma uygulayıcılarını açık kaynak topluluęuna davet eden, kâr amacı gütmeyen baęımsız bir üyelik organizasyonu olarak faaliyet göstermektedir. Vizyonları; açık sürdürülebilir dijital koruma ve misyonları ise; etkili ve verimli dijital koruma için ortak çözümler sağlama, sürdürülebilir, açık kaynaklı dijital koruma araçları ve destekleyici kaynakların referans setini oluşturmak, sürdürmek ve geliřtirmek için ortak bir çaba göstermektir. Bu araç seti (yazılım ve standartlar dâhil), kuruluşların istenen içerięi ve topluluęun en iyi uygulamaları doęrultusunda korunmasını sağlamak için riski deęerlendirmek, doęrulamak, belgelemek, riski azaltmak ve işlemek için dijital içerik sağlar (Open Preservation Foundation (OPF), 2020).

Açık Koruma Vakfı, kullandığı PDF ile ilgili birtakım sorunlar yařandığı gözlemlemiřtir. Bu bağlamda da ilk akla gelen sorular bunlardır; PDF hatası ne anlama geliyor? Bu hatayı nasıl düzeltebilirim? Bu hatanın uzun süreli kullanılabilirlik üzerine bir etkisi var mı, var ise nedir? OPF dijital arřivinde kalıcı depolama alanında 213.913 PDF dosyası bulunmaktadır. Önceki yıllarda tüm bu PDF'leri PDF / A-2b'ye dönüřtürmek için pdfaPilot satın almıřlar ve pdfaPilot'u, Dijital Arřiv Sistemi olan Rosetta'nın Koruma Planlama modülüne eklenti olarak entegre etmiřler ve sisteme başarı katmıřlardır (Open Preservation Foundation (OPF), 2020).

OPF, bünyesinde bir dizi açık kaynaklı dijital koruma ürünü bulundurmaktadır. Bu ürünler ağırlıklı olarak koruma öncesi ve sisteme aktarma aşamalarından önce (pre-ingest) kullanılmaktadır. Sahip olduęu ürünler; Jpylyzer (JP2 görüntüler için açık kaynaklı bir doęrulayıcı ve özellik çıkarıcıdır), Fido ((Dijital Nesneler için Biçim Tanımlama), dijital nesnelerin dosya biçimlerini tanımlamak için açık kaynaklı bir komut satırı aracıdır), JHOVE (tanımlama, doęrulama ve karakterizasyon için açık kaynaklı, genişletilebilir bir yazılım çerçevesidir), veraPDF³⁷ (PDF/A standartlarının tüm bölümlerini kapsayan ilk eksiksiz açık kaynaklı PDF/A doęrulayıcıdır) bu řekildedir. Bu ürünler sürekli bir üst versiyona çıkarıp geliřtirilmektedir (Open Preservation Foundation (OPF), 2020). Aynı zamanda ISO' da PDF/A'yı dijital belgelerin arřivlenmesi açısından onaylamıřtır. ISO 19005-1 standardına göre "PDF/A; PDF'nin elektronik belgeleri, görñnüşlerini zaman içerisinde koruyan ve dosyaları oluřturma, depolama veya geri

³⁷ veraPDF, dijital koruma uzmanlarının ihtiyaçlarını karřılamak üzere tasarlanan ve PDF yazılım geliřtirici topluluęunun önde gelen üyeleri tarafından desteklenerek geliřtirilen, tüm PDF/A parçalarını ve uygunluk düzeylerini kapsayan amaca yönelik, açık kaynaklı, izin verilen lisanslı bir dosya biçimi doęrulayıcıdır (VeraPDF, 2020).

verme için kullanılan araç ve sistemlerden bağımsız tutan bir tarzda temsil etmek için bir düzenek sunan" bir dosya biçimidir (ISO, 19005-1:2005).

PRONOM

PRONOM, veri dosyası formatları ve destekleyici yazılım ürünleri hakkında çevrimiçi bir bilgi sistemidir. PRONOM sadece teknik bilgi veri tabanından daha fazlasıdır. Koruma riski değerlendirmesi, geçiş yolu planlaması, nesne tanımlama ve doğrulama ve üst veri çıkarma gibi dijital koruma işlevlerini destekleyen bir dizi araç ve hizmeti kapsamayı amaçlamaktadır. İngiliz Milli Arşivleri tarafından elektronik belgelerin erişimi ve uzun süreli korunmasını desteklemek için geliştirilen PRONOM şimdi bu tür bilgilere erişim isteyen herkes için bir kaynak olarak sunulmaktadır. PRONOM, yazılım ürünleri ve her ürünün okuyabileceği ve yazabileceği dosya biçimleri hakkında bilgi tutmaktadır. PRONOM, yazılım ürünleri, yaşam döngüleri ve teknik gereksinimleri desteklemek ve destekledikleri dosya formatları hakkında yetkili bilgilere ihtiyaç duyan herkes için bilgi kaynağı olarak sunulmaktadır (What is PRONOM?, 2020).

PRONOM'un ilk versiyonu İngiliz Milli Arşivi Dijital Koruma Departmanı tarafından Mart 2002'de geliştirilmiştir. PRONOM'a olan ihtiyacın doğuşu, İngiliz Milli Arşivi'nin dijital arşivinde saklanan elektronik belgelerin doğası hakkında güvenilir teknik bilgilere kolayca erişilmesi ihtiyacından kaynaklanmıştır. Elektronik, dijital belgeler doğası gereği insan tarafından okunamaz. Dosya formatları bilgileri yalnızca çok özel donanım ve yazılım kombinasyonları ile işlenebilen ve anlaşılabilir hale getirilerek kodlanmaktadır. Bu bağlamda bu bilgilerin erişilebilirliği günümüzün hızla gelişen teknolojik ortamında oldukça savunmasızdır. Bu konu sadece dijital arşivcilerin değil, aynı zamanda nispeten kısa zaman dilimleri içinde elektronik belgelere erişimin yönetilmesinden ve sürdürülmesinden sorumlu olanların da bir endişesidir. Bu nedenle, dosya formatlarının yapısı ve bunları destekleyen yazılım ürünleri hakkında teknik bilgiler herhangi bir dijital koruma rejimi için bir ön koşuldur. PRONOM bunu başlangıçta İngiliz Milli Arşivlerinin personeli için özel bir kaynak olarak geliştirilmiş ancak daha sonra herkesin kullanımına açık hale getirilmiştir (PRONOM, 2020).

DROID (Digital Record Object Identification)

Dosya profili oluşturma aracı DROID, Dijital Kayıt Nesnesi Tanımlama anlamına gelmektedir. İngiliz Milli Arşivi tarafından geliştirilen ve çok çeşitli dosya formatlarını otomatik olarak profillemeye yardımcı olacak ücretsiz bir yazılım aracıdır. Örneğin,

DROID kullanımı ile kurumlar hangi sürümlere sahip olduklarını, belgelerin yaşlarını, boyutlarını ve en son ne zaman değiştirildiğini belirlemeye yardımcı olurken aynı zamanda fazla nüshaları da bulmayı sağlayacaktır. Dosya biçimlerinin profilini oluşturmak bilgileri daha etkili bir şekilde yönetmeye ve riskleri belirlemeye yardımcı olacaktır. Ayrıca, örneğin veri azaltmayı destekleyerek paradan tasarruf etmeye de katkı sağlayacaktır.

DROID kullanmak, belirli bir bilgi riskini (dijital süreklilik riski) yönetmeye yardımcı olacaktır. DROID, kurumların bilgi varlıklarını anlamak için ihtiyaçları olan bilgileri toplamaya yardımcı olur. Bu, kurumların dijital süreklilik gereksinimlerini tanımlamalarına, bilgilerinin nerede risk altında olduğunu değerlendirmelerine yardımcı olacaktır. DROID' den alınan bilgiler, sahip olunan veri miktarını azaltmaya yardımcı olarak daha verimli ve düşük maliyetli çalışmaya olanak tanımaktadır (File profiling tool (DROID), 2020).

İngiliz Milli Arşivi DROID ile ilgili kurumların kullanımı kolaylaştırmak adına bir rehber hazırlamışlar ve açık erişim olarak rehberi web sayfalarına eklemişlerdir. Rehberin aşağıdaki unsurlara yardımcı olması amaçlanmıştır:

- dijital dosyaların DROID'e nasıl yükleneceğini ve çalıştırılacağını anlama,
- sonuçlarını yorumlama, yaygın tuzaklardan kaçınma,
- DROID ile dosya profilini oluşturmak için bazı olası sürücülerini anlamak (*DROID : user guide*, 2017).

Archivematica

Archivematica, kurumların otantik ve güvenilir dijital içeriğe uzun süreli erişimine koruma sağlayan web ve standartlara dayalı açık kaynaklı bir uygulamadır. Archivematica, kullanıcıların dijital nesneleri girişten erişime ISO-OAIS fonksiyonel modeline uygun olarak işlemesine olanak tanıyan entegre bir açık kaynaklı yazılım araçları paketidir. Kullanıcılar, mikro tabanlı hizmetleri web tabanlı bir gösterge tablosu aracılığıyla izler ve kontrol eder. Archivematica, tercih edilen depoda depolamak için güvenilir, otantik, güvenilir ve sistemden bağımsız Arşiv Bilgi Paketleri (AIP) oluşturmak için METS, PREMIS, Dublin Core ve diğer tanınmış standartları kullanmaktadır (Archivematica, 2020).

COPTR (Community Owned digital Preservation Tool Registry - Topluluğa Ait Dijital Koruma Aracı Kaydı)

COPTR, uzun süreli dijital koruma için yararlı araçları tanımlar. Öncelikle, uygulayıcıların belirli koruma görevlerini yerine getirmek için ihtiyaç duydukları araçları keşfetmelerine yardımcı olmak için bir bulma ve değerlendirme aracı görevi görür. COPTR, dijital koruma topluluğunun koruma araçları hakkındaki bilgilerini tek bir yerde toplamaktadır. COPTR, kendi sicilleriyle birbirleriyle rekabet eden organizasyonlar yerine, onları bir araya getiriyor. Bunu yaparken amaç, dijital koruma araçları konusunda uygulayıcılara en iyi kaynağı sağlamaktır. COPTR'de tanımlanan 506 farklı araç bulunmaktadır (COPTR (Community Owned digital Preservation Tool Registry 2020).



BEŞİNCİ BÖLÜM

5. DOĞUŞTAN DİJİTAL BELGELERİN ARŞİVE TRANSFERİ SÜRECİ İLE İLGİLİ YAKLAŞIMLAR, ULUSAL VE ULUSLARARASI ÇALIŞMALAR

Bu bölümde milli arşivlerin doğuştan dijital belgelerin milli arşive transfer süreçleri ile ilgili çalışmaları incelenmiştir. Kurumların web sayfalarından elde edilen veriler incelenmiş ve ülke ve milli arşiv bazında bulgular sunulmaya çalışılmıştır.

5.1. İngiltere – İngiliz Milli Arşivi /TNA (The National Archives)

İngiliz Milli Arşivi alanında her yönü ile en iyilerin başında gelmektedir. Bunun sebebi hem uygulama odaklı olması hem de kamu kurum ve kuruluşlarına sunduğu politikalarıdır. İngiliz Milli Arşivi'nin doğuştan dijital belgelerin arşive transfer süreçleri ile ilgili çalışmaları oldukça gelişmiş düzeydedir. İngiliz Milli Arşivi (The National Archives) dijital belgelerin transferi aşamasına geçmiştir. Fakat dijital belgelerin arşive transferi fiziksel belgelerinki kadar basit değildir. İngiltere'de belgelerin transferinde ilk aşama 2013'te başlamıştır. Bu değişim kamu kurum ve çalışanları için büyük bir değişim olarak görülmüştür. Bu sürecin aşamalı olarak gerçekleştirilmesi ve yönetilmesi uygun bulunmuştur (20-year rule, 2020). Bilgi Edinme Hakkı Kanunu'nun getirilmesinden önce kamu kurumlarının belgeleri 30 yaşına gelene kadar genel olarak herkesin erişimine açık değildi fakat Bilgi Edinme Hakkı Kanunu (2005) gereği belgenin tarihi ne olursa olsun yasa gereği belirlenen gizlilik şartlarının içine dâhil olmadıkça herkesin erişimine açık olmalıdır (*Records Review*, 2014, s. 26).

İngiliz Milli Arşivi dijital belgelerin transferi, bilgi yönetim süreçleri için birtakım rehberler ve stratejiler oluşturmıştır. İngiliz Milli Arşivi dijital belgelerin transfer aşamasını; değerlendirme, seçim/ayıklama, hassasiyet değerlendirmesi, transfere hazırlık, paketleme ve teslim olmak üzere beş adıma ayırmıştır (*Digital transfer steps*, 2019). Tüm bu süreçlerin her biri ile ilgili ayrıntılı bir şekilde politika ve rehberler hazırlamışlardır. Ayrıca İngiltere, dijital belgelerin korunması ile ilgili dijital koruma politikası, dijital süreklilik politikası ve rehberi de hazırlamış ve web sitesinde araştırmacılar için açık erişim halinde sunmuştur. İngiliz Milli Arşivi'ne göre dijital belgelerin transfer aşamaları olan değerlendirme ve seçim/ayıklama aşamaları kalıcı koruma için hangi belgelerin saklanacağı, hangi belgelerin ayıklanmasına karar verileceği aşamadır. İngiliz Milli Arşivi bu aşamada “makro değerlendirme ve seçim” yöntemini tercih edip önermektedir. Bu yöntem tüm kayıtların tek tek değerlendirip

seçilmesi/ayıklanması değil verimlilik ve ölçeklenebilirlik açısından makro düzeyde işlemlerin yapıldığı bir yöntemdir. Değerlendirme yaparken iki değer önem arz eder. Bunlar birincil ve ikincil değerlerdir. Birincil değerler; belgeleri oluşturan idari, yasal ve mali koşullardır. İkincil değerler ise; kuruma toplumsal ve tarihsel boyutta değer sağlayan belgeleri içerir (*What is appraisal?*, 2013, s. 3-4). İngiliz Milli Arşivi ilk olarak belgelerin kapsam olarak tanımlamakla başlamak gerektiğinin altını çizer. Bunlar; tarih, bulunduğu ortam (EBYS vb.), boyut, format, fazla nüsha ve koleksiyonu tanımadır. Örneğin; geçmiş belge transferleri, bilgi varlık kaydı, belgenin yaşı, yapısı, önemli olaylar vb. İngiliz Milli Arşivi tüm bu işlemleri yaparken yararlandığı ve herkese önerdiği, dijital belgelerin değerlendirme ve seçim/ayıklama aşamalarında yardımcı bir program olan DROID³⁸'i kullanmaktadırlar. Bu aşama aynı zamanda dijital süreklilik ile de bağlantı kurup kurumun bilgi varlıklarını belirlemesi gerektiğini belirtir (*Steps 1 and 2: Appraisal and selection*, 2019). İngiliz Milli Arşivi fiziksel belgelerin değerlendirme aşamasında “Grigg Sistemi” adı verdikleri bir sistem kullanmaktadır. Bu sistem fiziksel belgelerin değerlendirilmesinde iki aşamada (ilk aşama; belgeleri devam eden beş yıl içinde değerlendirme, ikinci aşama; 25 yıl arşivsel değer açısından değerlendirme) yürütülmektedir. Fakat bu sistem dijital belgeler için uygun değildir. Zira belgelerin değerini belirlemek ve değerlendirmek için 25 yıl beklemek uygun değildir, aynı zamanda yıllar içinde sistemsel ya da yazılımsal bakımdan belgelerin uzun vadeli korunması sağlanamayabilir. Bu ve benzer sebeplerden ötürü dijital belgeler için Grigg sistemi kullanılması önerilmemektedir (*Background paper-the "Grigg System" and beyond*, 2004). Diğer bir aşama olan hassasiyet değerlendirmesi dijital belgelerin transferinde en çok zorlanılan kısım olarak ifade edilmektedir. Bu aşama dijital belgelerin hangilerinin saklanması gerektiğini ve hangilerinin arşive açık veya kapalı olarak aktarılacağını belirlenmesi ile ilgilidir. Bu süreç iki adımla ilerlemektedir;

- Düşün ve bul,

Önemli hassasiyet alanlarını belirlemek önceki değerlendirme ve seçim/ayıklama aşamalarında araştırmaya dayanarak neler yaptığınızı anlamak için koleksiyonu araştırmak gerekir. Hassas belgeleri belirlemek için belgeler ve üst verileri gözden geçirilmelidir.

- Kontrol et ve yap,

³⁸İngiliz Milli Arşivi tarafından oluşturulan açık kaynak kodlu ve ücretsiz bir yazılımdır.

Dijital belgelerin hassasiyeti adına kapatılması ve saklanması için başvuruları inceleme ve tavsiye için milli arşivlere gönderilir. Başvurular Danışma Konseyine (Advisory Council for National Records and Archives) sunulur ve toplantılarından birinde gözden geçirilir. Konsey kararı sizinle paylaşılır. Onaylandıktan sonra, saklanan bilgilerin aktarım dışında bırakıldığından emin olunur; kapalı belgeler ve üst veriler düzeltilir (gerekirse) ve düzeltilmiş belgelerin kopyaları oluşturulur. Teknik işlemler yapılırken dikkat edilmesi gereken bir konu ise bağlamdır. Belgelerdeki duyarlılıkları karakterize etmenin en iyi yolu düşünülüp bulunmalıdır. Hassasiyet incelemesinde bir takım yazılım araçları kullanılabilir. Örneğin hukuk alanında e-keşif aracı isimler, sigorta numaraları vb. hassas bilgileri bulmada kilit rol oynamaktadır (*Step 3: Sensitivity review*, 2019). Dördüncü aşama olan transfere hazırlık, sürecin en teknik kısmıdır ve belgelerin ve üst verilerin kurumdan Milli Arşive fiziksel olarak taşınma sürecini oluşturur (*Step 4: Preparation for transfer*, 2019). Transfer sürecinin son aşaması olan paketlenme ve teslimat ise; dijital koruma ekibinin yoğun teknik bir süreç içerisinde belgeleri sisteme alma, virüs kontrolü, belgelerde bir hasar var mı vb. işlemlerin yapıp test edildiği bir aşamadır (*Step 5: Packaging and delivery*, 2019). İngiliz Milli Arşivi'nin dijital belgelerin değerlendirme ve seçim/ayıklama aşamalarında paralel olarak bahsettiği diğer bir konu dijital süreklilik konusudur. Dijital süreklilik; ihtiyaç duyduğunuz sürece bilgiyi bulma, bilgiyi açma, bilgiyle çalışma, bilgiyi anlama ve bilgiye güvenmektir. Milli Arşivi dijital sürekliliği yönetmek için dört aşamalı bir süreç izlemiştir. Bunlar; eylem planı, dijital süreklilik gereksinimlerini tanımlamak, dijital süreklilik risklerini değerlendirmek ve yönetmek, dijital sürekliliği sağlamak'tır (*What is Digital Continuity?*, 2019).

İngiliz Milli Arşivi'nin bir koruma politikası bulunmaktadır, bu politika fiziksel ve dijital tüm arşiv materyalleri içindir. Aynı zamanda dijital belgeler için bir dijital koruma rehberi ve el kitabı bulunmaktadır. Koruma politikasındaki amaç; koleksiyonları gelecek nesiller için koruma, özgünlüğü ve değeri koruma ve aynı zamanda bozulma, hasar, kayıp, eskime vb. risklere karşı koruma ile sınırlı değildir. İngiliz Milli Arşivi aynı zamanda tüm koleksiyon için risk yönetimi stratejisi ve koruma riski değerlendirmesi yapmaktadır. Dijital koleksiyon için ise İngiliz Milli Arşivi dijital koruma riskinin modellenmesi için bir "Dijital Strateji" modellemesi benimsemiştir (*Preservation Policy*, 2018, s. 3). Dijital Strateji modellemesinde üç yıl içinde hedeflenen planlar şu şekildedir; yıkıcı (disruptive), ikinci nesil bir dijital arşiv oluşturmak, interneti kullanarak yeni kullanıcı kitlelerinin katılımı sağlama ve erişimi genişletmek, fiziksel arşive nasıl

erişildiğini ve kullanıldığını dönüştürmek, dijital yetenek, kültür ve becerileri geliştirmek, dijital dönüşüm sürecinde ilerleyen diğer arşivlerle iş birliğine gitmek'tir. Bu dokümanda bir takım dijital zorluklardan bahsedilmektedir. Bunlar;

- Belgeler fizikselden dijitale taşınır/dönüşür.
- Dijital koruma zordur.
- Beklentiler değişmiştir.
- Değişim bundan sonraki süreçte de devam edecektir.
- Dijital beceriler (dijital veri süreçleri ile baş edebilecek profesyonel düzeyde bilgi ve beceri) önem kazanmıştır (*Digital Strategy*, 2017, s. 3-5).

İngiliz Milli Arşivi dünyanın önde gelen arşivlerinin başında olmasına rağmen kendini birinci nesil olarak görmektedir ve amaçları ikinci nesil bir arşiv olmaktır. İkinci nesil arşiv birinci nesil arşiv anlayışından vazgeçmek, fizikseli bırakıp tüm süreçleri dijital olarak yönetmek ve ilerletmekten geçmektedir. İkinci nesil (disruptive) arşivin vizyonu; içgüdü ve tasarımla dijital ikinci nesil bir dijital arşiv olmaktır (*Digital Strategy*, 2017, s. 6).

Dijital arşivin kullanıcılarına sunduğu değer için dört kategori vardır:

- Koruma (preserve),
- Bağlamsallaştırma (contextualise),
- Sunma (present),
- Kullanımı etkinleştirme (enable use) (*Digital Strategy*, 2017, s. 6).

İngiliz Milli Arşivi, 2016 yılında doğuştan dijital belgelerin değerlendirmesi, seçimi/ayıklaması ve hassasiyet değerlendirmesinin elektronik keşif yazılımını (e-discovery)³⁹ kullanarak teknoloji tabanlı desteklenmesi ile ilgili bir rapor yayımlamıştır (*The application of technology assisted review to born-digital records transfer, Inquiries and beyond*, 2016). Doğuştan dijital belgeler kamu kurumları için yüksek hacimli belgelerdir ve Milli Arşivlere aktarım sırasında sadece değerlendirme, seçim/ayıklama ve hassasiyet süreçlerini etkilemez aynı zamanda bilgi özgürlüğü kapsamında vatandaşın taleplerini karşılama bakımından da oldukça önemlidir. Doğmuş dijital belgelerin yönetim süreçleri ile ilgili birtakım zorluklar bulunmaktadır. Bu zorlukları belirleyip

³⁹ Elektronik keşif, bir davada veya soruşturmada üretim talebine yanıt olarak elektronik olarak depolanan bilgileri tanımlama, toplama ve üretmenin elektronik yönüdür.

özüm önerileri getirmek için İngiliz Milli Arşivi e-keşif aracını kullanarak teknoloji tabanlı değerlendirme denemelerini sekiz bölümle özetlemiştir:

- Doğuştan dijital belgeleri anlama, (belgenin format, hacim, kopya, tarihi hakkında bilgi)
- İncelenecek bilgi miktarını azaltma, (yinelenen bilgiler, büyük veri hacmi)
- Anlam çıkarma, (belgenin hacmi, bağlamı, personel bilgisi konularının alaka düzeyi ve değerinin anlaşılması ve belirlenmesi)
- Kişisel bilgilerin belirlenmesi,
- Tedarik/Sağlayıcı, (ilgili süreçler için doğru yazılımın ve ürünün seçilmesi)
- Kullanıcı arayüzü,
- Diğer ekiplerle iş birliği,
- Teknoloji destekli incelemeye güven.

Tamamen otomatik bir özüm hiçbir zaman yoktur, her zaman insana ihtiyaç olacaktır, fakat bu tür teknolojik özümler ve öneriler bize kolaylık sağlayacaktır. Denemeler göstermiştir ki; insan incelemesinin aksine, yazılım araçlarını kullanarak teknoloji destekli inceleme tüm içeriği ve üst verileri eşit olarak dizine ekler ve arar. Teknoloji destekli inceleme yazımlarını kullanmak tek başına manuel inceleme ve kelime araması yapmaktan daha güçlüdür ve aynı zamanda gözden geçirilen büyük miktarda bilgiyi işlemeye yardımcı olmaktadır. İngiliz Milli Arşivi belirli bir miktar veri üzerinden e-keşif aracı ile değerlendirme, seçim/ayıklama ve hassasiyet üzerine çalışmış, sonra da aynı işlemi manuel olarak yapmış ve hangisi daha etkili diye karşılaştırmış bu ise kullanıcı arayüzü olarak karşımıza çıkmaktadır. E-keşif aracı doğuştan dijital belgelerin formatı, hacmi, kopyaları ve tarihi konusunda bilgi vermektedir. Yine incelenecek bilgi miktarını azaltmak için büyük miktardaki belgeleri alt gruplara ayırıp inceleme, bazı belge gruplarını incelemeye hiç dâhil etmeme (her belge grubunun incelenmesi gerekmez) gibi aşamaları içermektedir. Ayrıca araç, bilgi güvenliği konusunda da yardımcı olmaktadır. Anlam çıkarma aşaması; genel olarak belgenin hacmi, bağlamı, personel bilgisi konularının alaka düzeyi ve değerinin anlaşılması ve belirlenmesi ile ilgilidir. Bunun için de e-keşif aracı sınıflandırma, kümeleme ve e-posta görselleştirme yöntemlerini kullanır. Bu yöntemler sayesinde belge grupları arasında daha hassas belgeler grupları ayırıştırıp onların üzerinde çalışılabilmesine olanak verir. Kişisel bilgilerin belirlenmesi sürecinde herkesin aklına gelebilecek kimlik numaraları, telefon numaralı, kredi kartı numaraları gibi temel hassas veri grupları belirlenmelidir. Bunun

dışında bu bilgileri belirlemek için teknolojiye %100 güvenemeyiz. Örnekler göstermiştir ki bir ismin yazılışının 112 farklı şekli olabilmektedir ve anahtar kelime aramasıyla hassas veriyi gözden kaçırmak olasıdır. Tedarik aşaması kısmı ilgili süreçler için doğru yazılımın ve ürünün belirlenmesi kısmıdır. İngiliz Milli Arşivi e-keşif aracını doğuştan dijital belgelerin bilgi yönetim süreçlerinde kullanılabilir olduğunu yaptığı denemelerden sonra anlamıştır. E-keşif aracı teknoloji destekli gözden geçirme sürecinde yaygın hale gelmektedir. Ancak yine de hiçbir teknoloji ilgili işlemlerde %100 sonuç vermez ve e-keşif aracı gibi farklı araçlar da piyasa girmektedir ve girecektir (*The application of technology assisted review to born-digital records transfer, Inquiries and beyond*, 2016).

İngiliz Milli Arşivi'nin dijital koruma stratejisi ve politikası bulunmaktadır. İngiliz Milli Arşivi'ne göre dijital koruma stratejinin amacı, dijital belgelerin yönetiminde tutarlılık sağlamak olmalıdır. Strateji aktif koruma için gerekli eylemleri tanımlamalıdır. Dijital koruma stratejisi bir politika ile desteklenmelidir. Dijital koruma stratejisi, bir kurum tarafından dijital belgelerin içeriğinin zaman içinde kullanılabilir bir biçimde kalmasını sağlar. Aynı zamanda dijital strateji, dijital belgelerin ne zaman alınabileceğini belirleyecek tetikleyicilerin bulunduğu yerdir. Örneğin; göç ve içeri alma. Göç/taşıma; eskimeye yakın dosya biçimlerini daha sürdürülebilir bir biçime getirmek için yapılır. İçeri alma (Ingest); belgeler dosya formatlarında alındığında tanımlanmış bir normalleştirme yapılır ve belge içeriğini daha sürdürülebilir bir formatta sunulur. Aynı zamanda İngiliz Milli Arşivi dijital koruma politikasında ve dijital stratejide olması gereken unsurları şu şekilde belirtmiştir. Dijital korumada politikasında olması gereken unsurlar; dijital koruma mülkiyeti, dijital korumanın stratejik hizalanması, dijital korumanın kapsamı, roller ve sorumluluklar, diğer politikalarla ilişki, diğer çalışmalarla ilişki şeklindedir. Dijital stratejide olması gereken unsurlar; dijital belgeler için depolama türü, tercih edilen/kabul edilen formatlar/biçimler, göç/taşıma için tetikleyiciler, göç türleri, normalleştirme tetikleyicileri, normalleştirme türleri şeklindedir (*Digital Preservation Policies: Guidance for archives*, 2011).

5.2. Avustralya-Avustralya Milli Arşivi/National Archives of Australia (NAA)

2011 yılında Dijital Geçiş Politikası Avustralya Hükümeti tarafından onaylanıp, yayımlanmıştır. Bu politikanın ana amacı, bundan sonraki bilgi ve belge sürecinin mümkün olduğunca dijital olarak oluşturulması ve kâğıt belgelerin oluşturulmamasıdır (*Digital transition policy*, 2011).

Avustralya Hükümeti dijital dönüşüm sürecinde dijital sürekliliğe büyük önem vermiş ve konu ile ilgili 2015 yılında Dijital Süreklilik Politikası 2020'yi hazırlamıştır. Politikanın amacı, devletin tüm süreçleri ile entegre bir dijital bilgi yönetimini sağlamaktır. Politika üç altın değer üstüne kurulmuştur. Bunlar; bilginin değerli olduğu, bilginin dijital olarak yönetilmesi gerektiği ve bilgi, sistemler ve süreçlerin birlikte çalışabilmesi üzerinedir (*Digital Continuity 2020 Policy*, 2015).

Avustralya Milli Arşivi'nin önümüzdeki iki yıl için önlerini görebilmek, yönlerini bulabilmek adına oluşturdukları bir Stratejik Planı vardır. Hepimizin nereye gittiğini, ne yaptığını ve neden bu dijital çağda dünya lideri bir arşiv olma vizyonuna ulaşmak için birlikte çalıştığını bilmelerine yardımcı olacağı düşünülmektedir. Arşiv bu planı 18 Haziran 2018'de yayımlanmıştır (*The Archives 2020 Strategic Plan*, 2018).

Avustralya Milli Arşivi, 2018 yılında Dijital Koruma Politikasını yayımlamıştır. Bu politikanın amacı; dijital belgelerin içeriği yazılım eskimesi sebebiyle erişilemez hale gelmesi, dijital belgeleri depolamak için kullanılacak olan donanımın arızalanması ya da eskiyip veri kaybolması, içeriğin kötü amaçlarla değiştirilip veri kaybı olması veya aktarım sırasında veri kaybı yaşanması risklerine karşı korumadır (*Digital Preservation Policy*, 2018).

Avustralya Milli arşivi dijital belgelerin arşive transferi için belirli aşamalar belirlemiştir. Bunlar; kurumun transfer edilecek belgeleri belirlemesi, transfer için Milli Arşivle irtibata geçilmesi (bu kısımda eğer kurum transfer için hazır olduğunu düşünüyor ise Milli Arşiv'deki yetkili kişilerle iletişime geçiyor ve yetkililer kuruma dijital belgelerin transferi için belgelerin format, boyut, üst veri ve depolama aygıtı gereksinimleri süreçlerini bildiriyor), belgelerin transfer için hazırlanması (bu kısımda belgelerin sınıflandırılmamış olması gerekiyor (fiziksel belgeler için sınıflandırma ve belge numarası, güvenlik numarası istenmekte) ve (belgelerin USB veya taşınabilir sabit sürücülerde saklanması), transferden önce tüm belgelerin Avustralya Hükümeti Bilgi Güvenliği Kılavuzu ile uyumlu olmasına dikkat edilmesi gerektiği, transfer için gerekli formları doldurma (sırasıyla işlemler halledildikten sonra yetkililer kuruma ilgili formları doldurmaları için gönderirler bu formlar fiziksel ve dijital belgeler için aynıdır), transfer onayı ve tarihi belirleme, son olarak transfer işleminin gerçekleşmesi aşamalarıdır (*Transferring information to the National Archives. (2020, 5 Mayıs), 2020*).

Avustralya Milli Arşivi dijital belgeleri transfer ederken sınıflandırılmış dijital belgeleri işleyememekte, sınıflandırılmamış dijital belgeleri işlemektedir. Bunun yanı sıra dijital belgelerin nerede tutulduğu, hangi formatta olduğu, boyutları, sayıları da önemlidir. Belgelerin taşınabilir bir ortamda tutulması gerekmektedir. Her dijital belge için doğru dosya yolu sağlanmış olmalıdır. Aktarımdan önce Bilgi Güvenliği Kılavuzu'na uygun olmalı ve sağlama toplamlarının oluşturulmuş olması gerekmektedir. Belgeler transfer edilirken antivirüs taramasından geçirilir. Daha az hassasiyet veya sınıflandırmaya sahip bir sisteme aktarılan tüm veriler güvenilir bir kaynak tarafından gözden geçirilir ve onaylanır. Transfer için seçim/ayıklama aşamasında bazı prensipler vardır. Bunlar; belgenin önemini bilme ve tanımlama, devlet otoritesi, eylem ve hesap verilebilirlik, kimlik, etkileşim, haklar ve yetkiler, bilgi ve toplum belleği'dir. Belgelerin ayıklanması ile ilgili uyguladıkları da birtakım kriterler bulunmaktadır. 1980 sonrası oluşturulmuş belgeler, biçim bütünlüğü, erişim ve erişilebilirlik, okunabilirlik, üst veri olarak çıkartılabilme yeteneği, belgelerin orijinal formda tutmanın maliyet analizi gibi faktörler ayıklama için birer unsurdur (*Transferring information to the National Archives. (2020, 5 Mayıs), 2020*). Aynı zamanda yapılan çalışmalar incelendiğinde Avustralya Milli Arşivi'nin politika ve çalışmalarında dijital ve fizikseli ayrı ayrı ele almamış ve birlikte yürütülmeye çalışılmakta olduğu gözlemlenmiştir.

5.3. Amerika Birleşik Devletleri–ABD Milli Arşivi/The National Archives and Records Administration (NARA)

ABD farklı eyaletlerden oluşan bir yapıya sahip olmasından dolayı çalışmalar farklı kurumlar tarafından yapılmıştır. İncelenen çoğu çalışmanın dijital belgelerin arşivlere transferinden ziyade dijitalleştirme projelerine ait olduğu gözlemlenmiştir. Çalışmamız odak grubu olan dijital belgelerin arşive transferi kapsamında ABD'de dijital belgelerin transfer edileceği arşiv ABD Milli Arşivi/The National Archives and Records Administration (NARA)'dır. NARA'nın bu konudaki yaptığı çalışmalara bakacak olduğumuzda; ilk olarak bu arşivin düzenli aralıklara güncellediği bir "Stratejik Plan"'ı bulunmaktadır. 2018 yılında yayımlanan bu plan önlerindeki birkaç yıl için hedeflerini ve bu hedeflere ulaşmak için kullanacakları stratejileri, ilerlemelerinde değerlendireceği önlemleri içermektedir (*2018–2022 Strategic Plan, 2018*).

NARA 2017 yılından Dijital Koruma Stratejisi'ni yayımlamıştır. Yine bu strateji sonrasında güncellenerek Dijital Koruma Stratejisi 2010-2022 yayımlanmıştır. Bu strateji, dijital korumada kullanılacak özel stratejilerini özetlemekte ve özellikle altyapı,

biçim, medya sürdürülebilirliği ve standartları, veri bütünlüğü ve bilgi güvenliği konularını ele almaktadır. Altyapı bölümünde, dijital koruma altyapısı (donanım, yazılım, ağlar, depolama, ilgili ekipman ve bilgi teknolojisi hizmetlerini geliştirmek, test etmek, işletmek, izlemek, yönetmek, desteklemek için kullanılan yöntemler) şunları içerir: doğuştan dijital belgelerin sisteme alınması, işlenmesi, aktif dosya yönetimi ve korunması için sistemler ve araçlar, eski dijital dosyalar ve dijital taşıyıcılar için uygun fiyatlı, yönetilen, çoğaltılan içerik depolama altyapısı, NARA doğumlu dijital dosyaları ve dijital taşıyıcıların alınması veya oluşturulması, işlenmesi, aktif dosya yönetimi ve korunması için sistemler ve araçlar'dır (*Preservation Strategy 2019- 2022*, 2019).

NARA elektronik belgelerin NARA'ya transferi için iki rehber yayımlanmıştır. Bunlar; 2014-04 Rehberi ve 2015-04 Rehberi'dir. NARA elektronik belgeleri transfer etmeden önce hangi adımları atacağına 2014-04 Rehberi'nde yer vermiştir. 2014-04 Rehberi (2018 yılında güncellenmiştir), Elektronik Belgelerin Transferi için Revize Format Rehberi (elektronik belgeleri NARA'ya transfer ederken hangi dosya biçimlerinin kabul edilebilir olduğunu belirtir). Bu rehberde göre elektronik belgeleri aktarmadan önce; geçici belgelerin kalıcı elektronik belgelerden ayırma işlemi, elektronik belgelerin aktarılmadan önce hassasiyet değerlendirilmesi işleminin yapılması, elektronik belgeleri NARA'ya aktarmak için kullanılan fiziksel medyanın şifrlenmesine ilişkin kurallara uymak, adımlarının izlenmesi gerektiği belirtilmiştir (*NARA Bulletin 2014-04: Format Guidance for the Transfer of Permanent Electronic Records*, 2014). 2015-04 Rehberi, Elektronik Belgelerin Transferi için Üst veri Rehberi (elektronik belgeleri NARA'ya transfer ederken üst veri öğelerini tanımlamaya rehberlik eder) konularına yer verir. Üst veriler, elektronik belgelerle ilgili "kim, ne, nerede, ne zaman ve neden" sorularını yanıtlayan bilgi unsurlarıdır. Üst veri öğeleri, elektronik belgelerin yapısını ve içeriğini açıklayan yönetimsel, açıklayıcı ve teknik bilgiler sağlar. Üst veri öğeleri, elektronik belgelerin NARA'ya aktarılmadan önce nasıl oluşturulduğunu, kullanıldığını, yönetildiğini ve saklandığını ve bunların diğer belgelerle nasıl ilişkili olduğunu açıklayan bağlamsal bilgiler de sağlar. Bu bilgiler, NARA'nın elektronik belgeleri gerektiği kadar yönetmesini, korumasını ve bunlara erişim sağlamasını sağlar (*Bulletin 2015-04: Metadata Guidance for the Transfer of Permanent Electronic Records*, 2015).

2019 yılında ABD Hükümeti'nin NARA'ya gönderdiği "elektronik belgeye geçiş" başlıklı yazı ile bazı kararlar NARA'ya bildirilmiştir. Yazıda bulunan ilgili önemli kararlar; 2022 yılının sonuna kadar kâğıt belge transferi kabul edilecek, 2023 yılının

başından itibaren ise artık kâğıt belge transferi hiçbir şekilde kabul edilmeyecek ve tüm işlemler elektronik olarak yapılacaktır. Henüz transfer edilemeyen fiziksel belgeler ise dijitalleştirilerek transfer edilecek (*Transition to Electronic Records*, 2019).

5.4. Fransa-Fransa Milli Arşivi/France National Archives

Fransa Milli Arşivi Paris’te bulunan dünyanın sayılı zengin arşivleri arasında yer almaktadır. Milli Arşiv web sitesinde “dijital arşivler ve veri” adlı ayrı bir bölüm bulunmaktadır. Bu bölümde dijital verilerin arşivlenmesi üzerine durulmaktadır. Dijital verilerin arşivlenmesi şunları içermektedir: üretim uygulama ortamlarının teknolojik geçmişinin, biçimlerinin ve desteklerinin ötesinde, zaman içinde anlaşılır ve kullanılabilir olmalarını sağlamak, bütünlüklerini garanti etmek (içeriklerinin eksiksiz olması), özgünlüklerini garantilemek (içeriklerinin değiştirilmemiş olması veya değişikliklerin izlenmesi).

Fransa Milli Arşivi şu anda 200 milyon dijital dosya bulundurmaktadır. Fransa Milli Arşivi’nde 35 yıllık elektronik ve görsel işitsel verileri bünyesinde barındırır ve dolayısı ile milli hafızaya oldukça önem vermektedir (*L’archivage numérique aux Archives nationales*, 2020, 5 Mayıs). Bu kapsamda “ADAMANT: Gelecek için bir proje” çalışması başlatılmıştır. Fransız hükümeti, devlet idareleri vb. kurum ve kuruluşlar tarafından oluşturulan dijital bilgi ve belgelerin sayısı ve boyutu fazlaştı ve bunları yönetmek zorlaştı, dolayısı ile bu belgelerin zamanla bozulmasını önlemek, uzun vadede korunmasını sağlamak ve yeniden erişilebilir olması amacı ile bu proje başlamıştır (*ADAMANT: A project for the future*, 2018). Fransa Milli Arşivi’nin konu ile ilgili dijital belgelerle ilgili yapmış olduğu bir çalışma ya da yayımladığı bir politika bulunmamaktadır. Fransa Milli Arşivi henüz dijital transfere başlamamıştır fakat elektronik belgelerin uzun vadeli koruma ile ilgili çalışmaları bulunmaktadır.

5.5. Yeni Zelanda–Yeni Zelanda Milli Arşivi/Archives New Zealand

Yeni Zelanda’da 2003 tarihli yasa (National Library of New Zealand Act 2003) ile birlikte web siteleri kamuya açık belge haline getirilmiştir ve web sitelerini olağanüstü durumlara karşı nasıl yönettiklerine dair sorunlar bulunmaktadır. Kamu Belge Kanun’una göre belgeler 25 yılını tamamlayınca Milli Arşive aktarılacak zorundadır (Public Records Act 2005, 2017). Yeni Zelanda Milli Arşivi, Yeni Zelanda Milli Kütüphanesi ile birlikte eşgüdümlü bir Dijital Koruma Politikası ve Stratejisi oluşturup, yayımlamışlardır. Dijital Koruma Politikası’nda tüm süreçlerin birbirileri ilişkileri bir diyagramda gösterilmiş ve ayrıntılı olarak ele alınmıştır. Bu süreçleri şu şekilde belirtmek faydalı olacaktır:

- Dijital içeriğin (ingest) içeri alınması (ön hazırlık, virüs taraması, teknik analiz, format kullanımı aşamaları ile bağlantılı),
- Dijital içeriğin bütünsel olması (ön hazırlık, dosya sabitliği, kabul edilebilir değişiklikler aşamaları ile bağlantılı),
- Dijital içerik erişilebilir olması (içeriğe erişim için teknik hususlar aşaması ile bağlantılı),
- Dijital içeriğin depolanması (güvenlik, yedekleme, olağanüstü durum kurtarma, temsil deposu aşamaları ile bağlantılı),
- Dijital içeriğin yönetilebilir olması (format kütüphanesi kullanımı, risk yönetimi, koruma uygulaması, silme, temsil aşamaları ile bağlantılı)'dır (*Digital Preservation Policy Manual* 2012, s. 8).

Aynı zamanda Yeni Zelanda Milli Arşivi, kamu kurumlarının dijital ortamlarını tanımlamak ve sürdürmek ve uzun vadeli değerini korumak için politika ve eylemler geliştirmelerine yardımcı olacak “Dijital Süreklilik Eylem Plan”ını 2009 yılında başlatmıştır (*Digital Continuity Action Plan*, 2009).

Yeni Zelanda Milli Arşivi dijital belgelerin transferini beş aşamaya ayırmıştır. Bunlar;

- transfer girişimi (Kurumların dijital transfer yapıp yapamayacağı belirlenir, kurumlarla görüşmeler başlar. Fazla kopyaların belirlenmesi, belgelerin açık erişim olarak yüklenmesi (hassas belgeler hariç), aktarımı yapılacak içeriğin boyutu, üst veri ve dosya formatları belirlenmesi),
- transferi planlama (kurumun transferin belirlenip planlanması için arşivde transfer sürecinde görevli bir personelle iş birliği yapması, kurum ve personelin bir Transfer Yönetim Planı Anlaşmasını kabul ederek roller ve sorumluluklar üzerinde anlaşması),
- transfer hazırlığı (arşive transfer yapılmadan önce koleksiyonun değerlendirilmesi, dosyaları tanımlamak için analiz etmek, hangi üst verilerin gerekli olduğunu belirlemek),
- transfer (belgelerin sisteme aktarılması, aktarıldıktan sonra ilgili kuruma bilgi verilmesi),
- transfer sonrası (aktarılan belgeleri çevrimiçi bulma yardımımız 'Archway' ile kamuya açık hale getirmek için içeriksel bilgilerinin yayımlanması, aktarım gerçekleştiği Archway'de bulunur hale geldiğinin kamu ile paylaşılması) 'dır.

Dijital transfer için transfer yapacak kurumdan bir sorumlu atanmalı ve küçük bir ekip oluşturulmalı, bu ekipte bilgi ve belge yönetiminden anlayan ve teknik bilgiye sahip personel bulunmalıdır. Yeni Zelanda Milli Arşivi fiziksel ve dijital belgelerin transferi aşamasındaki birçok işlemin benzer olduğunu belirtmiştir. Fakat dijital transferin de fiziksel transfere benzemeyen bir yapıya sahip olduğu ve transfere başlamadan önce bazı analizler yapmak gerekliliği belirtilmiştir (*Digital transfer - overview*, 2018). Yeni Zelanda Milli Arşivi 2016 yılında Sivil Havacılık Örgütü ile birlikte ilk dijital transfer işlemini (vaka çalışması) başarı ile gerçekleştirirler (*Digital transfer case study*, 2017). Sonrasında ise gerçek bir dijital transfer için gerekli olabilecek her aşama için planlama ve uygulama yapmayı, diğer kurumlarla iş birliğine gitmeyi ve kendilerini geliştirmeyi hedeflerler ve çalışmalarını tamamlayıp tam anlamıyla dijital transfere başlanır ve yine devam eden süreçte hala kendilerini geliştirmeyi hedef alırlar. Tüm bu süreçlerin içinde dijital transferin dijital süreklilik ile de bağlantılı olarak yürütülmesine önem gösterirler. Yeni Zelanda Milli Arşivi dijital belgelerin transferini yaparken dosya formatlarını sınırlandırmazlar ve bütün dosya formatlarını kabul ederler. Belgelerin uzun vadeli koruması için ExLibris'in uzun vadeli koruma sistemi olan Rosetta⁴⁰'yı kullanır. Transfer için dosya format tanımlamasında Rosetta, İngiliz Milli Arşivleri tarafından sağlanan DROID'i ve PRONOM'u kullanır. Belgeleri orijinal biçimlerinde (EBYS'de bulunan halleri ile) koruyarak aktarmaya özen gösterirler (*File formats for digital transfers*, 2018). Yeni Zelanda Milli Arşiv'nin dijital transfer sırasında önemseydiği diğer bir konu ise, dosyaların bütünlüğüdür. Bunun için ise "checksum" olarak ifade edilen dosyanın orijinal ve hatasız olmasını sağlayan, bir veri parçasında genellikle tek bir dosyada, kriptografik sağlama işlevi adı verilen bir algoritmanın çalışması ile oluşan bir sağlama toplamıdır (*The importance of checksums*, 2017). Yeni Zelanda Milli Arşivi'nin önemseydiği diğer bir konu ise dijital hassasiyet değerlendirmesi kavramıdır. Milli Arşive göre dijital belgelerin bu aşaması transfer sırasında Milli Arşiv tarafından değil öncesinde kurum tarafından yapılmalı ve hazır bir şekilde transfer sırasında ilgili yetkililere bildirilmelidir. Yüksek riskli bilgi ve belgeler, kurumların çalışma şeklini, ticari işlemlerini, müşterilerini, çalışanlarını vb. riske atacak bilgi ve belgeler olabilir. Kötü yönetilen riskler kurumu büyük bir itibar kaybına, maddi ve manevi zarara ve yasal yükümlülük

⁴⁰ Rosetta; yeni, eski herhangi bir dosya biçimini yönetebilen, Açık Arşiv Bilgi Sistem Referans Modeline (ISO 14721: 2021) dayanan bir koruma sistemidir. Detaylı bilgi için bakınız <https://archives.govt.nz/manage-information/resources-and-guides/transfer/file-formats-for-digital-transfers>

ihlaline maruz bırakabilir. Bu sebeple kurum ve kuruluşlar bu süreçlerde bir plana sahip olmalı, varlık yönetimi için uzun vadeli bir strateji sağlamalıdır (High value and high risk, 2016).

Yeni Zelanda Milli Arşivi, dijital belgelerin değerlendirme süreci ile ilgili adımları şu şekilde belirtmiştir; değerlendirme, kararların etkinleştirilmesi ile ilgilidir. Bir kurumun işlevlerinin ve faaliyetlerinin değerlendirilmesini, bilgi ve belgelerinin oluşturulması ve yönetimi ile ilişkili risklerin değerlendirilmesiyle birleştiren analiz sürecidir. Bunu yapmak için, zaman içinde uygun yönetimini, saklama sürelerinin ne olduğunu ve elden çıkarma eylemlerini belirlemek için kuruluşun bilgi ve belgelerine bakmanız gerekir. Değerlendirme, bilgi ve belge yönetiminin proaktif bir bileşenidir. Değerlendirme erken yapıldığında, zamanında elden çıkarılmalarını ve faydalarını en üst düzeye çıkararak bilgi ve belgelerin tüm yaşamları boyunca yönetimini iyileştirmek mümkündür. Ayrıca belgelerin uygunsuz bir şekilde yönetilmesi veya imha edilmesi riskini de azaltır. Bilgi ve belgeleri değerlendirmenin yararları şu şekildedir;

- Kurum, acil ve sürekli iş ihtiyaçları için yüksek riskli, yüksek değerli veya her ikisi birden olan bilgi ve belgeleri tanımlayabilir ve yönetebilir.
- Kurum kaynakları verimli bir şekilde kullanabilir.
- Kurum bilgi ve belgeleri kolayca bulabilir, alabilir ve kullanabilir.
- Kurum kalıcı bilgi için hangi bilgi ve belgelerin arşiv değeri olduğunu anlayabilir (Appraisal process, 2020)

Belgeler ne zaman değerlendirilmelidir?

- Belgeler oluşturulmadan önce ve iş süreçlerinin tasarımı sırasında,
- kullanım ömürleri boyunca doğru bir şekilde yönetilmelerini sağlamak için belgeler oluşturulduğunda,
- amaçların ulaşmış belgeler için geriye dönük olarak,
- bir kamu dairesi bir bertaraf makamı oluşturduğunda veya değiştirdiğinde,
- idari bir değişiklik veya işlev aktarımı gerçekleştiğinde,
- yerel makam korumalı belgeleri elden çıkarmak istediğinde (Appraisal process, 2020).

Yeni Zelanda Milli Arşivi'ne göre belgelerin değerlendirilmesi şu şekildedir:

Değerlendirme kararları, bir kuruluşun fonksiyonları ve bu fonksiyonları destekleyen belge yönetimi süreçleri hakkındaki bilgilere dayanarak verilir. Belirlenen unsurlar değerlendirme aşamasına yardımcı olacak unsurlardır. Bunlar; mevzuat, yönetmelikler, standartlar, uygulama kuralları, yıllık raporlar, niyet beyanları gibi kurumsal belgeler, ticari faaliyetler hakkında bilgi sahibi olan dâhili personel ile görüşmeler, mevcut değerlendirme raporları, mevcut işletme sınıflandırma şemaları veya sınıflandırma bilgilerini topladıktan sonra, gerçekleşen iş faaliyetlerini ve bunların ilişkili belgelerini gruplar veya sınıflar halinde organize etmek ve tanımlamak gerekir (*Appraisal process*, 2020).

Seçim/ayıklama; bilgi yönetimi içinde elden çıkarma, bir kurumun bilgi ve belgelerini tutup tutamayacağına, aktaracağına veya yok edeceğine karar veren karar verme sürecini içerir. Yeni Zelanda Milli Arşivi'ne göre ayıklamanın faydaları şu şekildedir:

- belge ve bilgi depolama maliyetlerinde azalma,
 - daha iyi kayıt kontrolü ve sistem etkinliği sayesinde kazanılan sistem verimliliğini artırmak,
 - bilgilere ve belgelere yasa dışı erişimi veya tahribatı en aza indirerek gizlilik ve güvenlik ihlallerinin azaltılması riski,
 - gelişmiş bilgi ve belge yönetimi,
 - kamu kurumlarının bilgilerinin şeffaflığının ve hesap verebilirliğinin artırılması
- (*Disposal process*, 6 Haziran 2020).

5.6. Hollanda–Hollanda Milli Arşivi/ Netherlands National Archives

Hollanda Milli Arşiv⁴¹'i incelendiğinde, ülkenin henüz dijital belge transferi aşamasına geçmediği görülmektedir. Hollanda milli arşivinin bir dijital koruma politikası bulunmaktadır. Bunun yanı sıra Milli Arşivin şu anki durumu elektronik belgelerin nasıl korunacağına ilişkin çalışmalarla devam etmektedir.

5.7. Macaristan-Macaristan Milli Arşivi/Hungarian National Archives

Macaristan Milli Arşivi⁴²'ni dijital transfer bağlamında incelediğimizde kurumların henüz dijital transfer aşamasına geçmediğini görmekteyiz. Macaristan Milli

⁴¹Hollanda Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <https://www.nationaalarchief.nl/en>

⁴²Macaristan Milli Arşivi'nin ilgili çalışmalarına bu bağlantıdan erişebilirsiniz. Erişim adresi: <https://mnl.gov.hu/angol>

Arşivi'nin sitesinde konu ile ilgili sadece elektronik belgelerin arşive transferi adlı bir excell dosyasından başka bir veriye rastlanamamıştır.

5.8. İsviçre-İsviçre Federal Arşivi/Swiss Federal Archives

İsviçre Federal Arşivi İsviçre'nin milli arşividir. İsviçre Milli Arşivi öncelikle tüm görev ve yetki hâkimiyetlerinde İsviçre Federal Arşiv Yasası (Federal Act on Archiving (Archiving Act, ArchA), 1998)'na bağlı olarak hareket eder. Bu yasa en son 2013'te güncellenmiştir. 1992'de yayımlanıp 2019'da güncellenen bir Veri Koruma Politikaları mevcuttur.

İsviçre Federal Arşivi 2016-2020 stratejisi yayımlamışlardır. Bu strateji; dijital dönüşümden dolayı arşivlerin de dönüşüm geçirmesi ve çağı yakalamak, dijital arşivleme süreçlerini geliştirmeyi amaçlamaktadır. Stratejinin odak noktası, dijital bir depo oluşturmaktan koruma ve transfer için dijital arşivleme süreçlerini geliştirmekten çevrimiçi erişimi genişletmeye kaydırmaktır (*Federal Archives Strategy 2016 - 2020*, 2015).

İsviçre Federal Arşivi 2019 yılında bir dijital arşiv politikası yayımlamıştır. Bu politikada hem dijital belgelerin dijital formda arşive aktarılacağından, fiziksel belgelerin ise sayısallaştırılarak arşive aktarılacağından bahsedilmektedir. Politikada, dijital belgeler için kabul ettikleri “arşivlenebilir belge formatları”ndan bahsedilmektedir. Belgelerin arşive devredilmeden önce kabul edilen dosya formatlarında olması devredecek kurumun sorumluluğuna bırakılmıştır. Politika, dijital belgelerin değerlendirmesi ile ilgili konunun transfer işlemi yapacak kurum ve İsviçre Federal Arşivi arasında ortak görevi olması gerektiğini belirtmiştir. Değerlendirme bu nedenle her zaman bu iki taraf arasındaki yakın iş birliğinin sonucudur. Dijital belgeler ile ilgili olarak, belge gönderen kurumun teknik yönetimi ile ilgili bilgi birikimi uygulamaların yanı sıra veritabanlarının içeriği de büyük önem taşımaktadır. Bu bilgi birikimi, belgelerin yasal, idari ve tarihsel değerinin belirlenmesi yardımcı olmaktadır. Dijital belge transfer edecek kurum İsviçre Federal Arşivi'ne aşağıdaki unsurlara uyacak şekilde kendini hazırlamalıdır:

- Birincil verilerin ve üst verilerin sağlanması (birincil veriler, doğrudan çekirdek (yönetim) faaliyetleri sırasında üretilen belgelerken, üst veriler «birincil veriler hakkında bilgi», yani birincil verileri daha ayrıntılı olarak tanımlayan bilgiler),
- dosyaları arşivlenebilir dosya formatlarına dönüştürme,

- İsviçre Federal Arşivi'nin gerekliliklerine uygun bir SIP (Gönderim Bilgi Paketi) oluşturmak (*Digital Archiving Policy*, 2019).

Politika genel olarak bir dijital arşivde neler olması ve süreçlerin nasıl ilerlemesi gerektiğinden bahsetmiş olsa da teknik kısımlar ya da süreçlerin nasıl ilerleyeceğine ilişkin açıklamalı bilgilere yer vermemiştir.

İsviçre Federal Arşivleri henüz dijital transfer sürecine başlamamış, bunun için gerekli olan adımların başında yer almakta ve çalışmalarına devam etmektedir.

5.9. Estonya–Estonya Milli Arşivi/ The National Archives of Estonia

Estonya Milli Arşivi, Estonya'daki arşiv yönetiminin merkezidir ve bölümleri Tallinn, Tartu, Rakvere ve Valga'da bulunmaktadır. Estonya Milli Arşivi, Eğitim ve Araştırma Bakanlığı alanında *Arşiv Yasası* ve arşiv kuralları temelinde hareket eden bir devlet kurumudur (The National Archives of Estonia, 2020). Estonya Milli Arşivi, dijital belgelerin arşivlere transferi çalışmalarının başlarındadırlar. Estonya Milli Arşivi, uzun süreli korumaya dikkat ederek ve farklı araçlar kullanılarak bu işlemin yapılabilceğini savunur. Bu işlemler için kendilerinin oluşturdukları ve kullandıkları ve “Evrensel Arşiv Modülü” bulunmaktadır. Bu modül; Milli Arşivler tarafından elektronik belge yönetim sistemlerinden çıkarılan dijital belgelerin hazırlanması ve aktarılması için oluşturulmuş bir yazılımdır. Modül, bir kurumun EBYS'sinin belgelerini ve üst verileri XML biçiminde dışa aktarması ile çalışır. Bu modül birçok emek yoğun işi otomatikleştirerek kolaylaştırmayı sağlar. Bunlar; arşivlerin açıklayıcı hiyerarşisini manuel olarak derlemek ve tekrar tekrar kullanmak; arşiv işlemleri için elektronik belge yönetim sisteminden ayrılmış verileri almak, manuel ve otomatik olarak bir açıklama hiyerarşisi oluşturmak için içe aktarılan verileri kullanmak, tanımlama seviyelerini ve hiyerarşisini işlemek, üst verilerin toplanmasını otomatikleştirmek, zorunlu üst verilerin varlığını otomatik olarak kontrol etmek, çeşitli raporları otomatik olarak derlemek, arşiv şemasının düzenliliğini doğrulamak, dosya formatlarını kontrol etmektir (*The universal archiving module (UAM)*, 2020, 6 Mayıs). Estonya'da arşiv değeri oluşturan kurumlar, tüm belgelerini oluşturulduktan 10 yıl sonra Estonya Milli Arşivi'ne aktarmak zorundadır. Fakat Estonya Milli Arşivi şu an dijital arşiv oluşturma, dijital belgeleri arşivleme, uzun süreli koruma, belgeler için format belirleme aşamalarındadır. Henüz dijital belge transfer aşamasına ulaşmamışlardır. Estonya Milli Arşivi Arşiv Yasa'sına göre değerlendirme işleminde şu unsurlara dikkat ederler:

- kamu otoritesini kullanma ihtiyacı,
- kişilerin haklarını ve işlemlerini onaylama gereği,
- bilginin kültürel ve tarihsel değeri.

Ayıklama ile ilgili olarak kişiler, arşiv belgelerinin belirlenmesinden önce belgeleri imha etmeyecektir. Arşiv belgelerinin arşiv değerinin iptaline devlet arşivcisi tarafından karar verilir (Archives Act, 2012).

Estonya Milli Arşivi 2008 yılında “Dijital belgeleri arşivleme gereksinimleri” adlı bir kılavuz hazırlamıştır. Bu kılavuzun amacı; dijital arşiv materyallerinin toplanması, otantik bir formda kullanılması, uzun süreli korunması için temel gereklilikleri oluşturmaktır. Aynı zamanda dijital belgelerin ve bunların üst verilerinin ayrılması, elektronik belge yönetim sistemleri (ERMS) ve bunların kamuya transferi ile ilgilidir. Dijital belgeler dijital yönetimin doğal bir parçası olarak arşivlenmelidir. Dijital belgeleri arşivlerken, yapılan işin büyük bir bölümünü bilgi teknolojisi aracılığıyla otomatikleştirmek mümkündür.

Kurumun belge yönetim sistemindeki üst verilerin çeşitli amaçları vardır. Üst verilerin aşağıdaki dağılımı:

- belgeleri tanımlayan üst veriler;
- politikaları veya yetkileri tanımlayan üst veriler;
- kişileri tanımlayan üst veriler;
- faaliyetleri ve süreçleri tanımlayan üst veriler;
- belge yönetimi süreçlerini açıklayan üst veriler.

Dijital belgeleri arşivlerken, ana belgelerin uzun vadeli kullanılabilirlik riskleri teknolojik risklerden kaynaklanmaktadır. Buna göre ayrıca milli arşivler tarafından kullanılan uzun vadeli depolama ve sürekli dosya takibi çözümüne dayanmaktadır. Milli arşiv tarafından arşive transfer sürecinde uygun bulunan bir takım dosya formatları bulunmaktadır (*Digitaaldokumentide arhiveerimise nõuded/Dijital belgeleri arşivleme gereksinimleri*, 2008).

Estonya Milli Arşivi, 2005 yılında “Dijital Arşivleme Stratejisi” yayımlamışlardır. Bu strateji milli arşivde dijital materyalin değerlendirilmesi, kabulü, depolanması ve kullanımı ve dijital belgelerin doğru yönetilmesine, tanımlanmasına, arşivlenmesine ve korunmasına katkıda bulunarak entelektüel ve teknolojik hazır

bulunmayı amaçlamaktadır. Estonya Milli Arşivi belge yapısında dijital arşivin OAIS (Açık Arşiv Bilgi Sistemi) modeline kullanmaktadır.

Dijital belgelerin açıklamasını oluşturan verilere genellikle üst veri denir. Arşivin iç yapısının ve arşivin yaratıcısının daha yüksek seviyeleri kendisi de belgelerle aynı şekilde tanımlanmalıdır. Milli arşivin faaliyetleri açısından dijital belgelerin arşivlere alınabilmesi için şu anda kurumlarda oluşturulan üst verilerin bileşimi yetersizdir. Üst verilerde yer alan bilgiler, belgenin orijinallliğini, güvenilirliğini, bütünlüğünü ve kullanılabilirliğini koruyup korumadığını belgeler üzerinde yapılan işlemleri izlemeye ve karar vermeye olanak tanır. Üst verileri standartlaştırmak gerekir. Dijital belgeler mevcut arşiv yasasına göre ayıklama ve değerlendirme işlemine tabi tutulurlar. Yeterli üst verinin oluşturulmaması, operasyonel içeriğin kaybolması ve değiştirilmesi riskinden dolayı dijital belgeyi anlamak ve gelecekte kullanmak imkânsız olacaktır. Dijital belgeler hayatlarının mümkün olan en erken aşamasında değerlendirilmelidir. Arşivci için dijital belgelerin ne olduğu ve ne olacağı erken bir aşamada açık bir şekilde belirlenmelidir. Dijital belgeleri öncelikle ön değerlendirme sürecine almak gerekir. Ön değerlendirme aşamasında değerlendirilecek belgeler arasından bir örneklem seçilip onun üstünde denemeler yapılır. Dijital belgelerin milli arşive transferi aşamasında değerlendirilmesi büyük ölçüde teknik bir faaliyettir. Dijital belgelerin değerlendirilmesi sırasında aşağıdakiler yapılmalıdır:

- belge yönetimi için kullanılan formatları değerlendirir,
- kullanılabilirliğe dikkat edilmelidir,
- format uyumluluğu, dijital arşivlerin kamu arşivlerine aktarılması gereksinimlerde belirtilen arşivlenebilir biçimlerle,
- verilerin kullanım ortamına bağımlılığını (bağlam) değerlendirmek,
- yazılım ve arşiv dostu bir formata,
- teknik özelliklerin otomatik olarak ayrılması olasılıklarını değerlendirmek.

Dijital belgeleri tanımlayıp değerlendirdikten sonra arşive aktarma süreci başlar.

Milli arşivler, aktarılan dijital materyalin korunması için formatların değiştirilmesi ve gerekirse güncellenmesine kadar periyodik bir depolama ortamı planlamaktadır. Estonya Milli Arşivi dijital koruma yöntemini geliştirirken, teknolojik gelişmeleri yakından takip etmek, diğer arşivlerin bu konuda neler yaptıklarını takip etmek, dijital materyalin ve ilgili bir metodolojinin korunması için bir zaman çizelgesi

geliştirmek vb. gibi unsurlara dikkat etmektedir. Dijital materyalin kullanılabilirliğini sağlamak için arşivlerde yer alan bilgilerin bütünsel ve bağlamsal olarak özgün tutulması gerekmektedir. Bu amaçla, teknolojik gelişimin farklı aşamalarında önemli adımlar atılmalıdır (*Dijital Arşivleme Stratejisi 2005-2010*, 2005).

5.10. İrlanda –İrlanda Milli Arşivi/National Archives of Ireland

İrlanda Milli Arşivi'nin sahip olduğu bir “Milli Arşiv Yasası (1986)” ve “Arşiv Yönetmeliği (1988)” bulunmaktadır. Arşiv ile ilgili yapılacak tüm faaliyetler ve düzenlemeler bu yasal mevzuata bağlıdır. Yasa'ya göre 30 yılını geçmiş ilgili belgeler milli arşive devredilmelidir. Devretme sorumluluğunda olan kurum ise Dışişleri Bakanlığı olarak belirlenmiştir. Bu kurum, ilgili belgelerin düzenlenmesi, numaralandırılması, temizlenmesi, paketlenmesi vb. işlerden ve ayrıca tüm belgelerin milli arşive güvenli bir şekilde taşınmasından sorumlu tutulmuştur (*Responsibilities under legislation*, 2020, 7 Mayıs). İrlanda Milli Arşivi henüz dijital transfer aşamasına gelmemiştir. Şu an milli arşivin bir dijital koruma politikası, dijital belgeler için bir çalışması bulunmamaktadır. Arşiv hali hazırda fiziksel arşiv transfer süreçleri ile ilgilenmektedir.

Kuzey İrlanda Kamu Kayıt Ofisi DPC (Digital Preservation Coalition) üyesidir.

İrlanda Milli Arşivi'nin temel misyonu, İrlanda'nın kamuya açık belgelerini toplamak, yönetmek, korumak, araştırma kaynağı olarak uzun vadeli kullanılabilirliğini sağlamak ve vatandaşların haklarını desteklemektir. Kamu belgelerinin uzun vadede ulaşılabilirliği, demokratik süreçte şeffaflığı ve hesap verebilirliği göstermektedir.

5.11. İskoçya–İskoçya Milli Arşivi/ National Records of Scotland (NRS)

İskoçya Milli Arşivi 2014 yılında Dijital Koruma Stratejisi'ni yayımlamıştır. Bu strateji doğuştan dijital belgeler odaklıdır. Belge transferlerinin kapsamını olabildiğince iyi yönetebilmek için İskoçya Milli Arşivi belge yaratıcıları ile iyi ilişkiler kurmaya çalışmaktadır (*The Digital Preservation Strategy*, 2014). İskoçya Milli Arşivi, transfer yapacak kurumun hangi belge sistemlerini kullandıklarını dikkate almak, hangi biçimlerin ve üst verilerin dolaşımda olduğunu saptamak, bu belgelerden kaç tanesinin kendilerine aktarılmasının muhtemel olduğunu, bunların ne zaman alacağını tanımlanması ve bunlardan kaç tanesinin hassas veya kişisel bilgi içerdiğinin değerlendirilmesi unsurlarını planlayıp yönetmektedir.

İskoçya Milli Arşivi'nde dijital transfer henüz başlamasa da altyapısı bulunmaktadır. Bu altyapı henüz geçici depolama olarak oluşturulmuşsa olsa da uzun vadeli dijital bilgi toplama çözümü üzerindeki çalışmaları devam etmektedir. Ayrıca dijital koruma stratejisinde dijital süreklilik terimi kullanılmamış olsa bile bu dokümanda format vb. gereksinimlerden bahsedilmekte ve bu unsurlar dijital süreklilikle bağlantılıdır (*The Digital Preservation Strategy*, 2014).

İskoçya Milli Arşivinin iş birliği yaptığı birtakım proje, kurum, kuruluş bulunmaktadır. Bunlar; Dijital Koruma Koalisyonu (DPC)'na üyedir, Glasgow Üniversitesi ile ortaklaşa belgelerin hassasiyet değerlendirmesi projesi, Avrupa Arşiv Grubuna üyelik ve iş birliği, uluslararası arşiv konseyi üyesi ve iş birliği bunlardan bazılarıdır.

İskoçya Milli Arşivi dijital koruma stratejisinin anahtar prensipleri şunlardır:

- önleyici harcama,
- cimri koruma - anlamsız süreçlerin önlenmesi,
- belge yakalamanın ve seçimin/ayıklanmasının önemi,
- ölçeklenebilirlik,
- açıklık,
- daha geniş uygulanabilirlik,
- yeterli ve yetkin personel,
- otantiklik (*The Digital Preservation Strategy*, 2014).

5.12. Danimarka–Danimarka Milli Arşivi/The Danish National Archives

Danimarka Milli Arşivi'nin yapmış olduğu tüm çalışmaların yasal altyapısını sahip olduğu Danimarka Arşiv Kanunu oluşturmaktadır.

1973'ten beri, Danimarka Milli Arşivi herkese açık dijital belgeleri almıştır. Başlangıçta, Danimarka Milli Arşivi sadece elektronik veri tabanlarını kabul etmiş, ancak 1980'lerden itibaren elektronik dosyalama sistemleri de kabul etmiştir. 1990'ların sonunda, elektronik belge yönetim sistemlerini de almak mümkün oldu. Eski dijital belgeler çok sayıda format ve yapıda mevcuttur. Bunun nedeni, 1990'ların sonunda, dijital arşivleme için mevcut koruma standartları yeterli değildi. Makine tarafından okunabilen bir formatta herhangi bir format veya yapı açıklaması yoktur. 1980'lerin sonuna kadar, yapı için kapsamlı bir gereklilik yoktu ya da gönderilen dijital belgelerin formatı veya bunun nasıl olması gerektiğine dair belgelenmiş herhangi bir yönerge yoktu. Bu nedenle,

tüm dijital belgelerin koruma standardına geçirilmesine karar verilmiştir. Standart, hangi veri yapısının ve formatlarının saklanması gerektiği tanımlar.

Dijital belgeler farklı güvenlik açıklarına sahiptir ve fiziksel belgelere göre farklı zorluklar getirmektedir. Medya verilerin saklandığı veriler bozulabilir ve okuyabilmek için gereken teknoloji medya eskimiş olabilir. Aynı şekilde, dijital belgelerin tutulduğu formatlar kullanılamaz hale gelir ve verilerin ve bağlamının nasıl yorumlanacağı bilgisi kaybolabilir. Dijitalin korunması uzun vadeli bilgi, yöntem, teknoloji ve dokümantasyon açısından onu yeniden kullanılabilir hale getirecek şekilde, bazı kasıtlı seçimlerin yapılmasını gerektirir (*Strategy for archiving digital records at the Danish National Archives* 2013).

Danimarka Milli Arşivi, gelecekteki dijital arşiv materyallerinin korunmasına yönelik strateji ve yöntemler geliştirmekle sorumludur. Danimarka dosya arşivlerinin uzun süreli korunması için Danimarka Milli Arşivi tarafından bir dönüşüm stratejisi geliştirilmiştir. Dönüşüm, verilerin (uygulamalarla değil) mevcut teknolojiyle sürekli olarak uyumlu olmasını sağlamak için uygun aralıklarla taşındığı anlamına gelir. Bu nedenle devlet arşivlerine gönderilen elektronik arşiv materyalleri, önemli veri kaybı olmadan sürekli dönüşümler için uygun formatlara veri dönüşümü sağlayacak şekilde saklanmaktadır.

Yetkililer tarafından kullanılan elektronik dosyalama sistemleri ile ilgili tek gereklilik söz konusu makamların Danimarka Milli Arşivi tarafından kullanılan dosyalama biçimine nasıl ve ne zaman dönüştürmeyi planladıklarını; şu anda kullandıkları biçimler ve kelime işlemci sistemlerinin değişmesinden kaynaklanan sorunları çözmeyi amaçladıkları yöntem bir dosyalama versiyonunun gerekli formatlarda çoğaltılabilmesini sağlamaktır.

Danimarka Milli Arşivi tarafından elektronik dosyalama sistemlerinin aktarılması için belirlenen teknik gereklilikler, sistemden bağımsız dosyalama sürümlerine dönüştürülebilirlik sağlamayı amaçlamaktadır. Ayrıca, Danimarka Milli Arşivi tarafından tanımlanan kriterlere uyması gereken elektronik belgelerin depolama formatları için açık gereklilikler de geçerlidir. Aktarılan tüm dijital arşiv materyallerinin, gelecek nesiller tarafından okunabilir ve kullanılabilir olmasını sağlayacak şekilde güvenli bir şekilde gözüktüne alınması için Danimarka Milli Arşivi, dijital belgeler aktarılırken kullanılacak bir dizi iyi tanımlanmış ve yaygın olarak bilinen formatları belirtmiştir. Seçilen biçimler

ve gelecekteki biçimler arasında dönüştürülebilirlik sağlanmalıdır. Bu nedenle formatlar standartlaştırılmalı veya en azından iyi belgelenmelidir. Yaygın olarak desteklenmeli, platformdan bağımsız ve açık olmalı, amaç lisanslama veya yenilemeye tabi olmamalarıdır. Veri kaybı veya daha sonra veri kalitesinin bozulması riski olmamalı ve formatların uzun ömür beklentisi olmalıdır. Gelecekteki biçimlere dönüştürme olasılığını sağlamak için sistemlerden ve uygulamalardan bağımsız olmalıdırlar. Son olarak, görünüm önemliyse biçimler yazı tiplerinden bağımsız olmalıdır.

Her türlü arşiv materyali form, içerik ve medya ile ilgili tüm gerekliliklerin yerine getirildiğinden emin olmak için Danimarka Milli Arşivi tarafından teslim alındıktan sonra test edilir. Test araçları alındıktan sonra verileri test etmek için kurum içinde geliştirilmektedir. Danimarka Milli Arşivi tarafından barındırılan medya koleksiyonunun aynı kalitede olmasını sağlamak için medya kalitesinin sürekli test edilmesi için diğer araçlar kullanılmaktadır (Digital records – strategies and requirements, 2020).

5.13. Türkiye–Türkiye Cumhuriyeti Cumhurbaşkanlığı Devlet Arşivleri

Devlet Arşivleri 2018 yılında alınan kararla bağlı bulunduğu Başbakanlık’tan ayrılmış ve Cumhurbaşkanlığı’na bağlı olarak görev yapmaya başlamıştır. Cumhurbaşkanlığı Devlet Arşivlerinin iki ana kolu bulunmaktadır. Merkezi Ankara’da bulunan binasında Cumhuriyetten günümüze ulaşan belgelerle ilgilenilirken, İstanbul’da olan diğer birimi ise daha çok Osmanlı belgeleri le ilgilenmektedir. Son yıllarda önemli dijitalleştirme projelerine imza atan Cumhurbaşkanlığı Devlet Arşivleri milyonlarca belgeyi halkın erişimine sunmuştur. 2018 yılında Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı 8 milyonu aşan belgeyi dijital ortama aktarmış ve bu zamana kadar başkanlık bünyesinde toplam 60 milyon belge dijitalleştirilmiş ve bu belgelerin 40 milyonu kullanıcıların erişimine açılmıştır (60 milyon tarihi belge..., 2019). Fakat bunun yanı sıra milli arşiv politikalarının hazırlanmasından sorumlu olmasına rağmen Türkiye’nin bir Milli Arşiv Kanun’u bulunmamaktadır. Daha önce belirttiğimiz tasarı halinde meclise sunulan gelişmeden sonra bir ilerleme olmamıştır. Milli arşiv kanunu oluşturma konusu ile ilgili çalışmaların devam ettiği düşünülmektedir. Türkiye’de henüz dijital belgelerin arşive transferi başlamamıştır. Her ne kadar kurumsal bilgi yönetim süreçlerine dair kullanılan yönetmelik, standart olsa da henüz Türkiye’de dijital belgelerin arşive transferi ile ilgili bilgi yönetim süreçlerine dair yayımlanan bir resmi yasal dayanak da bulunmamaktadır. Kurumsal bilgi yönetim süreçleri ile ilgili resmi yasal dayanaklara çalışmanın önceki bölümlerinde değinilmiştir.

Milli arşivler bir ülkenin tarihini, değerlerini elinde tutan, gelecek nesiller için muhafaza eden ve erişime sunan bellek kurumlarıdır. Milli arşivlerin rol ve sorumlulukları bu kapsamda önemli görülmektedir. Milli Arşivler misyon ve vizyonlarını belirlemeleri, bu kapsamda hareket etmelidirler. Türkiye Cumhuriyeti Devlet Arşivleri Başkanlığı'nın kendi sitesinde yayımlamış olduğu konu ile ilgili bilgiler şu şekildedir: Misyonu “Devlet ve toplum hafızasını barındıran arşiv belgelerini arşivcilik standartları ve gelişen teknolojiler çerçevesinde tespit etmek, derlemek, korumak ve araştırmaya açmak suretiyle kamuoyuna güvenilir, kaliteli ve hızlı erişilebilen arşiv hizmetlerini sunmak ve kamu belge yönetimini etkinleştirmektir” şeklinde belirlenmiştir. Vizyon, “Ülkemiz arşivlerinin tek merkezden yönetimini sağlamak ve dünyada arşivcilik alanında referans bir kuruluş olmak” şeklindedir. Bununla birlikte devlet arşivlerinin temel değerleri “tarihe karşı sorumluluk, gelecek nesillere karşı sorumluluk, belgelerin orijinalliğinin korunması, kişisel verilerin korunması, mesleki uzmanlık, erişilebilirlik, güvenilirlik, yararlanıcı memnuniyeti, tarafsızlık ve şeffaflık, yenilikçilik, iş birliğine açık olma” şeklinde belirlenmiştir (T. C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı, t.y.).

Dijital belgelerin milli arşive transferi ile ilgili önemli bir gelişme Devlet Arşivleri Başkanlığı ve Sanayi Bakanlığı arasında 22.09.2020 tarihinde imzalanan BAYS (Bütünleşik Arşiv Yönetim Sistemi) Projesi'dir. Bu proje ile “arşiv belgelerinin tespiti, milli arşive transferi, depolanması ve tasnif edilerek araştırma hizmetine sunulması, yükümlü kurum ve kuruluşların yürütmüş olduğu arşiv hizmet ve faaliyetlerinin değerlendirilmesi, belgelerin tanımlanmasına yönelik kavramsal dizin oluşturulması, Devlet Arşiv Ağı ve Devlet Arşivi Veri Merkezinin oluşturulması, birimler ve faaliyetler arası ilişki ve iş akışlarının tanımlanması ve akabinde birçok modül ve arayüzden oluşacak kapsamlı bir otomasyon sistemi kurulması” hedeflenmektedir (2020 Yılı Faaliyet Raporu, 2020, s.49).

Yalçinkaya “milli arşivlerin elektronik belge yönetiminde rolü ve önemi” adlı çalışmasında, arşivlerin sahip oldukları belgeleri hangi şartlarda ve ortamda olursa olsun bilimsel unsurlara göre korumaları gerektiğinden bahsetmiştir. Bu unsurlar ise bir elektronik belgenin üretimi ile başlayıp ve arşive transferine kadar olan süreci ifade etmektedir. Tüm süreçlerde milli arşivlerin rol ve sorumlulukları bulunmaktadır. Çalışmada milli arşivlerin rol ve sorumlulukları ise mevzuat, idari, mali, teknik ve eğitim anlamında olmak üzere beş başlık altında incelenmiştir (Yalçinkaya, 2015).

ALTINCI BÖLÜM

6. BULGULAR VE ANALİZLERİN DEĞERLENDİRİLMESİ

Çalışmanın bu bölümünde araştırma kapsamımızda yer alan üniversiteler, belediyeler, bakanlıklar ve diğer kamu kurumlarının dijital belgelerin kurumsal bilgi yönetim süreçlerine dair analizinden elde edilen bulgulara yer verilmiştir. Bulgular 120 kurum kapsamında ayrıntılı olarak değerlendirilmiştir. İlgili bulgular tablolar ile görselleştirilerek sunulmuştur. Bu bölümde veriler genel bilgiler, dijital belge ve EBYS bilgileri, dijital belgeler için bilgi varlığı, saklama planı, dosya formatları ve dijital süreklilik, uzun vadede erişilebilirlik, koruma, üst veri ve tanımlama süreçleri, dijital belgelerin e-değerlendirme, e-ayıklama, hassasiyet değerlendirmesi süreçleri, politika, eğitim ve milli arşive transfer süreci adlı başlıklar altında değerlendirilmektedir.

6.1. Anket Bulgularının Değerlendirilmesi

6.1.1. Genel Bilgilere İlişkin Bulgular

Bu bölümde, katılımcıların eğitimleri, kurumda yürüttükleri görevleri, kurum türleri, çalıştıkları sektörlere ait veriler sunulmakta ve değerlendirilmektedir.

Demografik Bilgiler

Tablo 5. Katılımcıların eğitim bilgileri

Eğitim	Sayı	%
Doktora	9	7,5
Yüksek lisans	37	30,8
Lisans	68	56,7
Ön lisans	5	4,2
Lise ve dengi okul	1	0,8
Toplam	120	100

Tablo 5'e göre ankete katılanların yarısından fazlası (%56,7; n=68) lisans mezunudur. Ankete katılanların %30,8'i (n=37) yüksek lisans, %7,5'i (n=9) doktora mezunu, %4,2 (n=5) ön lisans ve %0,8 (n=1) lise ve dengi okul mezunudur. Ankete katılanlardan ortaöğretim, ilköğretim ve altı seviyesinde bir eğitim alan katılımcı yoktur. Genel anlamda ankete katılım seviyesi lisans ve üstü eğitim alanlardan oluşmaktadır.

Tablo 6. Katılımcıların yapmış oldukları görevleri

Görev	Sayı	%
Ağ ve Sistem Yöneticisi	1	0,8
Arşiv Uzmanı	14	11,7
Bilgi Güvenliği Uzmanı	3	2,5
Bilgi İşlem Daire Başkanı	10	8,3
Bilgi Yöneticisi	16	13,3
Bilgisayar Mühendisi	8	6,7
Bilgisayar Programcısı	1	0,8
EBYS Sorumlusu	34	28,3
İdari İşler Sorumlusu	2	1,7
İnfaz Koruma Memuru	1	0,8
İnsan Kaynakları	1	0,8
Kütüphaneci	22	18,3
Yazılım Geliştirici	7	5,8
Toplam	120	100

Tablo 6’ da ankete katılım sağlayanların yapmış oldukları görevler listelenmiştir. Ankete katılanların farklı görev dağılımları olduğu görülmektedir. Aşağıdaki tabloda ise bu görev dağılımlarının meslek grupları açısından yansımaları sunulmuştur.

Tablo 7. Katılımcıların mezuniyetleri ile görevleri

Görev	Sayı	%
BBY mezunu	86	71,6
Diğer	34	28,4
Toplam	120	100

Katılımcıların kurumlarda yapmış oldukları görevlerle ilgili verdikleri yanıtlara bakıldığında, ankete katılanların çok büyük bir bölümü (%71,6, n=86) Bilgi ve Belge Yönetimi (BBY) Bölümü mezunudur ve ilgili görevlerde çalışırken (kütüphaneci (%18,3, n=18,3), arşiv uzmanı (%11,7, n=14), bilgi yöneticisi (%13,3, n=16), EBYS sorumlusu (%28,3, n=34), geriye kalan katılımcılar ise toplam %28,4 oranıyla farklı meslek gruplarındandır. Görev tanımları ağ ve sistem yöneticisi (%0,8, n=1), bilgi güvenliği uzmanı (%2,5, n=3), bilgi işlem daire başkanı (%8,3, n=10), bilgisayar mühendisi (%6,7, n=8), bilgisayar programcısı (%0,8, n=1), idari işler sorumlusu (%1,7, n=2), infaz koruma memuru (%0,8, n=1), insan kaynakları (%0,8, n=1), yazılım geliştirici (%5,8, n=7) şeklindedir (Tablo 7).

Tablo 8. Katılımcıların kurum türleri

Kurum Türü	Sayı	%
Üniversite	67	55,8
Bakanlık	10	8,3
Belediye	32	26,7
Diğer kamu kurum ve kuruluşları	11	9,2
Toplam	120	100

Tablo 8’de katılımcıların görev aldıkları kurum türleri gösterilmektedir. Buna göre ankete katılanların %55,8’i üniversitede, %26,7’si belediyede, %9,2’si diğer kamu kurum ve kuruluşlarında ve %8,3’ü bakanlıklarda çalışmaktadırlar.

Ankette katılımcılara çalıştıkları sektör türü sorusu yöneltilmiştir. Alınan cevaplara göre katılımcıların eğitim, bilişim teknolojileri, iş ve yönetim, adalet ve güvenlik, kültür ve sanat, sağlık, ulaştırma, hizmet, kültür ve turizm, basın, çevre, güvenlik ve hukuk gibi birbirinden farklı sektörlerde görev aldıkları gözlemlenmiştir.

6.1.2. Dijital Belge ve EBYS

Bu bölümde, kurumlardaki belgelerin saklanma biçimleri, belgelerin dijitalleştirme bilgileri, fiziksel belgelerin dijital ortam bilgileri, kurumlardaki personelin EBYS algıları, EBYS kullanma süreleri, kurumların EBYS değiştirme sebepleri, dijital ortamda belge üretme sürelerine ait veriler sunulmakta ve değerlendirilmektedir.

Tablo 9. Kurumlarda belgenin hibrit saklanması

Belge saklama	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Evet	32	26,7	4	3,3	21	17,5	5	4,2	62	51,7
%		47,8		40		65,6		45,5		
Hayır	8	6,7	1	0,8	0	0	1	0,8	10	8,3
%		11,9		10		0		9,1		
Bir kısmı saklanıyor bir kısmı saklanmıyor.	26	21,7	5	4,2	11	9,2	5	4,2	47	39,2
%		38,8		50		34,4		45,5		
Diğer	1	0,8	0	0	0	0	0	0	1	0,8
%		1,5		0		0		0	120	100

Kamu kurumlarında belgelerin saklanma ortamına bakıldığında; üniversitelerin %47,8'i, bakanlıkların %40'ı, belediyelerin %65,6'sı ve diğer kamu kurum ve kuruluşlarının %45,5'i belgenin hem fiziksel hem de dijital halini saklamaya devam etmektedirler. Genel toplama bakıldığında da ankete katılan kurumların yarısından fazlası (%51,7) belgelerinin hem fiziksel hem de dijital halini saklamaktadırlar. Bunun yanı diğer seçeneğini belirten üniversite “kurumlarda EBYS’ye güven duyulmadığı için EBYS içerisinde bulunan dijital belgelerin fiziksel çıktısını da alıp sakladıkların, sisteme entegre olmayan kurumlara giden yazıların da bir nüshasının bazı durumlarda saklandığını” belirtmişlerdir.

Tablo 10. Kurumlarda fiziksel belgelerin dijitalleştirilmesi

Fiziksel belgelerin dijitalleştirilmesi	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Evet	49	40,8	7	5,8	26	21,7	7	5,8	89	74,2
%		73,1		70		81,3		63,6		
Hayır	16	13,3	2	1,7	4	3,3	2	1,7	24	20,0
%		23,9		20		12,5		18,2		
Diğer	2	1,7	1	0,8	2	1,7	2	1,7	7	5,8
%		3		10		6,2		18,2	120	100

Tablo 10’da, diğer kurumlara göre toplamda (%74,2) fiziksel belgeleri en çok dijitalleştiren grup belediyelerdir (%40,8). Fiziksel belgeleri dijitalleştirmeme oranı ise tüm gruplar için %20’dir. Grupların kendi içlerinde fiziksel belgeleri dijitalleştirme oranlarına baktığımızda, belediyeler %81,3, üniversiteler %73,1, bakanlıklar %70 ve diğer kamu kurum ve kuruluşları %63,6’dır. Diğer seçeneğini işaretleyen katılımcılar fiziksel belgeleri belli müdürlüklerin dijitalleştirdiğini, devlet arşivlerine gönderilmeden önce dijitalleştirme yapıldığını, EBYS kullanımından önceki belgelerin dijitalleştirildiğini, belgenin durumuna göre karar verildiğini ve gizli belgelerin dijitalleştirilmediğini belirtmişlerdir.

Tablo 11. Kurumların fiziksel belgelerinin dijital ortamda bulunma oranları

Fiziksel belgelerin dijital ortamda bulunma oranı	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
%10'dan az	8	6,7	0	0	3	2,5	2	1,7	13	10,8
%		11,9		0		9,4		18,2		
%11-20 arası	2	1,7	0	0	2	1,7	3	2,5	7	5,8
%		3		0		6,3		27,3		
%21-40 arası	12	10	3	2,5	6	5	0	0	21	17,5
%		17,9		30		18,8		0		
%41-60 arası	10	8,3	2	1,7	5	4,2	4	3,3	21	17,5
%		14,9		20		15,6		36,4		
%61- 80 arası	14	11,7	1	0,8	4	3,3	1	0,8	20	16,7
%		20,9		10		12,5		9,1		
%81-100 arası	17	14,2	3	2,5	8	6,7	1	0,8	29	24,2
%		25,4		30,0		25		9,1		
Bilmiyorum	4	3,3	1	0,8	4	3,3	0	0	9	7,5
%		6		10		12,5		0	120	100

Ankete katılan kurumların fiziksel belgelerin dijital ortamda bulunma oranlarına bakıldığında, %17,5-%24,2 arası oranlarında dağınık bir gruplanma görülmektedir. Grupların kendi içlerindeki oranlara bakıldığında ise; üniversiteler (%25,4) yaklaşık %81-100 oranında, bakanlıklar %21-40 oranı ve üstünde, belediyelerin ağırlıklı olarak %21-40 ve sonrası, kamu kurum ve kuruluşlarında ise %41-60 arası dağılım gösterdiği anlaşılmaktadır (Tablo 11). Bu tablodan kurumlarda dijitalleştirme faktörünün yaygınlığı ve hibrit ortamda belge yönetiminin durumu gözler önüne serilmektedir.

Tablo 12. Kurumlardaki katılımcıların EBYS algıları

EBYS Algısı	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
EBYS bir arşivdir.	4	3,3	0	0	1	0,8	0	0	5	4,2
%		6		0		3,1		0		
EBYS bir Bilgi Yönetim Sistemi'dir.	22	18,3	3	2,5	7	5,8	5	4,2	37	30,8
%		32,8		30		21,9		45,5		
EBYS hem arşiv hem de Bilgi Yönetim Sistemi'dir.	41	34,2	7	5,8	24	20	5	4,2	77	64,2
%		61,2		70		75		45,5		
Diğer	0	0	0	0	0	0	1	0,8	1	0,8
%		0		0		0		9,1	120	100

Tablo 12'ye göre kurumların %64,2'si EBYS'yi hem arşiv hem de bilgi sistem olarak görmekte, kurumların %30,8'si EBYS'yi bilgi sistemi olarak görmekte ve yine kurumların %4,2'si EBYS'yi bir arşiv olarak görmektedirler. Kurumların kendi işlerinde dağılımına baktığımızda, dört grupta da ağırlıklı olarak EBYS'yi hem arşiv hem de bilgi sistemi olarak görmektedirler. Diğer şıkkını işaretleyen kurum ise EBYS'si bir belge yönetim sistemi olarak görmektedir. EBYS'ler birer bilgi yönetim sistemidirler fakat günümüzde çoğu kamu kurum ve kuruluşu EBYS'yi aynı zamanda ağırlıklı olarak arşiv olarak da düşünüp kullanmaktadırlar.

Tablo 13. Kurumlardaki katılımcıların EBYS kullanımları

EBYS Kullanımı	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
1-3 yıl	4	3,3	0	0	9	7,5	3	2,5	16	13,3
%		6		0		28,1		27,3		
4-6 yıl	21	18	3	2,5	16	13,3	2	1,7	42	35,0
%		31		30		50		18,2		
7-9 yıl	37	31	3	2,5	4	3,3	5	4,2	49	40,8
%		55		30		12,5		45,5		
10+ yıl	5	4,2	4	3,3	3	2,5	1	0,8	13	10,8
%		7,5		40		9,4		9,1	120	100

Ankete katılan kurumların %40,8 oranında 7-9 yıl arası, %35 oranıyla da 4-6 yıl arası, %13,3 oranıyla yıl arası ve %10,8 oranıyla 10+ yıl arası EBYS kullandıkları ortaya çıkmıştır. Bu oranın 7-9 yıl arasında daha fazla olması 2008 yılında EBYS sinin tüm kamu kurumlarında zorunlu tutulmasına yorumlanabilir. Belediyelerin kendi işlerinde EBYS kullanım yıl aralıklarına bakıldığında 4-6 yıl arası seçeneği ile diğer kurumlara göre daha geç EBYS kullanımına başladıkları gözlenmektedir (Tablo 13).

Tablo 14. Kurumların EBYS değişim sebepleri

EBYS Değişikliği Sebebi	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Maliyet	6	5	0	0	4	3,3	1	0,8	11	9,2
%		9		0		12,5		9,1		
İşlevsellik	20	17	2	1,7	8	6,7	5	4,2	35	29,2
%		30		20		25		45,5		
Üst yönetim kararı	10	8,3	2	1,7	6	5	3	2,5	21	17,5
%		15		20		18,8		27,3		
Maliyet-işlevsellik ve üst yönetim kararı	2	1,7	1	0,8	1	0,8	1	0,8	5	4,2
%		3		10		3,1		9,1		
EBYS değişikliği yapılmadı.	36	30	5	4,2	15	12,5	5	4,2	61	50,8
%		54		50		46,9		45,5		
Bilmiyorum	4	3,3	1	0,8	5	4,2	0	0	10	8,5
%		6		10		15,6		0		

Tablo 14'e göre ankete katılan kurumların %50,8'i EBYS değişikliği yapmamıştır. Yine ankete katılan kurumların %29,2'si işlevsellik sebebiyle, %17,5'i üst yönetim kararı sebebiyle, %9,2'si maliyet sebebiyle, %4,2'si maliyet, işlevsellik ve üst yönetim kararlarının hepsi sebebiyle EBYS'yi değiştirmişlerdir.

Tablo 15. Kurumların dijital ortamda belge üretme süreleri

Dijital Belge Üretimi	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
1-5 yıl	10	8,3	1	0,8	15	12,5	3	2,5	29	24,0
%		14,9		10		46,9		27,3		
6-10 yıl	40	33,3	2	1,7	16	13,3	3	2,5	61	51,0
%		59,7		20		50		27,3		
11-15 yıl	15	12,5	6	5	1	0,8	2	1,7	24	20,0
%		22,4		60		3,1		18,2		
16-20 yıl	2	1,7	1	0,8	0	0	1	0,8	4	3,3
%		3		10		0		9,1		
20+	0	0	0	0	0	0	2	1,7	2	1,7
%		0		0		0		18,2	120	100

Kamu kurumlarında dijital belge üretime bakıldığında, üniversiteler %59,7 oranında 6-10 yıldır, bakanlıklar %60 oranında 11-15 yıldır, belediyeler %50 oranında 6-10 yıldır ve diğer kamu kurumları ise %27,3 oranıyla hem 6-10 hem de 11-15 yıldır dijital ortamda belge ürettiklerini belirtmişlerdir. Genel toplama bakıldığında ankete katılan kurumların %51'i 6-10 yıldır ve %24'ü 1-5 yıldır dijital ortamda belge üretmektedirler. Bu durum Tablo 13'teki kurumların EBYS kullanım yılları ile de örtüşmektedir (Tablo 15).

6.1.3. Dijital Belgeler için Bilgi Varlığı, Saklama Planı, Dosya Formatları ve Dijital Süreklilik

Bu bölümde, kurumların bilgi varlığı envanterine sahip olup olmadıkları, kurumlarda bilgi varlık sorumlusu olup olmadığına, kurumlarda e-arşiv sistemi bulunup bulunmadığına, kurumlarda dijital belge saklama sürelerinin belirlenmesine, dijital belgeler için standart dosya planına, kurumların standart dosya planına uyma bilgilerine, kurumlarda EBYS içerisinde birden fazla nüsha belge bulunmasına, sistem içerisinde nüsha belge bulunmasında yapılanlara, kurumlarda dijital belge oluştururken dikkat edilen unsurlara, kurumlarda saklanan belge format çeşitlerine, kurumlarda kullanılan formatların belirlenmesine, kurumlardaki dijital süreklilik terimi algısına ve dijital sürekliliğin iyi yönetilemediğinde kurumların karşılaşılabileceği zorluklara ait veriler sunulmakta ve değerlendirilmektedir.

Tablo 16. Kurumlarda bilgi varlığı envanteri

Bilgi Varlığı Envanteri Sahip Olma	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Evet	37	30,8	8	6,7	18	15,0	8	6,7	71	59,2
%		55,2		80,0		56,3		72,7		
Hayır	28	23,3	2	1,7	13	10,8	3	2,5	46	38,3
%		41,8		20,0		40,6		27,3		
Diğer	2	1,7	0	0	1	0,8	0	0	3	2,5
%		3,0		0		3,1		0	120	100

Tablo 16'ya bakıldığında ankete katılan üniversitelerin yarısından fazlası (%55,2), bakanlıkların %80'i, belediyelerin %56,3'ü ve diğer kamu ve kuruluşlarının %72,7'si bilgi varlığı envanterine sahipken, üniversitelerin yarıya yakını (%41,8), bakanlıkların %20'si, belediyelerin yarıya yakını (%40,6), diğer kamu kurum ve kuruluşlarının ise %27,3'ü bilgi varlığı envanterine sahip değildir. Diğer seçeneği işaretleyen kurumların verdikleri cevaplar ise, "Her bir bilgi varlığının envanteri profesyonel anlamda bulunmadığını, gelişigüzel birtakım çalışmalar olduğu, kısmen olduğu, tam anlamıyla uygulanmadığı, kurumun oluşturduğu 27001'e göre bir şablonun var olduğu, KVKK ve BGYS kapsamında yapılan çalışmalarda adreslenen bilgi varlıklarının olduğu, diğer bilgi varlıklarının envanterlerinin olmadığı" şeklindedir.

Tablo 17. Kurumlarda bilgi varlığı sorumlusu

Bilgi Varlığı Sorumlusu	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Evet	32	26,7	6	5,0	17	14,2	7	5,8	62	51,7
%		47,8		60,0		53,1		63,6		
Hayır	32	26,7	3	2,5	12	10,0	4	3,3	51	42,5
%		47,8		30,0		37,5		36,4		
Bilmiyorum	3	2,5	1	0,8	3	2,5	0	0	7	5,8
%		4,5		10,0		9,4		0	120	100

Üniversitelerin yarısının (%47,8) bilgi varlık sorumlusu varken yarısının ise (%47,8) yoktur ve %2,5 oranında bir bilgi varlık sorumlusu olup olmadığını bilmediklerini belirtmişlerdir. Bakanlıkların %60'ının bilgi varlık sorumlusu varken, %30'unun bilgi varlık sorumlusu bulunmamaktadır. Ankete katılan belediyelerin yarısından fazlasının (%53,1) bilgi varlık sorumlusu varken, yarısına yakını (%37,5) ise

sorumlusu yoktur. Diğer kamu kurum ve kuruluşlarının ise %63,6'sı bilgi varlık sorumlusu varken, %36,4'ünün bilgi varlık sorumlusu yoktur. Toplam orana baktığımızda kurumların %51,7'sinin bilgi varlığı sorumlusu varken, %42,5'nin bilgi varlığı sorumlusu yoktur (Tablo 17).

Tablo 18. Kurumlarda e-arşiv sisteminin varlığı

E-arşiv sistemi varlığı	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Evet	11	9,2	4	3,3	13	10,8	4	3,3	32	26,7
%		16,4		40,0		40,6		36,4		
Hayır	53	44,2	6	5	19	15,8	7	5,8	85	70,8
%		79,1		60,0		59,4		63,6		
Diğer	3	2,5	0	0	0	0	0	0	3	2,5
%		4,5		0		0		0	120	100

Tablo 18'e göre üniversitelerin yarısından fazlasının (%79,1), bakanlıkların %60'ının, belediyelerin %59,4'ünün diğer kamu kurum ve kuruluşlarının %63,6'sının bir e-arşiv sistemleri olmadığı anlaşılmaktadır. Genel oranlara bakıldığında ise ankete katılan kamu kurumlarının %70,8 'sinin bir e-arşiv sistemi bulunmadığı, %26,7'sinin e-arşiv sistemi bulunduğu bunun dışında ise ankete katılanların %2,5'inin EBYS içindeki modülü e-arşiv olarak gördükleri bunun dışında ayrı bir e-arşivleri olmadıkları anlaşılmaktadır. Evet diyenlerin de benzer bir yaklaşımı kabul ettiği varsayılmaktadır.

E- arşiv ve EBYS içerisinde bulunan e-arşiv modülü birbirinden farklı kavramlardır. E-arşiv her kurumda olması beklenen, kurumların e-imzalı belgelerinin dijital ortamda arşivlendiği, saklandığı, korunmasının sağlandığı EBYS uygulamalarından sonraki süreci içeren bir yapıdır. E-arşiv sistemlerinde, EBYS uygulamasında üretilen e-belgeler, arşivlerde muhafaza edilen ve dijitalleştirilmesi gereken fiziksel belgeler ile EBYS uygulamasına dâhil edilemeyen fiziksel belgeler yer alır (Akdoğan ve Özdemirci, 2016). EBYS uygulamaları e-arşivin oluşumunu sağlayan süreç uygulamasıdır.

Tablo 19. Kurumların dijital belge saklama sürelerinin belirlenmesi

Dijital Belgelerin Saklama Süreleri	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Belgeyi üretirken	20	16,7	1	0,8	7	5,8	4	3,3	32	26,7
%		29,9		10,0		21,9		36,4		
Belgeler oluşturulmadan önce	3	2,5	1	0,8	2	1,7	1	0,8	7	5,8
%		4,5		10,0		6,3		9,1		
Belge üzerinde son işlem yapıldıktan sonra	7	5,8	2	1,7	3	2,5	0	0	12	10,0
%		10,4		20,0		9,4		0		
Belgeyi arşivlerken	6	5,0	1	0,8	7	5,8	1	0,8	15	12,5
%		9,0		10,0		21,9		9,1		
Kurumumuzda dijital belgeler için saklama süresi belirlenmemektedir.	27	22,5	4	3,3	12	10,0	4	3,3	47	39,2
%		40,3		40,0		37,5		36,4		
Diğer	4	3,3	1	0,8	1	0,8	1	0,8	7	5,8
%		6,0		10,0		3,1		9,1	120	100

Kurumlardan toplanan dijital belgeleri saklama süreleri ile ilgili verilere bakıldığında; ankete yanıt veren üniversitelerin %40,3'ü, bakanlıkların %40'ı, belediyelerin %37,5'i ve diğer kamu kurum ve kuruluşlarının %36,4'ü dijital belgeler için bir saklama süresi belirlemedikleri görülmektedir. Yine ankete katılan üniversitelerin %29,9'u belgeyi üretirken, bakanlıkların %20'si belge üzerinde son işlem yapıldıktan sonra, belediyelerin 21,9'u belgeyi üretirken ve belgeyi arşivlerken, diğer kamu kurum ve kuruluşları %36,4'ü ise belgeyi üretirken saklama sürelerini belirlediklerini belirtmişlerdir. Tablo 19'da genel sonuçlara bakıldığında kamu kurumlarının %26,7'si belgeyi üretirken saklama süresini belirlerken, %39,2'si dijital belgeler için bir saklama süresi belirlememektedir. Diğer seçeneğini işaretleyen kurumlarda ise devlet arşivleri yönetmeliğine göre belirlendiğini, konunun standartlaşması için çalışmaların devam ettiğini belirtilmiştir. Çıkan sonuçlar içerisinde saklama süresi belirlenmemektedir seçeneğinin fazlaca seçilmesi konu hakkında farkındalık olarak eksik kalındığının da bir göstergesidir. EBYS üzerinde oluşturulan belgelerde dosya kodu sebebiyle belgeyi oluştururken saklama süresi de otomatik olarak belirlenmiş olur. Burada belgeyi doğru dosya numarasında konumlandırmak konusu da bir hayli önemlidir. Sonrasında ise son

kullanıcı belge üzerinde işlem yapabilir ve belgenin saklama süresi tekrar değişebilir. Esasen belge üzerinde son işlem yapıldıktan sonra saklama süresi belirlenmesi daha sağlıklı olacaktır. Kurumlarda belgelerin saklama süreleri ile ilgili dağınık bir yapı olduğu gözlemlenmiştir.

Tablo 20. Dijital belgelere ait standart dosya planı

Dijital belgeler için dosyalama sistemi	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Evet	2	1,7	3	2,5	11	9,2	4	3,3	20	16,7
%		3,0		30,0		34,4		36,4		
Hayır	65	54,2	7	5,8	21	17,5	7	5,8	100	83,3
%		97,0		70,0		65,6		63,6		120 100

Tablo 20'ye göre kurumların %83,3'ü dijital belgeler için dosyalama sistemi bulundurmazken, %16,7'si dijital belgeler için bir dosyalama sistemi bulundurmaktadır. Üniversitelerin %97'si, bakanlıkların %70'i, belediyelerin %65,6'sı ve diğer kamu kurum ve kuruluşlarının %63,6'sı dijital belgeler için bir dosyalama sistemi kullanmamaktadırlar.

Tablo 21. Kurumların standart dosya planına uymaları

Dosya Planına Uyma	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Çok yeterli	1	0,8	1	0,8	0	0	0	0	2	1,7
%		1,5		10,0		0		0		
Yeterli	8	6,7	0	0	4	3,3	0	0	12	10,0
%		11,9		0		12,5		0		
Kararsızım	26	21,7	4	3,3	11	9,2	5	4,2	46	38,3
%		38,8		40,0		34,4		45,5		
Yetersiz	24	20,0	2	1,7	6	5,0	4	3,3	36	30,0
%		35,8		20,0		18,8		36,4		
Bütünyle yetersiz	8	6,7	3	2,5	11	9,2	2	1,7	24	20,0
%		11,9		30,0		18,2		18,2		120 100

Kurumların iş süreçlerinde standart dosya planına uyma ile ilgili yaklaşımlarına baktığımızda, %1,7 çok yeterli, %10 yeterli görülürken, %38,3 oranıyla kararsız kaldıkları, %30 ile yetersiz ve %20 oranında bütünyle yetersiz oldukları

gözlemlenmiştir. Kurumlar özelinde bakıldığında üniversitelerin %47,7, bakanlıkların %50'si, belediyelerin %37'si, diğer kamu kurum ve kuruluşlarının ise %54,6'sının standart dosya planına uyma konusunda yetersiz olduğu görülmektedir. Bu durumun geniş perspektifte belge yönetim süreçlerinde ve arşive transfer süreci ve daha sonrası için büyük sorunlara yol açacağı aşikârdır (Tablo 21).

Tablo 22. Kurumlarda sistem içerisinde bir belgenin birden fazla nüshasının bulunma sorunu

Birden fazla nüsha sorunu	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Evet mevcuttur.	42	35	3	2,5	11	9,2	9	7,5	65	54,2
%		62,7		30,0		34,0		81,8		
Hayır mevcut değildir.	24	20,0	7	5,8	21	18,0	2	1,7	54	45,0
%		35,8		70,0		66,0		18,2		
Diğer	1	0,8	0	0	0	0	0	0	1	0,8
%		1,5		0		0		0	120	100

Üniversitelerin %62,7'sinde, bakanlıkların %30'unda, belediyelerin %34'ünde, diğer kamu kurum ve kuruluşlarının ise %81,8'inde sistem içerisinde bir belgenin birden fazla nüshanın mevcut olduğu görülmektedir. Toplam orana bakıldığında, kurumların %54,2'sinin sistem içerisinde fazla nüsha bulundurmaları mevcutken, %45'inin ise mevcut değildir (Tablo 22). Bu durumun son çıkan mevzuatta (Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik) değişikliğe gidilmesi ile birlikte sistem içerisinde artık nüsha sorununa çözüme kavuşturacağına dair bir ışık olarak görülmektedir. Yönetmeliğe göre “Elektronik ortamda güvenli elektronik imza ile imzalanan belgeler tek nüsha olarak hazırlanır” kararı alınmıştır (Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik, 2020, s. 3). Bunun dışında ise mevzuattan önceki sistem içerisinde bulunan birden fazla nüsha sorunu hala devam etmektedir.

Tablo 23. Belgenin sistemde fazla nüshasının olmasında yapılanlar

Bir belgenin sistem içerisinde birden fazla nüshasının bulunması	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Manuel olarak her belge tek tek sistemden kontrol edilip ayıklanmaktadır.	5	4,2	1	0,8	2	1,7	3	2,5	11	9,2
%		7,5		10,0		6,3		27,3		
Bir yazılım programı tarafından fazla nüsha olan belgeler sistem içerisinde tespit edilmektedir.	1	0,8	0	0	0	0	1	0,8	2	1,7
%		1,5		0		0		9,1		
Hiçbir çalışma yapılmamaktadır.	46	38,3	4	3,3	14	11,7	6	5	70	58,3
%		68,7		40,0		43,8		54,5		
Bir fikrim yok.	0	0	0	0	4	3,3	0	0	4	3,3
%		0		0		12,5		0		
Sistemimizde birden fazla nüsha bulunma sorunu yoktur.	15	12,5	5	4,2	12	10,0	1	0,8	33	27,5
%		22,4		50		37,5		9,1	120	100

Tablo 23'te görüldüğü üzere, üniversitelerin %68,7'si, bakanlıkların %40'ı, belediyelerin %43,8'i, diğer kamu kurum ve kuruluşlarının %54,5'i sistemlerinde birden fazla nüsha olmasına karşı bir çalışma yapmamaktadırlar. Diğer bir açıdan ise üniversitelerin %7,5'i, bakanlıkların %10'u, belediyelerin %6,3'ü, diğer kamu kurum ve kuruluşlarının ise %27,3'ü sistemlerindeki fazla nüshaya karşı manuel olarak her belgeyi tek tek sistemden kontrol edip ayıklama yöntemine başvurmaktadır. Bu soruna karşı ankete katılan tüm kamu kurumlarının %1,7'si sadece bir yazılım programı kullanarak sistemdeki fazla nüshaları tespit etmektedirler. Onun dışında kamu kurumlarının %27,5'i sistemlerinde birden fazla nüsha sorunu olmadığını belirtmişlerdir. Kısaca söylemek gerekirse kamu kurumlarında EBYS içerisinde bir belgenin birden fazla nüshası olmasına karşı çoğunlukla hiçbir çalışma yapılmamaktadır.

Tablo 24. Kurumlarda dijital belge oluştururken dikkate alınan unsurlar

		Aşırı derecede	Kısmen	Çok az	Hiç	$\bar{x}$	σ
Özgünlük	Sayı	68	20	25	7		
	%	56,7	16,7	20,8	5,8	1,76	0,979
Güvenilirlik	Sayı	65	32	16	7		
	%	54,2	26,7	13,3	5,8	1,71	0,911
Birlikte çalışabilirlik	Sayı	68	25	17	10		
	%	56,7	20,8	14,2	8,2	1,74	0,992
Tekrar kullanılabilirlik	Sayı	60	28	22	10		
	%	50,0	23,3	18,3	8,3	1,85	1,001
Tanımlama ve onaylama kolaylığı	Sayı	64	15	34	7		
	%	53,3	12,5	28,3	5,8	1,87	1,020
Gizlilik	Sayı	61	12	40	7		
	%	50,8	10,0	33,3	5,8	1,94	1,040
Bütünlük	Sayı	63	27	22	8		
	%	52,5	22,5	18,3	6,7	1,79	0,969

Tablo 24’te görüldüğü üzere, ankete katılan tüm kamu kurumlarının yarısından fazla dijital belge oluştururken özgünlüğe, güvenilirliğe, birlikte çalışabilirliğe, tekrar kullanılabilirliğe, tanımlama ve onaylama kolaylığına, gizliliğe ve bütünlüğe önem vermektedirler. Kurumların özgünlük (%56,7), birlikte çalışabilirlik (%56,7) ve güvenilirlik (%54,2) konulara diğer unsurlardan daha fazla önem verdiği görülmektedir. Ortalama değerlere baktığımızda kurumların güvenilirlik (1,71) ve birlikte çalışabilirlik (1,74) unsurlarına aşırı derece önem verdiği görülürken, diğer unsurlara kısmen önem verdikleri görülmektedir.

Tablo 25. Kurumlarda sistemde saklanan belge format çeşitleri

Saklanan belge formatları	Sayı	%
Microsoft Word 97 Binary Document Format (DOC)	44	36,7
Microsoft Word Office Open XML (DOCX)	59	49,2
Portable Document Format (PDF)	98	81,7
Portable Document Format (PDF/A-1a)	46	38,3
Portable Document Format (PDF/B-1b)	24	20,0
Düz metin (txt)	34	28,3
EPUB, Electronic Publication, version 3	15	12,5
Hypertext Markup Language (HTML)	23	19,2
Rich Text Format (RTF)	23	19,2
Bilmiyorum	9	7,5
Diğer	3	2,5
Toplam	120	100

Kurumların büyük çoğunluğunun sistem içerisinde dijital belgelerini Portable Document Format (PDF) (%81,7) formatında bulundurduğu görülmektedir. Kurumların %49,2'si belgelerini saklamada Microsoft Word Office Open XML (DOCX) formatını, %38,3'ü Portable Document Format (PDF/A-1a) formatını kullanmaktadırlar. Bunların yanı sıra kurumlar belgelerini saklamak için Microsoft Word 97 Binary Document Format (DOC) Portable Document Format (PDF/B-1b), düz metin (txt), EPUB, Electronic Publication, version 3, Hypertext Markup Language (HTML), Rich Text Format (RTF) formatlarını da tercih etmektedirler. Diğer (%2,5) seçeneğini işaretleyen kurumlar TIF, JPG formatlarında belgeleri sakladıklarını belirtmişlerdir. Bunun yanı sıra belirlenen herhangi bir format türü olmadığını tüm format türlerini kabul ettiklerini belirten kurumlar da vardır (Tablo 25).

Tablo 26. Kurumlarda kullanılan formatların belirlenmesi

Formatları Belirlemesi	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Kurum kendisi belirlemektedir.	11	9,2	5	4,2	8	6,7	2	1,7	26	21,7
%		16,4		50,0		25		18,2		
TS 13298 Standardında belirlenen dosya formatları kullanılmaktadır.	30	25,0	2	1,7	16	13,3	6	5,0	54	45,0
%		44,8		20,0		50,0		54,5		
Birlikte Çalışabilirlik Esasları Rehberinde belirlenmiş dosya formatları kullanılmaktadır.	7	5,8	2	1,7	0	0	1	0,8	10	8,3
%		10,4		20,0		0		9,1		
Belirlenmiş bir format yapısı yoktur.	19	15,8	1	0,8	8	6,7	2	1,7	30	25,0
%		28,4		10,0		25,0		18,2	120	100

Tablo 26'ya göre diğer kamu kurum ve kuruluşlarının %54,5'i, üniversitelerin %44,8'i, belediyelerin %50'si, bakanlıkların %20'si TS 13298 standardında belirlenen dosya formatlarını kullanmaktadırlar. Bunun yanı sıra bakanlıkların yarısı ise formatları kendilerinin belirlediğini belirtmiştir. Birlikte Çalışabilirlik Esasları Rehberinde

belirlenen dosya formatlarını kullanan kurumların oranı ise üniversiteler %10,4, bakanlıklar %20, diğer kamu kurum ve kuruluşları %9,1 şeklindeyken, belediyeler ise bu formatları kullanmadıklarını belirtmişlerdir. Ankete katılan üniversitelerin %28,4'ü, bakanlıkların %10'u, belediyelerin %25'i, diğer kamu kurum ve kuruluşlarının ise %18,2'si ise belirlenen bir format yapısı olmadığını belirtmişlerdir. Genel anlamda kurumlardan belirlenen ve kullanılan format yapısı ile ilgili dağınık bir yapılanma olduğu görülmektedir.

Tablo 27. Kurumlarda dijital süreklilik terimi algısı

Dijital Süreklilik Terimi	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
Algısı	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Evet	37	30,8	7	5,8	19	16,0	8	6,7	71	59,2
%		55,2		70,0		59,0		72,7		
Hayır	17	14,2	3	2,5	9	7,5	2	1,7	31	25,8
%		25,4		30,0		28,0		18,2		
Kısmen	13	10,8	0	0	4	3,3	1	0,8	18	15,0
%		19,4		0		13,0		9,1	120	100

Üniversitelerin %55,2'si, bakanlıkların %70'i, belediyelerin %59'u, diğer kamu kurum ve kuruluşlarının ise %72,7'si dijital süreklilik terimini daha önce duyduklarını belirtmişlerdir. Bunun yanı sıra üniversitelerin %25,4'ü, bakanlıkların %30'u, belediyelerin %28'i, diğer kamu kurum ve kuruluşlarının ise %25,8'i dijital süreklilik terimini daha önce duymadıklarını ifade etmişlerdir. Tablo genel olarak incelendiğinde ise ankete katılan kurumların %25'inin daha önce dijital süreklilik terimini duymadıklarını ve ne olduğunu bilemediklerini, %15'i kısmen duyduklarını, %59,2'si ise duyduklarını belirtmişlerdir (Tablo 27).

Tablo 28. Dijital süreklilik iyi yönetilemediğinde kurumların karşılaşılabileceği zorluklar

Dijital Süreklilikte Zorluklar		1	2	3	4	5	$\bar{x}$	σ
Bilgi kaybına yol açabilir.	Sayı	0	0	1	43	76	4,63	0,503
	%	0,0	0,0	0,8	35,8	63,3		
Etkili ve verimli çalışmayı olumsuz etkiler.	Sayı	0	0	8	55	57	4,41	0,615
	%	0,0	0,0	6,7	45,8	47,5		
Üst veri eksikliğinden ötürü çeşitli destek ödeneklerinin sağlanamamasına yol açar.	Sayı	0	4	23	54	39	4,07	0,807
	%	0,0	3,3	19,2	45,0	32,5		
Çeşitli formatlarda oluşturulmuş belgeleri açmak ve kullanmak istendiğimizde donanım ve yazılımın desteklememesi	Sayı	0	2	20	48	50	4,22	0,780
	%	0,0	1,7	16,7	40,0	41,7		
Veri göçünün gerçekleştirilememesi	Sayı	0	7	13	47	53	4,22	0,862
	%	0,0	5,8	10,8	39,2	44,2		
Kritik bir proje için gerekli olan bilginin bulunamaması	Sayı	0	7	23	48	42	4,04	0,883
	%	0,0	5,8	19,2	40,0	35,0		

1: Kesinlikle katılmıyorum, 2: Katılmıyorum, 3: Kararsızım, 4: Katılıyorum, 5: Kesinlikle katılıyorum

Tablo 28 incelendiğinde ankete katılan kurumlar, bir kurumda dijital süreklilik iyi yönetilemediğinde en güçlü olumsuz etkilerin, bilgi kaybına yol açabileceği (4,63), etkili ve verimli çalışmanın olumsuz etkileneceği (4,41), çeşitli formatlarda oluşturulmuş belgeleri açmak ve kullanmak istendiğimizde donanım ve yazılımın desteklememesi (4,22), veri göçünün gerçekleştirilememesi (4,22) şeklinde olduğunu belirtmişlerdir. Sonrasında ise onları takip eden oranda üst veri eksikliğinden ötürü çeşitli destek ödeneklerinin sağlanamamasına yol açması (4,07) ve kritik bir proje için gerekli olan bilginin bulunamaması (4,04) unsurları gelmektedir.

6.1.4. Uzun Vadede Erişilebilirlik, Koruma, Üst Veri ve Tanımlama Süreçleri

Bu bölümde, kurumlarda dijital belgelere uzun vadeli erişim için çalışma yapılıp yapılmadığı, bu çalışmalara kurumların ihtiyaç duyup duymadıkları, dijital belgelerin uzun vadeli korunması ile ilgili kaygıları ve bu konudan sorumlu birime, uzun vadeli koruma ile ilgili politika bilgisi, kurumların politika ihtiyaçları ve kurumlardaki personel farkındalık ve yeterliliğine ait veriler sunulmakta ve değerlendirilmektedir.

Tablo 29. Kurumlarda dijital belgelerin uzun vadede erişebilir olması için çalışma yapılıp yapılmadığı

Dijital Belgelere Uzun Vadede Erişilebilirlik	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Evet	15	12,5	3	2,5	12	10,0	2	1,7	32	26,7
%		22,4		30		37,5		18,2		
Hayır	39	32,5	6	5	13	10,8	6	5,0	64	53,3
%		58,2		60		40,6		54,5		
Çalışmalar planlanmaktadır.	13	10,8	1	0,8	7	5,8	3	2,5	24	20,0
%		19,4		10		21,9		27,3	120	100

Tablo 29'a bakıldığında üniversitelerin yarısından fazlasında (%58,2), bakanlıkların %60'ında, belediyelerin %40,6'sında, diğer kamu kurum ve kuruluşlarının %54,5'inde dijital belgelerin uzun vadeli erişebilir olması için bir çalışma yoktur. Tüm kurumlara baktığımızda ise, kurumların yarısından fazlasının (%53,3, n=64) uzun vadede erişim için bir çalışması yokken, %20'si konu ile ilgili çalışma yapmayı planlamakta, %26,7'sinin ise ileride dijital belgelerin uzun vadede erişimi için çalışması olduğu görülmektedir.

Tablo 30. Kurumlarda dijital belgelerin uzun vadede erişebilirliği çalışma ihtiyaçları

Uzun Vadede Erişebilirlik Çalışması İhtiyacı		1	2	3	4	5	$\bar{x}$	σ
Depolama ortamlarının sürekliliği sağlanmalı	Sayı	0	0	1	43	76		
	%	0,0	0,0	0,8	35,8	63,3	4,63	0,503
Dijital süreklilik tüm kurum bünyesinde önemsenmeli ve uygulanmalı	Sayı	0	0	5	68	47		
	%	0,0	0,0	4,2	56,7	39,2	4,35	0,560
Kurumda bilgi varlık envanteri oluşturulmalı ve sorumlular belirlenmeli	Sayı	0	0	10	47	63		
	%	0,0	0,0	8,3	39,2	52,5	4,44	0,646
Konu kapsamında politika, strateji, rehber vb. oluşturulmalı	Sayı	0	0	10	56	54		
	%	0,0	0,0	8,3	46,7	45,0	4,37	0,634
Bir risk planlaması yapılmalı	Sayı	0	0	15	50	55		
	%	0,0	0,0	12,5	41,7	45,8	4,33	0,690
Uygun veri formatları kullanılmalı	Sayı	0	0	17	56	47		
	%	0,0	0,0	14,2	46,7	39,2	4,25	0,689
Standartlara uygun üst veri oluşturulmalı	Sayı	0	0	8	62	50		
	%	0,0	0,0	6,7	51,7	41,7	4,35	0,603
Konu kapsamında düzenli aralıklarla eğitimler verilmeli	Sayı	0	0	10	61	49		
	%	0,0	0,0	8,3	50,8	40,8	4,33	0,624

1: Hiç ihtiyaç yok, 2: İhtiyaç yok, 3: Kararsızım, 4: İhtiyaç var, 5: Çok ihtiyaç var

Kurumlarda uzun vadede erişebilirlik çalışmalarına ihtiyaçları sorgulandığında, ortalama değerlere göre ankete katılan tüm kurumlarda depolama ortamlarının sürekliliği sağlanmasına ($\bar{x}=4,63$), kurumda bilgi varlık envanteri oluşturulması ve sorumluların belirlenmesine ($\bar{x}=4,44$), konu kapsamında politika, strateji, rehber vb. oluşturulmasına ($\bar{x}=4,37$), dijital sürekliliğin tüm kurum bünyesinde önemsenmesine ve uygulanmasına ($\bar{x}=4,35$), standartlara uygun üst veri oluşturulmasına ($\bar{x}=4,35$), bir risk planlaması yapılmasına ($\bar{x}=4,33$), konu kapsamında düzenli aralıklarla eğitimler verilmesine ($\bar{x}=4,33$), uygun veri formatları kullanılmasına ($\bar{x}=4,25$) çok ihtiyaç duyulduğu görülmektedir. Kurumların hiçbirisi bu unsurların uzun vadede erişebilirlik için ihtiyaç olmadığını düşünmemektedir (Tablo 30).

Tablo 31. Kurumlarda dijital belgelerin uzun vadeli korunması ile ilgili kaygıları

Uzun Vadede Koruma		1	2	3	4	5	$\bar{x}$	σ
Mevcut yazılım ve donanımın güncel tutulması ve korunmasının zor olması	Sayı	0	0	2	52	66		
	%	0,0	0,0	1,7	43,3	55	4,53	0,533
İçerik biçimlerinin karmaşık ve kırılgan olması	Sayı	0	0	3	41	76		
	%	0,0	0,0	2,5	34,2	63,3	4,61	0,539
Yasal ve politik risklerin var olması	Sayı	0	2	10	50	58		
	%	0,0	1,7	8,3	41,7	48,3	4,37	0,709
Hacim veya karmaşıklık kapsamında içerik toplamının zor olması	Sayı	0	2	12	62	44		
	%	0,0	1,7	10,0	51,7	36,7	4,23	0,695
Yetersiz personele sahip olmak	Sayı	0	5	18	57	40		
	%	0,0	4,2	15,0	47,5	33,3	4,10	0,803
İçeriğin yetersiz tanımlanması kullanımını ve keşfedilmesini zorlaştırabilmesi	Sayı	0	4	17	63	36		
	%	0,0	3,3	14,2	52,5	30	4,09	0,756
Dosya formatlarının hızlı değişiklik göstermesi ve eski dosya formatlarının okunamaması	Sayı	0	2	11	66	41		
	%	0,0	1,7	9,2	55,0	34,2	4,22	0,676

1: Kesinlikle katılmıyorum, 2: Katılmıyorum, 3: Kararsızım, 4: Katılıyorum, 5: Kesinlikle katılıyorum

Tablo 31'e göre kurumlar dijital belgelerin uzun vadeli korunması ile ilgili içerik biçimlerinin karmaşık ve kırılgan olması ($\bar{x}=4,61$), mevcut yazılım ve donanımın güncel tutulması ve korunmasının zor olması ($\bar{x}=4,53$), yasal ve politik risklerin var olması ($\bar{x}=4,37$), hacim veya karmaşıklık kapsamında içerik toplamının zor olması ($\bar{x}=4,23$), dosya formatlarının hızlı değişiklik göstermesi ve eski dosya formatlarının okunamaması ($\bar{x}=4,22$) konularında oldukça fazla kaygı duymaktadırlar. Onu takip eden oranda yine yetersiz personele sahip olmak ($\bar{x}=4,10$) içeriğin yetersiz tanımlanması kullanımını ve keşfedilmesini zorlaştırabilmesi ($\bar{x}=4,09$) dijital belgelerin uzun vadeli korunması ile kaygı duydukları konular arasındadır. Genel anlamda söylemek gerekirse kamu kurumlarının dijital belgelerin uzun vadeli korunması ile ilgili kaygıları yüksek düzeydedir.

Tablo 32. Kurumlarda dijital belgelerin uzun vadeli korunmasından sorumlu birim

Uzun Vadeli Korunmadan Sorumlu Birim	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Kütüphane ve Dokümantasyon Daire Başkanlığı	3	2,5	0	0	0	0	0	0	3	2,5
%		4,5		0		0		0		
Arşiv Daire Başkanlığı	3	2,5	0	0	2	1,7	1	0,8	6	5,0
%		4,5		0		6,3		9,1		
Bilgi İşlem Daire Başkanlığı	43	35,8	7	5,8	24	20,0	4	3,3	78	65,0
%		64,2		70		75		36,4		
İdari İşler Daire Başkanlığı	1	0,8	0	0	0	0	1	0,8	2	1,7
%		1,5		0		0		9,1		
Dijital belgelerin uzun vadeli korunmasından sorumlu bir birim yoktur.	10	8,3	2	1,7	5	4,2	3	2,5	20	16,7
%		14,9		20,0		15,6		27,3		
Dijital belgelerin uzun vadeli korunmasından sorumlu bir birimin kurulması planlanmaktadır.	2	1,7	0	0	0	0	0	0	2	1,7
%		3		0		0		0		
Diğer	5	4,2	1	0,8	1	0,8	2	1,7	9	7,5
%		7,5		10,0		3,1		18,2	120	100

Üniversitelerin %64,2'sinde, bakanlıkların %70'sinde, belediyelerin %75'inde, diğer kamu kurum ve kuruluşların %36,4'ünde dijital belgelerin uzun vadeli korunmasından sorumlu birim Bilgi İşlem Daire Başkanlığı olarak karşımıza çıkmaktadır. Bu oran ankete katılan tüm kurumların oranlarına bakıldığında ise %65'tir. Yine tüm kurumların %16,7'sinde ise dijital belgelerin uzun vadeli korunmasından sorumlu bir birimin olmadığı anlaşılmaktadır. Diğer (%7,5) şikkını işaretleyen kurumlar ise sorumlu birimin Yazı İşleri Birimin altında oluşturulmuş Elektronik Belge Yönetim Koordinatörlüğü, Personel Şube Müdürlüğü, Mali İşler Şube Müdürlüğü, Kültür Varlıkları ve Müzeler Şube Müdürlüğü, Yazı İşleri Şube Müdürlüğü, İnsan Kaynakları

Müdürlüğü birbirinden farklı birimlerin de bu konuda sorumlu olduğunu belirtmişlerdir. Bunun yanı sıra bu konuda Kütüphane ve Dokümantasyon Daire Başkanlığı'nın sorumluluğu %2,5 iken, Arşiv Daire Başkanlığı'nın sorumluluğu ise yalnızca %5 olarak görülmektedir (Tablo 32).

Tablo 33. Kurumlarda uzun vadeli koruma politikası

Koruma politikasının var olup olmadığı	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Evet, yazılı bir politika bulunmaktadır.	10	8,3	4	3,3	6	5	2	1,7	22	18,3
%		14,9		40,0		18,8		18,2		
Hayır, yazılı bir politika bulunmamaktadır.	43	35,8	6	5	19	15,8	7	5,8	75	62,5
%		64,2		60,0		59,4		63,6		
Kurumumuzda yazılı bir politika geliştirilmesi planlanmaktadır.	13	10,8	0	0	7	5,8	2	1,7	22	18,3
%		19,4		0		21,9		18,2		
Diğer	1	0,8	0	0	0	0	0	0	1	0,8
%		1,5		0		0		0	120	100

Tablo 33'te görüldüğü üzere, üniversite (%64,2), bakanlıklar (%60), belediyeler (%59,4) ve diğer kamu kurum ve kuruluşlarının (%63,6) yarısından fazlasının uzun vadeli koruma için bir politikası (strateji belgesi, plan, program, yönetmelik) yoktur. Diğer (0,8) seçeneğini işaretleyenler ise kurumlarında bazı süreçleri kapsayan (bazı belgelerin erişilebilir ve güvenliği) politikaların mevcut olduğunu ve genel bir politika için çalışma yapıldığını belirtmiştir.

Tablo 34. Kurumların politika ihtiyaçları

Politika İhtiyacı		1	2	3	4	5	$\bar{x}$	σ
Kurumumuzda dijital belgelerin kurumsal bilgi yönetim uygulamalarındaki tüm süreçleri içeren yazılı bir politikaya ihtiyaç vardır.	Sayı	1	4	11	43	61		
Dijital belgelerin uzun vadeli korumaya yönelik yazılı bir politikaya ihtiyacı vardır.	%	0,8	3,3	9,2	35,8	50,8	4,33	0,842
Kurumunuzda dijital belgelerin üst veri tanımlanması için politikaya ihtiyaç vardır.	Sayı	1	6	10	46	57		
	%	0,8	5,0	8,3	38,3	47,5	4,27	0,877
	Sayı	2	6	15	37	60		
	%	1,7	5,0	12,5	30,8	50,0	4,23	0,965

1: Kesinlikle katılmıyorum, 2: Katılmıyorum, 3: Kararsızım, 4: Katılıyorum, 5: Kesinlikle katılıyorum

Görüldüğü üzere, ankete katılan tüm kurumlar dijital belgelerin kurumsal bilgi yönetim uygulamalarındaki tüm süreçleri içeren ($\bar{x}=4,33$), uzun vadeli korumaya yönelik ($\bar{x}=4,27$) ve üst veri tanımlanması için ($\bar{x}=4,23$) yazılı bir politikaya ihtiyaç duyduklarına kesinlikle katılmaktadırlar. Yani kurumların büyük çoğunluğu ilgili konulardaki politikalara yüksek oranda ihtiyaç duymaktadırlar. Tabloya baktığımızda kurumların neredeyse hiçbiri politikaya ihtiyaç duymadığını belirtmemişlerdir (Tablo 34).

Tablo 35. Kurumların personelin farkındalık ve yeterliliği

Personel Farkındalık ve Yeterliliği		1	2	3	4	5	$\bar{x}$	σ
Kurumumuzda dijital belgelerin kurumsal bilgi yönetim süreçlerinde görev yapan personelin bu konuyla ilgili farkındalık düzeyi yeterli değildir.	Sayı	0	12	17	40	51		
	%	0,0	10,0	14,2	33,3	42,5	4,08	0,984
Kurumumuzda dijital belgelerin kurumsal bilgi yönetim süreçlerinde görev yapan nitelikli personel sayısı kurumumuz açısından yeterli değildir.	Sayı	1	9	17	42	51		
	%	0,8	7,5	14,2	35,0	42,5	4,11	0,968

1: Kesinlikle katılmıyorum, 2: Katılmıyorum, 3: Kararsızım, 4: Katılıyorum, 5: Kesinlikle katılıyorum

Tablo 35'e bakıldığında kurumlar, dijital belgelerin kurumsal bilgi yönetim süreçlerinde görev yapan personelin farkındalık düzeyinin yeterli olmadığına ($\bar{x}=4,08$) ve dijital belgelerin kurumsal bilgi yönetim süreçlerinde görev yapan nitelikli personel sayısının yeterli olmadığına ($\bar{x}=4,11$) katılmaktadırlar. Kısaca kurumlarda dijital belgelerin kurumsal bilgi yönetim süreçlerinde daha fazla personele ihtiyaç olduğu ve var olan personelin farkındalık düzeylerinin yeterli olmadığı görülmektedir (Tablo 35).

6.1.5. Dijital Belgelerin E-Değerlendirme, E-Ayıklama, Hassasiyet Değerlendirmesi Süreçleri

Bu bölümde, kurumlardaki dijital belgelerin e-değerlendirme, e-ayıklama, hassasiyet değerlendirme, kurumlarda bilgi yönetim süreçlerinde kullanılan yazılım programları, hassasiyet değerlendirme için üst veri tanımlamasına ait veriler sunulmakta ve değerlendirilmektedir.

Tablo 36. Kurumlarda dijital belgelerin e-değerlendirme süreci

E-değerlendirme	Sayı	%
Kurumumuzda e-değerlendirme personel tarafından el ile tek tek kontrol edilerek (geleneksel değerlendirme) yapılmaktadır.	9	7,5
Kurumumuzda e-değerlendirme için belirli programlar kullanılmaktadır.	0	0,0
Kurumumuzda e-değerlendirme hem personel tarafından el ile hem de belirli programlar ile yapılmaktadır.	0	0,0
Kurumumuzda dijital belgeler için e-değerlendirme yapılmamaktadır.	102	85,0
Kurumumuzda dijital belgeler için makro değerlendirme yöntemi kullanılmaktadır.	0	0,0
Kurumumuzda e-değerlendirme için özel bir yazılım oluşturulmuştur.	0	0,0
Bir fikrim yok.	9	7,5
Diğer	0	0,0
Toplam	120	100

Tablo 36'ya göre ankete katılan kurumların neredeyse tamamına yakınında (%85) dijital belgeler için e-değerlendirme yapılmamaktadır. Bunun yanı sıra kurumların %7,5'inde ise, e-değerlendirme personel tarafından el ile tek tek kontrol edilerek (geleneksel değerlendirme) yapılmaktadır. Ankete katılan kurumların %7,5'nin konu ile ilgili bir fikri yoktur.

Tablo 37. Kurumlarda dijital belgelerin e-ayıklama süreci

E-ayıklama	Sayı	%
Kurumumuzda e-ayıklama personel tarafından el ile tek tek kontrol edilerek yapılmaktadır.	15	12,5
Kurumumuzda e-ayıklama için belirli programlar kullanılmaktadır.	2	1,7
Kurumumuzda e-ayıklama hem personel tarafından el ile hem de belirli programlar ile yapılmaktadır.	2	1,7
Kurumumuzda dijital belgeler için e-ayıklama yapılmamaktadır.	90	75,0
Kurumumuzda e-ayıklama için özel bir yazılım oluşturulmuştur.	2	1,7
Bir fikrim yok.	9	7,5
Diğer	0	0,0
Toplam	120	100

Tablo 37'e göre ankete katılan kurumların çok büyük bir bölümünde (%75) dijital belgeler için e-ayıklama yapılmamaktadır. Bunun yanı sıra kurumların %12,5'inde ise, e-ayıklama personel tarafından el ile tek tek kontrol edilerek yapılmaktadır. Bunun dışında kurumların %1,7'sinde e-ayıklama için belirli programlar (e-ayıklama arşiv tetikleyicileri) kullanılırken, %1,7'sinde ise e-ayıklama hem personel tarafından el ile hem de belirli programlar ile yapılmaktadır. Kurumların yalnızca %1,7'sinde e-ayıklama için belirli programlar kullanılmaktadır. Ankete katılan kurumların %7,5'nin konu ile ilgili bir fikri yoktur.

Tablo 38. Kurumlarda dijital belgelerin hassasiyet değerlendirmesi süreci

Hassasiyet Değerlendirmesi	Sayı	%
Hassasiyet değerlendirmesi için oluşturulan özel bir yazılım programı kullanılmaktadır.	0	0,0
İşlemler uzman/uzmanlar tarafından tek tek gözden geçirilerek yapılmaktadır.	16	13,3
Bu işlem için bir komisyon kurulmuştur ve verilen karara göre süreç ilerlemektedir.	9	7,5
Hem bir uzman tarafından hem de özel bir yazılım kullanılarak yapılmaktadır.	0	0,0
Kurumumuzda dijital belgelerin hassasiyet değerlendirmesi yapılmamaktadır.	85	70,8
Bir fikrim yok.	10	8,3
Diğer	0	0,0
Toplam	120	100

Tablo 38'e göre ankete katılan kurumların büyük bir bölümünde (%70,8) dijital belgelerin hassasiyet değerlendirmesi yapılmamaktadır. Bunun yanı sıra kurumların %13,3'ünde ise işlemler uzman/uzmanlar tarafından tek tek gözden geçirilerek yapılmaktadır. Bunun dışında kurumların %7,5'inde dijital belgelerin hassasiyet değerlendirmesi için bir komisyon kurulmuştur ve verilen karara göre süreç ilerlemektedir. Ankete katılan kurumların %8,3'ünün konu ile ilgili bir fikri yoktur. Kurumların hiçbirinde hassasiyet değerlendirmesi için özel bir yazılım programı kullanılmamaktadır. Kurumlardan biri ise tam olarak nitelikli kişisel veri gibi olmasa da dijital belgelerin/verilerin gizlilik derecelerine göre muhafaza edilmesine ve taşınmasına yönelik yazılımsal DLP (data loss prevention) yaklaşımına geçilmesine yönelik çalışma yürütüldüğünden bahsetmiştir.

Tablo 39. Kurumlarda dijital belgelerin hassasiyet deęerlendirmesi süreci

Program Kullanımı	Sayı	%
Özel bir yazılım ya da program kullanılmamaktadır.	116	96,7
Dięer	4	3,3
Toplam	120	100

Kurumların neredeyse tamamı (%96,7) dijital belgelerin e-deęerlendirme, e-ayıklama, hassasiyet deęerlendirmesi süreçlerinde özel bir yazılım ya da program kullanılmamaktadırlar. Dięer (%3,3) seçeneęini işaretleleyen kurumlar ise süreçlerin EBYS üzerinden kontrol edildięini, e-ayıklama için arşiv tetikleyicileri oluşturulduęunu belirtmişlerdir (Tablo 39).

Tablo 40. Kurumlarda hassasiyet deęerlendirmesi için üst veri tanımlaması

Hassasiyet deęerlendirmesi için üst veri tanımlanması	Sayı	%
Her belge yöneticisi tarafından belgenin konusuna göre anlık oluşturulmaktadır.	23	19,2
Kurum tarafından belirlenmiş bir kelime seti içinden seçilerek tanımlanmaktadır.	3	2,5
Komisyon tarafından belirlenmektedir.	2	1,7
TS 13298 Standardında belirlenen alanlara göre	26	21,7
Dublin Core (DC) alanlarına göre	0	0,0
Dijital belgelerin hassasiyet deęerlendirmesi için üst veri tanımlaması yapılmamaktadır.	53	44,2
Bir fikrim yok.	9	7,5
Dięer	4	3,3
Toplam	120	100

Tablo 40'a bakıldığında, kurumların yarıya yakınında (%44,2) dijital belgelerin hassasiyet deęerlendirmesi için üst veri tanımlaması yapmadığı görülmektedir. Geleceęin milli hafızası açısından ve bilgi yönetişimi açısından bu durum risk temsil etmektedir. Bunun dışında, dijital belgelerin hassasiyet deęerlendirme için üst veri tanımlaması kurumların %21,7'sinde TS 13298 Standardında belirlenen alanlara göre %19,2'sinde her belge yöneticisi tarafından belgenin konusuna göre anlık oluşturulmakta, %2,5'inde kurum tarafından belirlenmiş bir kelime seti içinden seçilerek tanımlanmakta, %1,7'sinde komisyon tarafından belirlenmektedir.

6.1.6. Politika, Eğitim ve Milli Arşive Transfer Süreci

Bu bölümde, kurumların belge yönetim politikasına sahip olup olmadıklarına, belge yönetim politikasında olması gereken unsurlara, kurumların belge yönetim politikası ihtiyaçlarına, kurumlarda bilgi yönetim süreçlerine dair eğitim verilme ve ihtiyaçlarına, kurumlarda verilen eğitimlerin yeterliliğine, kurumsal politika oluşturulmasından sorumlu olacak birime, kurumsal bilgi yönetim sürecinde kurumların zorlanacağı alanlara, dijital transfer için kurumlardaki teknik altyapı yeterliliğine, dijital belgelerin bilgi yönetim süreçlerinden sorumlu birime, kurumların dijital transfer yükümlülüğüne, kurumların milli arşive transfer edilecek materyal bilincine, kurumların transfer için devlet arşivleri ile bağlantıya geçip geçmediklerine, kurumlarda dijital transfere ait hazırlığa, kurumların dijital transferi hangi zaman aralığında yapacağı bilgisine, kurumların dijital transfer konusunda denetlenmesi ve devlet arşivlerinin rollerine ait veriler sunulmakta ve değerlendirilmektedir.

Tablo 41. Kurumlarda belge yönetimi politikası

Belge Yönetimi Politikası	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Evet	10	8,3	0	0	4	3,3	1	0,8	15	12,5
%		14,9		0		12,5		9,1		
Hayır	57	47,5	10	8,3	28	23,3	10	8,3	105	87,5
%		85,1		100		87,5		90,9		100

Ankete katılan kurumların bir belge yönetimi politikasına sahip olup olmadığına ilişkin soruya çok büyük bir oranda (%87,5, n=105) hayır yanıtı verdiği görülmektedir. Kurumların %12,5'i ise kurumlarında bir belge yönetim politikası olduğu yönde yanıt vermişlerdir. Kurumlar özelinde bakıldığında, üniversiteler %14,9, belediyeler %12,5, diğer kamu kurum ve kuruluşları %9,1 oranında belge yönetimi politikasına sahip olduklarını belirtirken, bakanlıkların hiçbiri bir belge yönetimi politikasına sahip olmadıklarını belirtmişlerdir. Kurumların kendilerinin oluşturduğu bir genelge ya da dokümanı da belge yönetim politikası olarak kabul ettikleri düşünülmektedir.

Tablo 42. Belge yönetim politikasında olması gereken unsurlar

		1	2	3	4	5	$\bar{x}$	σ
Belge yönetimi politikasının amacı ve kapsamı	Sayı	0	0	0	62	58		
	%	0,0	0,0	0,0	51,7	48,3	4,48	0,502
	Sayı	0	0	6	51	63		
Roller ve sorumluluklar	%	0,0	0,0	5,0	42,5	52,5	4,48	0,594
	Sayı	0	0	14	56	50		
	%	0,0	0,0	11,7	46,7	41,7	4,30	0,669
Arşive uygun materyal türünün belirlenmesi	Sayı	0	0	9	46	65		
	%	0,0	0,0	7,5	38,5	54,2	4,47	0,634
	Sayı	0	0	4	52	64		
Elektronik belgelere erişim	%	0,0	0,0	3,3	43,3	53,3	4,50	0,565
	Sayı	0	3	19	55	43		
	%	0,0	2,5	15,8	45,8	35,8	4,15	0,774
Fiziksel ve dijital belgeler için saklama politikası	Sayı	0	0	9	62	49		
	%	0,0	0,0	7,5	51,7	40,8	4,33	0,613
	Sayı	0	1	7	65	47		
Ayıklama politikası	%	0,0	0,8	5,8	54,2	39,2	4,32	0,622
	Sayı	0	0	7	66	47		
	%	0,0	0,0	5,8	55,0	39,2	4,33	0,585
Dijital belgelerin transferi	Sayı	0	2	8	62	48		
	%	0,0	1,7	6,7	51,7	40,0	4,30	0,669
	Sayı	0	1	14	54	51		
Üst veri standardına uygunluk	%	0,0	0,8	11,7	45,0	42,5	4,29	0,703
	Sayı	0	1	8	61	50		
	%	0,0	0,8	6,7	50,8	41,7	4,33	0,640
Koruma	Sayı	0	6	4	66	44		
	%	0,0	5,0	3,3	55,0	36,7	4,23	0,420
	Sayı	0	0	4	74	42		
Hassas belgelerin süreçleri	%	0,0	0,0	3,3	61,7	35,0	4,28	0,638
	Sayı	0	0	4	74	42		
	%	0,0	0,0	3,3	61,7	35,0	4,28	0,638

1: Kesinlikle katılmıyorum, 2: Katılmıyorum, 3: Kararsızım, 4: Katılıyorum, 5: Kesinlikle katılıyorum

Katılımcılara kapsamlı bir belge yönetim politikasında olması gereken unsurlarla ilgili likert bir soru yöneltilmiştir. Tablo 42’de unsurların ortalama değerlerine bakıldığında katılımcıların sırasıyla elektronik belgelere erişim ($\bar{x}=4,50$), belge yönetimi politikasının amacı ve kapsamı ($\bar{x}=4,48$), roller ve sorumluluklar ($\bar{x}=4,48$), dosya planı ($\bar{x}=4,47$), ayıklama politikası ($\bar{x}=4,33$), dijital belgelerin transferi ($\bar{x}=4,33$), koruma ($\bar{x}=4,33$), imha politikası ($\bar{x}=4,32$), arşive uygun materyal türünün belirlenmesi ($\bar{x}=4,30$), üst veri standardında uygunluk ($\bar{x}=4,30$), hesap verebilirlik ve şeffaflık ($\bar{x}=4,29$), eğitim ve farkındalık ($\bar{x}=4,28$), hassas belgelerin süreçleri ($\bar{x}=4,28$) unsurlarının bir belge yönetimi politikasında kesinlikle olması gerektiğini düşünmektedirler. Ek olarak katılımcılar fiziksel ve dijital belgelerin için saklama politikası ($\bar{x}=4,15$) unsurun ise bir belge yönetimi politikasında olması gerektiğini düşündüklerini belirtmişlerdir (Tablo 42).

Tablo 43. Kurumların belge yönetim politikasına ihtiyaçları

Politika İhtiyacı		1	2	3	4	5	$\bar{x}$	σ
Kurumumuzun bir belge yönetim politikasına ihtiyacı vardır.	Sayı	3	4	11	41	61		
	%	2,5	3,3	9,2	34,2	50,8	4,28	0,943

1: Kesinlikle katılmıyorum, 2: Katılmıyorum, 3: Kararsızım, 4: Katılıyorum, 5: Kesinlikle katılıyorum

Tablo 43'e göre katılımcılara kurumlarında belge yönetim politikasına ihtiyaçları olup olmadığı sorusu yöneltilmiştir. Katılımcılardan gelen cevaplara bakıldığında; ankete katılanlardan yarısından fazlası (%50,8, n=61) kesinlikle katılıyorum seçeneğini işaretlerken yine katılanlardan yarıya yakını (%34,2, n=41) katılıyorum seçeneğini işaretlemişlerdir. Kararsızım seçeneğini işaretleyenler %9,2 iken, katılmıyorum (%3,3) ve kesinlikle katılmıyorum (%2,5) seçenekleri birbirine yakın orandadır. Sonuç olarak; kamu kurumlarında çalışan personel çok yüksek bir oranda (%85) belge yönetim politikasına ihtiyaç duymaktadırlar. Kurumlar, bir belge yönetim politikasına ihtiyaç duyduklarına kesinlikle katılmaktadırlar ($\bar{x}=4,28$).

Tablo 44. Kurumlarda bilgi yönetim süreçlerine dair eğitim verilip verilmediği

Eğitim verilip verilmediği	Evet		Hayır		Bir fikrim yok	
	Sayı	%	Sayı	%	Sayı	%
Dijital belgelerin değerlendirilmesi	0	0,0	119	99,2	1	0,8
Dijital belgelerin ayıklanması	0	0,0	119	99,2	1	0,8
Dijital belgelerin hassasiyet değerlendirilmesi	0	0,0	119	99,2	1	0,8
Dijital süreklilik	0	0,0	120	100	0	0,0
Uzun süreli koruma	17	14,2	103	85,8	0	0,0
Risk yönetimi	23	19,2	97	80,8	0	0,0
Bilgi iletişim teknolojileri	51	42,5	68	56,7	1	0,8
EBYS kullanımı	83	69,2	37	30,8	0	0,0
Bilgi güvenliği	46	38,3	74	61,7	0	0,0

Tablo 44'e bakıldığında, kurumlarda dijital süreklilik (%100, n=120), dijital belgelerin değerlendirilmesi (%99,2, n=119), dijital belgelerin ayıklanması (%99,2, n=119), dijital belgelerin hassasiyet değerlendirilmesi (%99,2, n=119), uzun süreli koruma (%85,8, n=103), risk yönetimi (%80,8, n=97) konularında neredeyse hiç eğitim verilmemektedir. Bunun dışında EBYS kullanımı (%69,2, n=83), bilgi iletişim teknolojileri (%42,5, n=51), bilgi güvenliği (%38,3, n=46) konularında yarıya yakın orada eğitim verildiği görülmektedir.

Tablo 45. Kurumlarda bilgi yönetim süreçlerine dair eğitim ihtiyacı

Eğitime ihtiyaç olup olmadığı		1	2	3	4	5	$\bar{x}$	σ
	Sayı	0	2	5	55	58		
Dijital belgelerin değerlendirilmesi	%	0,0	1,7	4,2	45,8	48,3	4,41	0,655
	Sayı	0	2	11	52	55		
Dijital belgelerin ayıklanması	%	0,0	1,7	9,2	43,3	45,8	4,33	0,714
Dijital belgelerin hassasiyet	Sayı	0	2	7	48	63		
değerlendirmesi	%	0,0	1,7	5,8	40,0	52,5	4,43	0,683
	Sayı	1	5	3	39	72		
Dijital süreklilik	%	0,8	4,2	2,5	32,5	60,0	4,47	0,809
	Sayı	0	4	3	45	68		
Uzun süreli koruma	%	0,0	3,3	2,5	37,5	56,7	4,48	0,710
	Sayı	1	6	6	52	55		
Risk yönetimi	%	0,8	5,0	5,0	43,3	45,8	4,28	0,842
	Sayı	1	8	8	56	47		
Bilgi iletişim teknolojileri	%	0,8	6,7	6,7	46,7	39,2	4,17	0,882
	Sayı	2	14	6	55	43		
EBYS kullanımı	%	1,7	11,7	5,0	45,8	35,8	4,03	1,016
	Sayı	1	6	6	50	57		
Bilgi güvenliği	%	0,8	5,0	5,0	41,7	47,5	4,30	0,846

1: Hiç ihtiyaç yok, 2:İhtiyaç yok, 3: Kararsızım, 4: İhtiyaç var, 5:Çok ihtiyaç var

Tablo 45'te ortalama değerlerini incelediğimiz zaman, kurumlar uzun süreli koruma ($\bar{x}=4,48$), dijital süreklilik ($\bar{x}=4,47$), dijital belgelerin hassasiyet değerlendirmesi ($\bar{x}=4,43$), dijital belgelerin değerlendirilmesi ($\bar{x}=4,41$), dijital belgelerin ayıklanması ($\bar{x}=4,33$), bilgi güvenliği ($\bar{x}=4,30$), risk yönetimi ($\bar{x}=4,28$) konularında eğitime çok ihtiyaç olduğunu belirtmişlerdir. Yine bilgi iletişim teknolojileri ($\bar{x}=4,17$) ve EBYS kullanımı ($\bar{x}=4,03$) konularında ise kurumlar eğitime ihtiyaçları olduğunu belirtmişlerdir. Tüm bu süreçler bilgi yönetişimi ile de ilgilidir. Bilgi yönetişimi yapılarında boşluklar bulunan kurumların çalışmaları risk altındadır. Değişim yönetimi, teknoloji yönetimi ve bilgi yönetimi süreçleri uygun şekilde entegre edilmediğinde bilgi yönetimi politikaları ve uygulamaları da yetersiz kalacaktır ve etkili bir bilgi yönetimi süreci olamayacaktır (Özdemir Şahin ve Saydam, 2022, s. 134).

Tablo 46. Kurumlarda verilen eğitimlerin yeterliliği

		1	2	3	4	5	$\bar{x}$	σ
	Sayı	8	50	38	19	5		
Verilen eğitimlerin yeterli olup								
olmadığı							2,69	0,960
	%	6,7	41,7	31,7	15,8	4,2		

1: Bütünüyle yetersiz, 2: Yetersiz, 3: Ne yeterli ne yetersiz, 4: Yeterli, 5: Çok yeterli

Tablo 46'ya göre verilen eğitimi kurumların %6,7'si bütünüyle yetersiz, %41,7'si yetersiz, %31,7'si ne yeterli ne yetersiz bulduklarını belirtmişlerdir. Kurumların yalnızca %15,8'si verilen eğitimi yeterli bulurken, %4,2'si çok yeterli bulmuştur. Genel anlamda kurumlarda verilen eğitimin pek yeterli olmadığı görülmektedir.

Tablo 47. Kurumsal politikanın kim/kimler tarafından oluşturulması gerektiği

Politikanın kim/kimler tarafından oluşturulması gerektiği	Sayı	%
Her kurumun kendisi tarafından,	14	11,7
T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı tarafından hazırlanmış örnek bir metin üzerinden kurumlar kendilerine göre uyarlayarak,	98	81,7
Bilgi Teknolojileri ve İletişim Kurumu	7	5,8
TÜBİTAK	1	0,8
Diğer	0	0,0
Toplam	120	100

Kurumların %81,7'si dijital belgelerin kurumsal bilgi yönetim süreçlerine yönelik yazılı politikanın T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı tarafından hazırlanmış örnek bir metin üzerinden kurumların kendilerine göre uyarlaması gerektiğini belirtmektedirler. Kurumların %11,7'si ise politikanın her kurumun kendisi tarafından oluşturulması gerektiğini ifade etmektedirler. Kurumların %5,8'i Bilgi Teknolojileri ve İletişim Kurumu, %0,8'i TÜBİTAK tarafından politika oluşturulması gerektiğini belirtmektedirler. Genel itibari ile kurumların neredeyse tamamına yakını politikanın yetkili kurum olan T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı tarafından hazırlanması gerektiğini ifade etmişlerdir (Tablo 47).

Tablo 48. Kurumsal bilgi yönetim süreçlerinde kurumların zorlandığı/zorlanacağı alanlar

Uygulamada zorlanılan/zorlanılacağı düşünülen alanlar	Sayı	%
Dijital belgelerin ayıklanması	93	77,5
Dijital belgelerin değerlendirilmesi	84	70,0
Hassasiyet değerlendirmesi aşaması	89	74,2
Dijital süreklilik aşaması	74	61,7
Dijital belgelerin korunması	63	52,5
Diğer	0	0
Toplam	120	100

Tablo 48'e bakıldığında, kurumlarının yarısından fazlası tüm konularda zorlandığını/zorlanacağını düşünmektedirler. Kurumların en çok zorlandığı/zorlanacağı

ilk iki alan ise dijital belgelerin ayıklanması (%77,5) ve hassasiyet değerlendirmesi (%74,2) aşamalarıdır. Dijital belgelerin değerlendirmesi aşaması da kurumların en çok zorlanacağı üçüncü olarak karşımıza çıkmaktadır.

Tablo 49. Dijital belgelerin bilgi yönetim süreçlerinde sorumlu birim

Dijital belgelerin kurumsal bilgi yönetim süreçlerinden hangi birimin sorumlu olduğu	Sayı	%
Bilgi İşlem Dairesi Başkanlığı	61	50,8
Strateji Geliştirme Daire Başkanlığı	3	2,5
Kütüphane ve/veya Arşiv Hizmetleri Birimi	13	10,8
İdari ve Mali İşler Daire Başkanlığı	1	0,8
Yazı İşleri Dairesi Başkanlığı	6	5,0
Konu ile ilgili sorumlu bir birim yoktur.	18	15,0
Diğer	18	15,0
Toplam	120	100

Tablo 49'a göre ankete katılan kurumların yarısından fazlasının (%50,8) dijital belgelerin kurumsal bilgi yönetim süreçlerinden Bilgi İşlem Daire Başkanlığı sorumludur. Yine kurumların %15'inde konu ile ilgili sorumlu bir birimin olmadığı görülmektedir. Kurumların %10,8'inde ise sorumlu birim Kütüphane ve/veya Arşiv Hizmetleri'dir. Diğer (%15) seçeneğini işaretleyen kurumlarda ise sorumlu birimler, İnsan Kaynakları Müdürlüğü, Bilgi işlem ve Arşiv Hizmetleri Birimi, Bilgi İşlem ve Strateji, Bilgi İşlem ve Kütüphane şeklindedir.

Tablo 50. Dijital belgelerin arşive transferi için teknik altyapının yeterliliği

	1	2	3	4	5	$\bar{x}$	σ
Sayı	9	36	31	31	13		
Transfer için altyapının yeterli olup olmadığı						3,03	1,141
%	7,5	30,0	25,8	25,8	10,8		

1: Bütünüyle yetersiz, 2: Yetersiz, 3: Kararsızım, 4: Yeterli, 5: Çok yeterli

Kurumlar, dijital belgelerin Milli Arşive transferinin gerçekleşmesi için gerekli olan teknik altyapılarını %7,5'i bütünüyle yetersiz, %30'u yetersiz, %25,8'i ne yeterli ne yetersiz, %25,8'i yeterli ve %10,8'i çok yeterli bulmaktadır. Konu ile ilgili teknik altyapının ne yeterli ne de yetersiz olduğu görülmektedir ($\bar{x} = 3,03$) (Tablo 50).

Tablo 51. Kurumların dijital belgeleri için Devlet Arşivlerine transfer yükümlülüğü

Transfer Yükümlülüğü	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Evet	34	28,3	6	5	13	10,8	5	4,2	58	48,3
	%	50,7		60		40,6		45,5		
Hayır	9	7,5	2	1,7	6	5,0	5	4,2	22	18,3
	%	13,4		20,0		18,8		45,5		
Bilmiyorum	24	20,0	2	1,7	13	10,8	1	0,8	40	33,3
	%	35,8		20,0		40,6		9,1	120	100

Tablo 51’e göre ankete cevap veren kurumların %48,3’ü dijital belgeleri için Devlet Arşivlerine transfer yükümlülüğü bulunduğunu belirtirken, %18,3’ü transfer yükümlülüğü bulunmadığını belirtmişlerdir. Kurumların %33,3’ü ise dijital belgelerini devlet arşivlerine transfer yükümlülüğü bulunup bulunmadığı ile ilgili bir fikre sahip değildir. Mevcut düzende belgelerini arşive transferden muaf kurumlar TBMM ve Milli İstihbarat Teşkilatı’dır. Bu durumda sonuçlar, kurumların transfer yükümlülüğü ile ilgili farkındalık eksikliği olduğunu göstermektedir.

Tablo 52. Kurumlarda Devlet Arşivlerine transfer edilecek materyal bilinci

Transfer Edilecek Materyal Bilinci	Üniversite		Bakanlık		Belediye		Diğer kamu kurum ve kuruluşları		Toplam	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
Evet	17	14,2	4	3,3	13	10,8	6	5	40	33,3
	%	25,4		40		40,6		54,5		
Hayır	50	41,7	6	5	19	15,8	5	4,2	80	66,7
	%	74,6		60		59,4		45,5	120	100

Tablo 52’ye göre ankete katılan kurumların %66,7’si Devlet Arşivlerine hangi materyallerini transfer edeceğini bilmezken, %33,3’ü ise hangi materyallerini transfer edeceklerini bilmektedirler.

Tablo 53. Dijital belgelerin arşive transferi için Devlet Arşivleri ile bağlantıya geçilip geçirmediği

Devlet arşivleri ile bağlantıya geçilip geçirmediği	Sayı	%
Evet	0	0
Hayır	96	80,0
Bilmiyorum	23	19,2
Diğer	1	0,8
Toplam	120	100

Tablo 53’e göre dijital belgelerin arşive transferi için kurumların %80’i devlet arşivleri ile bağlantıya geçmemiştir. Kurumların %19,2’si ise devlet arşivleri ile bağlantıya geçilip geçirmediğini bilmemektedir. Diğer (%0,8) seçeneğini işaretleyen kurum ise transfer yükümlülüğünün olmadığını belirtmiştir.

Tablo 54. Dijital transfer ile ilgili bir çalışma olup olmadığı

Transfer ile ilgili bir çalışma olup olmadığı	Sayı	%
Evet, dijital belgelerin milli arşive transferi ile ilgili bir çalışma vardır.	0	0
Hayır, henüz dijital belgelerin milli arşive transferi ile ilgili bir çalışma yoktur.	89	74,2
Bilmiyorum	31	25,8
Toplam	120	100

Tablo 54’e bakıldığında kurumların %74,2’sinin dijital belgelerini arşive devretmek için bir çalışması yoktur. Kurumların %25,8’i ise konu ile ilgili bir çalışma olup olmadığını bilmemektedir. Bunlara ek olarak daha önceki bölümlerde belirttiğimiz Devlet Arşivlerinin “Bütünleşik Arşiv Yönetim Sistemi Projesi Arşiv belgelerinin tespiti, milli arşive transferi, depolanması ve tasnif edilerek araştırma hizmetine sunulması, yükümlü kurum ve kuruluşların yürütmüş olduğu arşiv hizmet ve faaliyetlerinin değerlendirilmesi, belgelerin tanımlanmasına yönelik kavramsal dizin oluşturulması, Devlet Arşiv Ağı ve Devlet Arşivi Veri Merkezinin oluşturulması” amacı ile BAYS Projesi başlatılmıştır (2020 Yılı Faaliyet Raporu, 2020, s.49). Proje henüz tamamlanmamış olsa da girişim anlamında önemli bir adım olarak görülmektedir.

Tablo 55. Kurumların dijital transferi gerçekleştirmeyi düşündükleri zaman aralığı

Transfer için belirlenen zaman aralığı	Sayı	%
2021-2023	0	0
2024-2026	0	0
2027-2029	2	1,7
2030-2033	1	0,8
Planlanmıyor.	107	89,2
Diğer	10	8,3
Toplam	120	100

Tablo 55'e bakıldığında kurumların %89,2'sinde henüz dijital belgelerin transferi için bir çalışma planlanmamıştır. Bunun yanı sıra kurumların %1,7'sinde 2027-2029 yılları arasında, %0,8'inde ise 2030-2033 yılları arasında dijital belgeleri milli arşive transfer edecekleri görülmektedir. Diğer (%8,3) şikkını işaretleyen kurumlar ise transfer yükümlülükleri olmadığını, uzun bir süre dijital belgelerin transfer edileceğini düşünmediklerini, bunun için gerekli olan bilincin kurumlarda henüz olmadığını belirtmişlerdir.

Tablo 56. Kurumlarda dijital belgelerin transferinin denetlenmesi

Sürecin kontrolünden kimin sorumlu olması gerektiği	Sayı	%
T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı	91	75,8
Kamu Kurumlarının İç Denetim Mekanizması	18	15,0
TÜBİTAK	1	0,8
Özel Anlaşmalı Kurumlar	0	0
Bilgi Teknolojileri ve İletişim Kurumu	9	7,5
Yazılım şirketleri	1	0,8
Diğer	0	0
Toplam	120	100

Kurumların %75,8'i e-belgelerin Milli Arşive teslim edilip edilmediğinin (veya mevzuat esaslarına uygun olarak sürecin işleyip işlemediğinin) kontrolünün T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı tarafından yapılması gerektiğini belirtmişlerdir. Kurumların %15'i denetlemeyi Kamu Kurumlarının İç Denetim Mekanizması tarafından, %7,5'i Bilgi Teknolojileri ve İletişim Kurumu, %0,8'i TÜBİTAK, %0,8'i yazılım şirketleri tarafından yapılması gerektiğini belirtmişlerdir (Tablo 56).

Tablo 57. Devlet Arşivlerinin rolleri

Devlet Arşivleri ile ilgili ifadeler		1	2	3	4	5	$\bar{x}$	σ
Devlet Arşivleri Başkanlığı kurumların elektronik arşivleme süreçleri ile ilgili yeterli düzeyde takip ve denetleme yapmaktadır.	Sayı	28	44	33	15	0		
	%	23,3	36,7	27,5	12,5	0	2,29	0,965
Devlet Arşivleri Başkanlığı'nın kurumların milli hafızasını koruyup ileriki kuşaklara aktaracağına inancımız yüksektir.	Sayı	28	29	36	21	6		
	%	23,3	24,2	30,0	17,5	5,0	2,57	1,172
Devlet Arşivleri Başkanlığı görev ve sorumluluklarını yerine getirmektedir.	Sayı	18	34	43	25	0		
	%	15,0	28,3	35,8	20,8	0	2,63	0,979
Devlet Arşivleri Başkanlığı gerekli yasal düzenlemeler (arşiv kanunu, politika vb.) konusunda yeterli hizmeti sağlamaktadır.	Sayı	11	47	43	19	0		
	%	9,2	39,2	35,8	15,8	0	2,58	0,866

1: Kesinlikle katılmıyorum, 2: Katılmıyorum, 3: Kararsızım, 4: Katılıyorum, 5: Kesinlikle katılıyorum

Kurumlara Devlet Arşivleri Başkanlığı ile ilgili yöneltilen sorulardan alınan cevapların ortalama değerlerine bakıldığında; kurumlar “Devlet Arşivleri Başkanlığı kurumların elektronik arşivleme süreçleri ile ilgili yeterli düzeyde takip ve denetleme yapmaktadır” görüşüne katılmamaktadırlar ($\bar{x}=2,29$). Kurumlar, “Devlet Arşivleri Başkanlığı'nın kurumların milli hafızasını koruyup ileriki kuşaklara aktaracağına inancımız yüksektir” görüşüne katılmamaktadırlar ($\bar{x}=2,57$). Kurumlar, “Devlet Arşivleri Başkanlığı gerekli yasal düzenlemeler (arşiv kanunu, politika vb.) konusunda yeterli hizmeti sağlamaktadır” ifadesine katılmamaktadırlar ($\bar{x}=2,58$). Kurumlar, “Devlet Arşivleri Başkanlığı görev ve sorumluluklarını yerine getirmektedir” görüşüne katılmakta kararsız kalmaktadırlar ($\bar{x}=2,63$).

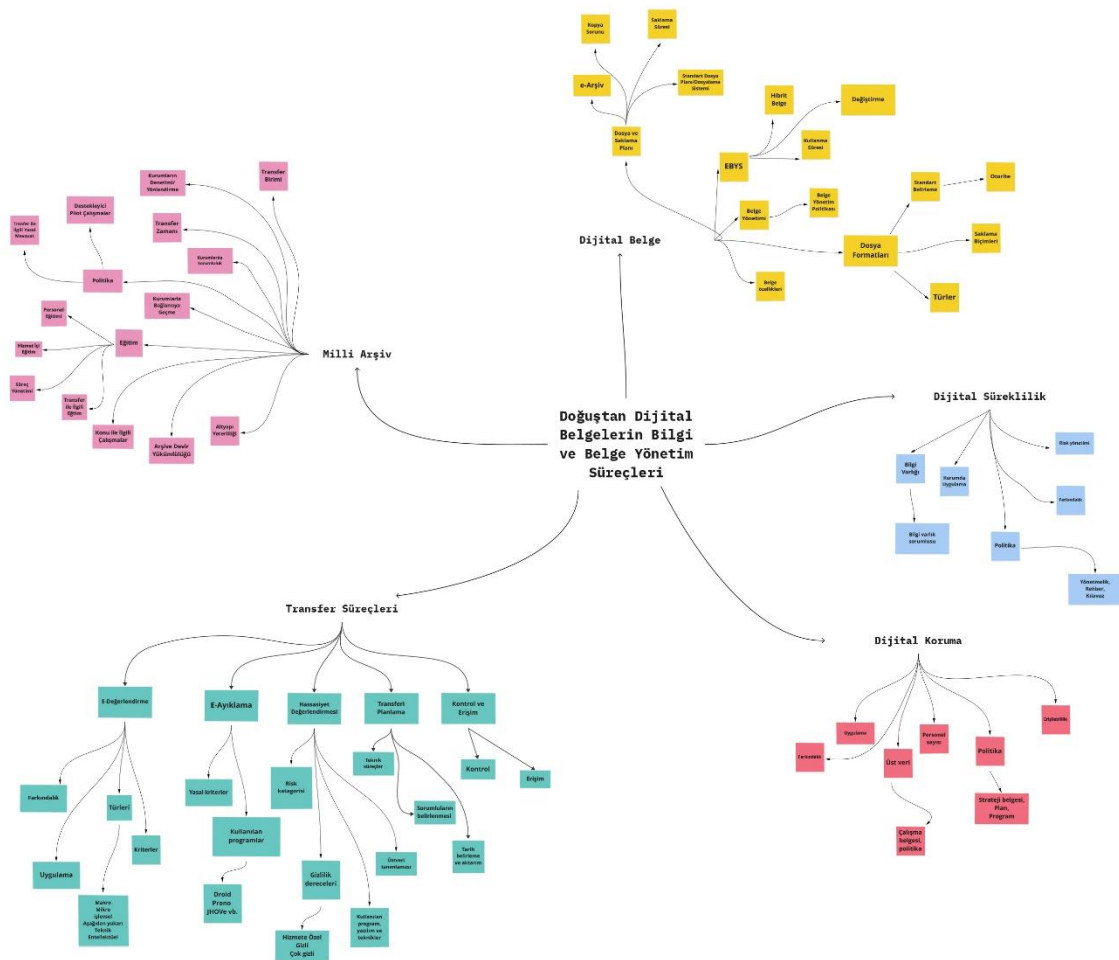
6.2 Doğuştan Dijital Belgelerin Bilgi ve Belge Yönetim Süreçleri Kavram Haritası

Çalışmanın bu bölümünde araştırmanın tüm süreç ve bulgularından yararlanılarak oluşturulan doğuştan dijital belgelerin bilgi yönetim süreçlerine dair bir desen (kavram haritası) sunulmuştur. Kavram haritası (concept map), bilginin görsel temsili niteliğindedir. Kavram haritaları genel terimlerle başlayarak anlamlı bağlantılara dayalı bilgileri parçalamaya olanak sağlar. Başka bir deyişle kavram haritaları ilgili konu hakkında büyük resmi görmeyi, ayrıntıları daha kolay hatırlamayı sağlar (Holschuh ve Nist, 2000). Türkiye’deki dijital belgelerin kurumsal bilgi yönetim süreçleri ile ilgili bir desen (kavram haritası) geliştirme önceki bölümlerde bahsedildiği gibi çalışmanın amaçlarından biridir. Kavram haritası dijital belge, dijital süreklilik, dijital koruma,

transfer süreçleri ve milli arşiv olmak üzere beş ana bölüm ve alt kırılımlardan oluşmaktadır. Kavram haritası oluşturmak için Miro online programı tercih edilmiştir.

Çalışmadan elde edilen bilgiler ışığında oluşturulan kavram haritasına Şekil 12’de yer verilmiştir. Kavram haritası beş ana bölüm ve çeşitli alt kırılımlardan oluşmaktadır. Kavram haritasını daha ayrıntılı gösterebilmek ve değerlendirmek için bölümler parçalanarak sunulmuştur.

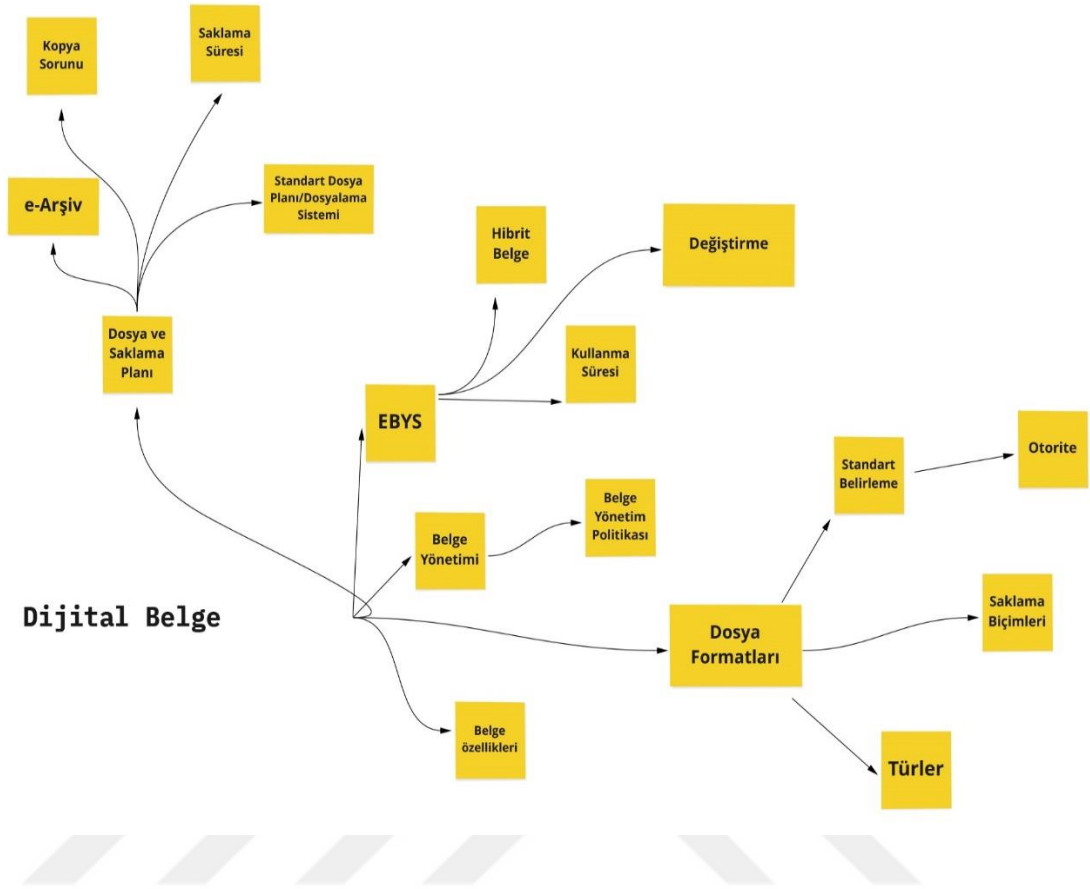
6.2.1 Kavram Haritası Genel Görünüm



Şekil 12. Doğuştan dijital belgelerin bilgi ve belge yönetim süreçleri kavram haritası

Şekil 12’deki kavram haritası “Dijital Belge”, “Dijital Süreklilik”, “Dijital Koruma“, “Transfer Süreçleri” ve “Milli Arşiv” olmak üzere beş ana bölümden oluşmaktadır. İlgili bölümler dijital belgelerin bilgi yönetim süreçlerinde düşünülmesi gereken süreçleri içermektedir.

6.2.1.1 Dijital Belge Bölümü

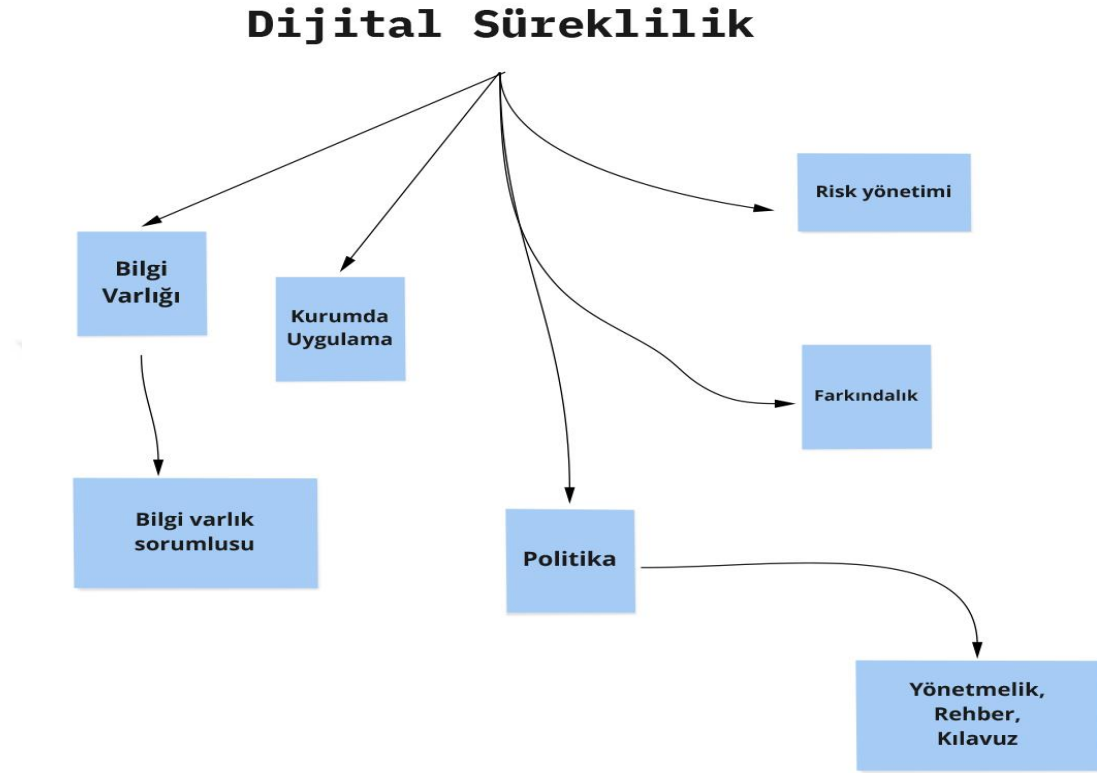


Şekil 13. Kavram haritası dijital belge bölümü

Dijital belgelerin bilgi yönetim süreçlerini ele alıp değerlendirmek, saptamalarda bulunabilmek ve varsa sorunlara çözüm önerileri getirebilmek için irdelenmesi gereken ilk adım belgenin kendisi yani kısaca dijital belgedir. Bu bölümde dijital belge ve ilgili alt kırılımları kavram haritasında gösterilmiştir (Şekil 13). Dijital belgenin yaşam evresi EBYS’de üretilmesi ile başlar. EBYS’nin kullanım süresi, değiştirilip değiştirilmediği, değiştirildiyse hangi sebeplerle değiştirildiği, buna ek olarak EBYS hibrit belge sürecinin devam edip etmediği son derece önemli unsurlardır. Dijital belge oluşturulurken dikkat edilmesi gereken özgünlük, güvenilirlik, birlikte çalışabilirlik, gizlilik, bütünlük, tekrar kullanılabilirlik, tanımlama ve onaylama kolaylığı gibi özellikler bulunmaktadır. Bunun yanı sıra belgelerin hangi dosya formatlarında olduğu, sürdürülebilirliği belgenin sonrasında açılıp kullanılabilmesi için hayati önem taşımaktadır. Bunun için kurumlarca ve milli arşiv tarafından standart dosya formatları belirlenmeli ve kabul edilen standartlara uyulmalıdır. Belgelerin işlemleri bittikten sonra kurumlarda e-arşivler saklanmalı, saklama süreleri belirlenmeli, saklama süresi için belirlenen bir dosyalama

sistemi olmalı, süreçler sistematik ilerlemelidir. E-arşiv içerisinde fazla nüsha sorununun önüne geçilmelidir.

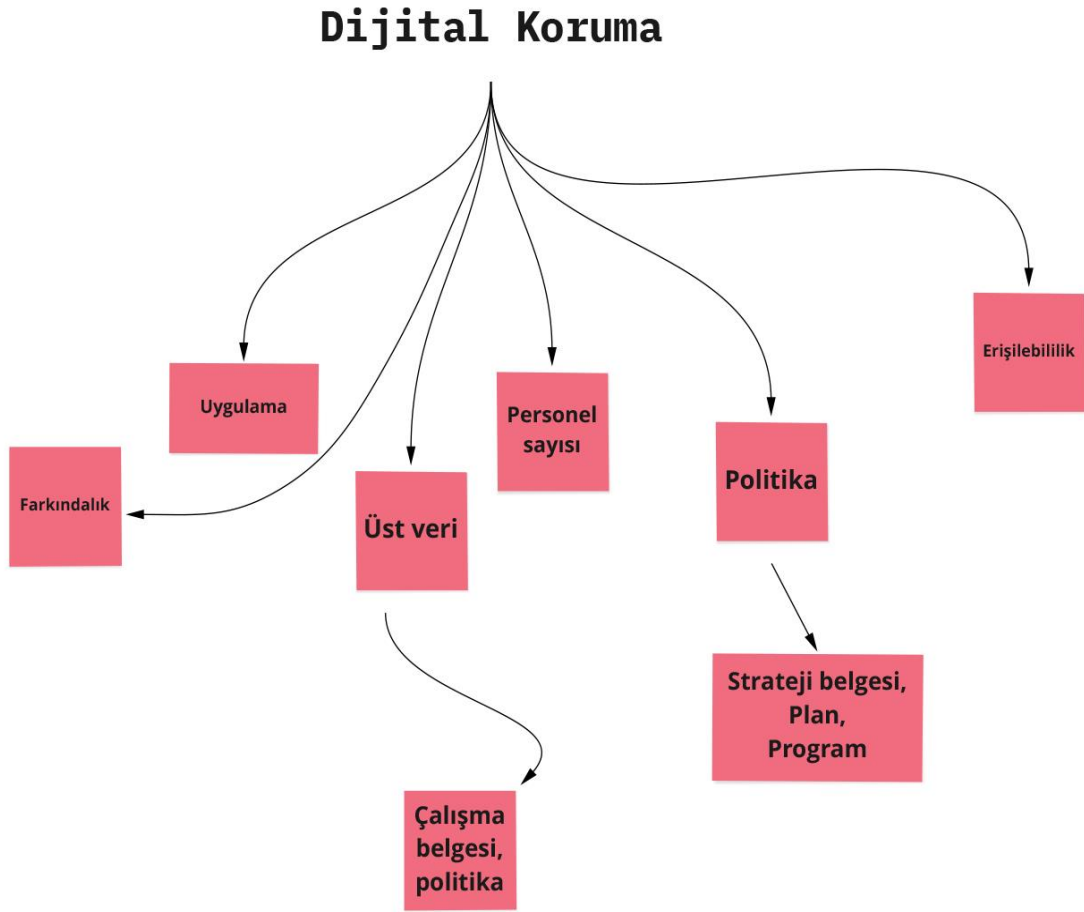
6.2.1.2 Dijital Süreklilik Bölümü



Şekil 14. Kavram haritası dijital süreklilik bölümü

Şekil 14’te dijital süreklilik bölümü ve alt kırımları gösterilmiştir. Buna göre dijital süreklilik kavramı dijital belgenin doğası gereği kurumlarda düşünülmesi gereken bir yapı olarak karşımıza çıkmaktadır. Dijital süreklilik kavramını kurumlarda belgenin yaşam döngüsü sürecinde yaşatabilmek için öncelikle eldeki bilgi varlığını bilmek ve anlamak gerekir. Bilgi varlıkları dijital sürekliliğin sağlanması ve yönetilmesinin gerçekleştirilmesinde öncüdür. Her bir bilgi varlığının ise bir varlık sorumlusu olmalıdır. Dijital sürekliliğin kurumlarda uygulanması bulması için dijital süreklilik modeli bulunmaktadır. Kurumlardaki personelin de bu konuda farkında olması son derece önemlidir. Dijital süreklilik aynı zamanda bir risk yönetimidir. Bu riski yönetmek de yine kurumlardaki personele düşmektedir. Bunu sağlamanın yolu ise politika gibi yasal düzenleyicilerden geçmektedir.

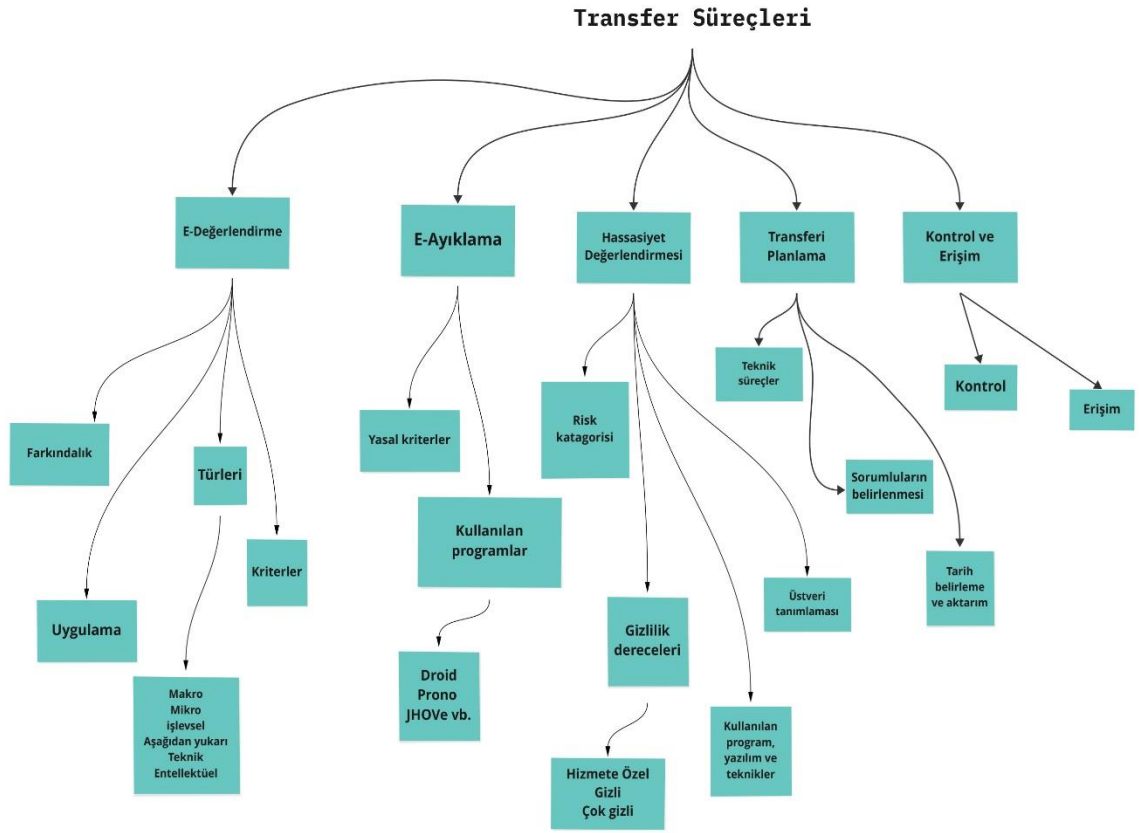
6.2.1.3 Dijital Koruma Bölümü



Şekil 15. Kavram haritası dijital koruma bölümü

Dijital koruma dijital belgeler için başlı başına çok eskilere dayanan bir sorundur. Bu sorunun henüz net bir çözümü olmasa da bazı yöntemlerle bu konunun üstesinden gelinebilmektedir. Dijital koruma için önemli unsurlardan biri üst veri meselesidir. Üst verinin düzgün tanımlanması, uygunluğu dijital korumayı da yakından ilgilendirir. Üst veri konusu için kurumlarda uyulması gereken bir kurul, standart olmalıdır. Her konuda olduğu gibi bu konuda da yetkin ve yeterli personel olmalı ayrıca personelin farkındalık sahibi olması gerekmektedir. Dijital koruma konusunda kurumların mutlaka bir politikası ya da en azından strateji belgesi gibi sağlam adımlarla ilerleyebileceği dayanakları olmalıdır (Şekil 15).

6.2.1.4 Transfer Süreçleri Bölümü

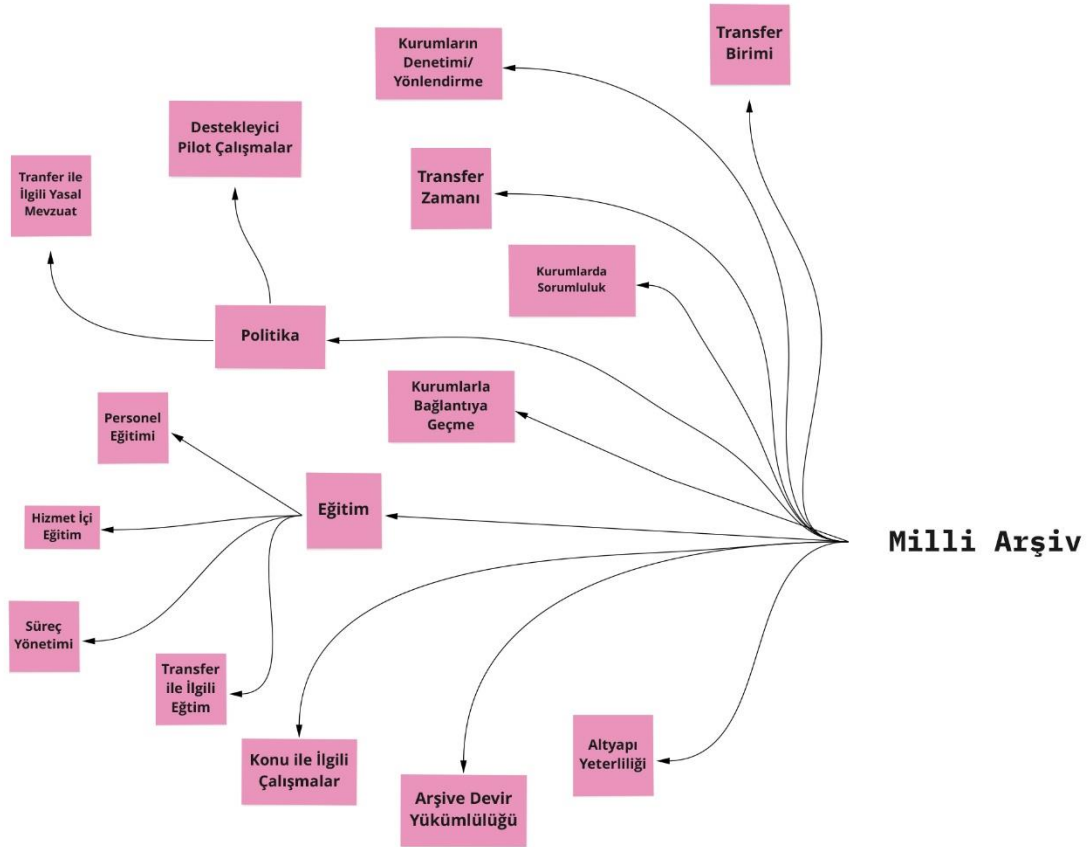


Şekil 16. Kavram haritası transfer süreçleri bölümü

Şekil 16’da dijital belgelerin transfer süreçleri e-değerlendirme, e-ayıklama, hassasiyet değerlendirme, transferi planlama ve kontrol ve erişim olarak haritalandırılmıştır. Bu beş süreç birbiriyle bağlantılı ve birbirini takip eden süreçlerdir. E-değerlendirme sürecinde bir belgenin türü, yapısı, değerlendirme kriterleri aklı gelmelidir. E-değerlendirmede kurumun ihtiyacına ya da belirlediği transfer sürece göre kullanacağı birbirinden farklı makro, mikro, teknik vb. değerlendirme türleri bulunmaktadır. E-ayıklama ile e-değerlendirme süreci de birbiriyle iç içe geçen süreçlerdir. E-ayıklamada uyulması gereken yasal kriterlerin yanı sıra kurumlardaki süreçleri rahatlatarak programlar/yazılımların kullanımı sağlanmalıdır. Hassasiyet değerlendirme süreci en zorlu süreçlerin başında gelirken bu süreci en hafif zorlanmayla atlatılabilmek için düzgün belirlenmiş bir üst veri tanımlama yapısı olmalıdır. Dijital belgelerin gizlilik dereceleri (hizmete özel, gizli, çok gizli) bulunmaktadır ve bu derecelere göre belgeler işlem görmektedirler. Hassasiyet değerlendirme sürecinin başında risk kategorilerinin belirlenmesi ve planlanması son derece önemlidir. Hassasiyet

değerlendirmesinde manuel teknikler yerine teknolojik edinimler kısaca yazılımlar, programlar kullanılmalıdır. Bu süreçlerden sonra kurum ve Milli Arşiv arasında transfer tarihi planlanmalı ve teknik süreçler halledilip transfer yapılmalıdır. Transfer sonrası ise Milli Arşiv tarafından aktarılan verilerin kontrolleri sağlanıp dosyalar erişime açılmalıdır.

6.2.1.5 Milli Arşiv Bölümü



Şekil 17. Kavram haritası milli arşiv bölümü

Milli arşiv bölümü bir dijital belgenin yaşam döngüsü sürecinin son evrelerinden biridir. Milli arşivlerin dijital belgenin bilgi yönetim süreçlerinde üstlenmesi gereken rol ve sorumlulukları vardır. Öncelikle milli arşivlerin her türlü süreç için gerekli olan yasal ve teknik altyapısı bünyesinden barındırması gerekmektedir. Eğitim milli arşivin üstlenmesi gereken bir diğer önemli unsurdur. Tüm süreçlerle ilgili kurumlara eğitimler verilmeli ve denetlemeler yapılmalıdır. Transfer için planlamalar yapılmalı, pilot çalışma gerçekleştirilmeli, transfer yükümlülüğü bulunan kurumlarla bağlantıya geçilmelidir. Milli arşiv kendi bünyesinde transfer için gerekli olan birim ve sorumluları, kilit noktaları belirlemelidir (Şekil 17).

6.3. Analizlerin Değerlendirilmesi

Bu bölümde, anketten elde edilen veriler birtakım analizlere tabii tutulmuştur. Verilerin analizinde SPSS 21 programı kullanılmıştır. Analizlere başlarken verilerin normal dağılıp dağılmadığına bakılmıştır. Normallik dağılımı incelenirken Kolmogorov Smirnov, Shapiro Wilk testi değerleri, basıklık (kurtosis) ve çarpıklık (skewness) değerleri, Q-Q Plot ve histogram analizi değerleri, varyasyon değerleri ele alınmıştır. Değerlendirme sonucu normal çıkan verilere normallik testlerinden regresyon analizi, bağımsız örneklem T testi, anova testi uygulanmıştır. Normal dağılmayan veriler için ise Mann-Whitney U testi uygulanmıştır.

Anketin geçerlik güvenirlik testi için literatürde sıklıkla başvurulanan Cronbach-Alpha değerine bakılmıştır (Bkz. Tablo 58).

Tablo 58. Anketin Cronbach-Alpha değeri

Cronbach-Alpha Değeri	Standartlaştırılmış Cronbach-Alpha Değeri	Madde Sayısı
,800	,798	73

Literatürde, Alfa katsayısının değerlendirilmesinde uyulan değerlendirme kriteri aşağıdaki gibidir.

- $0,00 \leq \alpha < 0,40$ ise ölçek güvenilir değildir.
- $0,40 \leq \alpha < 0,60$ ise ölçek düşük güvenirliktedir.
- $0,60 \leq \alpha < 0,80$ ise ölçek oldukça güvenirlidir.
- $0,80 \leq \alpha < 1,00$ ise ölçek yüksek derecede güvenilir bir ölçektir (Özdamar, 1997 s.500).

Doğuştan dijital belgelerin bilgi yönetim süreçlerine yönelik anketteki 73 maddenin Cronbach-Alpha değeri güvenirliği %80,0 bulunmuştur. Bu değer, maddelerin güvenirliğini yüksek derecede yeterli olduğunu göstermektedir. Yani anketin güvenirliği yüksek derece güvenirlidir.

6.3.1. Araştırma Hipotezleri

Çalışmada toplam 14 hipotez belirlenmiştir. Belirlenen her bir hipotez için gerekli testler yapılmış ve sonuçları yorumlanmıştır. Belirlenen hipotezlerin 10 tanesi kabul edilmiş, 4 tanesi ise reddedilmiştir.

Tablo 59. Araştırma hipotezleri

Hipotez 1	Dijital belgelerin milli arşive transfer sürecine dair bilinç ile Devlet Arşivleri Başkanlığı etkinliği arasında anlamlı ve pozitif yönlü bir ilişki bulunmaktadır.
Hipotez 2	Dijital belgelerin bir bilgi varlığı olarak görülmesi ile kurumsal politika oluşturma arasında anlamlı bir ilişki vardır.
Hipotez 3	e-değerlendirme, e-ayıklamayı doğrudan ve pozitif olarak etkilemektedir.
Hipotez 4	Belge yönetim politikasına sahip olmak, dijital belgelerin oluşturulmasında "gizlilik" unsurunu olumlu ve pozitif yönde etkilemektedir.
Hipotez 5	Dijital belgelerin saklama sürelerinin belirlenmesi, standart dosya planına uyumu olumlu ve pozitif yönde etkilemektedir.
Hipotez 6	Kurumsal bilgi yönetim süreçlerinin zorluğu, eğitime ihtiyaç duyulan alanları artırmaktadır.
Hipotez 7	Dijital belge yönetimine dair eğitimler, EBYS yeterliliğini artırmaktadır.
Hipotez 8	Devlet arşivlerinin kurumlara desteği, kurumların dijital belgeleri arşive devretme yükümlülüğünün farkında olmasını anlamlı ve olumlu yönde etkilemektedir.
Hipotez 9	Dijital süreklilik farkındalığı dijital belgelerin uzun vadede erişilebilir olması çalışmalarını artırmaktadır.
Hipotez 10	Kurumlarda e-arşiv sistemi bulunması ve hassasiyet değerlendirmesinin etkinliği arasında anlamlı ve pozitif yönlü bir ilişki bulunmaktadır.
Hipotez 11	Kurum türüne göre dijital süreklilik farkındalığı anlamlı ve pozitif yönde ayrılmaktadır.
Hipotez 12	Kurumların EBYS'yi değiştirmeleri, uzun vadeli korumadaki kaygıyı artırmaktadır.
Hipotez 13	Dijital belgelerin saklandığı formatın çeşitliliği, uzun vadede erişim çalışmalarını artırmaktadır.
Hipotez 14	Dijital süreklilik farkındalığı, dijital sürekliliğin iyi yönetilmesini olumlu ve pozitif yönde etkilemektedir.

6.3.2. Basit Doğrusal Regresyon Testi Analiz ve Yorumları

Regresyon analizi normal dağılan verilere uygulanan bir analiz türüdür. Regresyon analizi, bir bağımlı değişken (Y) ve bir bağımsız değişken (X) arasındaki matematiksel ilişkiyi inceler (Özdamar, 2004, s. 188). Çalışmanın bu kısmında, dijital belgelerin milli arşive transfer üzerindeki bilinç ve Devlet Arşivleri Başkanlığı'nın uygulamaları, dijital belge yönetimine dair eğitimler ile EBYS yeterliliği, Devlet arşivlerinin kurumlara desteği ile kurumların dijital belgeleri arşive devretme yükümlülüğünün farkındalığı, kurumların uzun vadeli korumadaki kaygısı ile EBYS'yi değiştirme politikaları arasındaki ilişkileri ölçmek için oluşturulan hipotezler basit

doğrusal regresyon analizine tabi tutulmuştur. Yapılan basit doğrusal regresyon analizi sonucu elde edilen bulgular Tablo 60'ta verilmiştir.

Tablo 60. H1-H7- H8-H12 hipotezleri regresyon analizi testi sonuçları

Hipotez	Değişken 1 (Bağımsız)	Değişken 2 (Bağımlı)	R ²	β	F	t	p	Sonuç
H1	Arşive transfer bilinci	DAB etkinliği	,223	0,420	25,278	5,028	,000	Kabul
H7	Eğitim	EBYS yeterliliği	,149	-,386	20,695	-4,549	,000	Kabul
H8	Transfer için destek	Devretme yükümlülüğü	,105	0,155	13,808	3,716	,000	Kabul
H12	Uzun vadeli koruma kaygısı	EBYS değiştirme	,031	-,177	3,818	-1,954	,053	Red

H1: Dijital belgelerin milli arşive transfer sürecine dair bilinç (Q48) ile DAB etkinliği (Q51) arasında anlamlı ve pozitif yönlü bir ilişki bulunmaktadır.

Yorum: Tablo 60 incelendiğinde, kurumların dijital belgelerini milli arşive transfer etme konusunda herhangi bir çalışması olmasa da, devlet arşivlerinin konu hakkında kurumlara olası bir desteği ve girişimleri (destek, politika geliştirme) ile bir farkındalık oluşabileceğine dair inanç görülmektedir. Kurumlar üzerindeki dijital belgelerin milli arşive transfer sürecine dair bilinç ile Devlet Arşivleri Başkanlığı'nın potansiyel desteği arasında anlamlı ve pozitif yönlü bir ilişki bulunmaktadır ($F=25,278$; $p<0,01$). Regresyon analizi sonucunda kurumlardaki Devlet Arşivleri Başkanlığı çalışmalarının (β : ,420, $p<0,01$) bilgi profesyonellerinin dijital belgeleri milli arşive transfer ile ilgili çalışmaları üzerinde olumlu etkisi olduğu görülmektedir. Bu doğrultuda dijital belgelerin milli arşive transfer sürecine dair bilinç ile Devlet Arşivleri Başkanlığı eylemleri arasında anlamlı ve pozitif yönlü bir ilişki olduğunu savunan H1 hipotezinin kabul edilmesi gerekmektedir ($F=25,278$; $p<0,01$). Devlet Arşivleri Başkanlığı'nın kurumlara vermiş olduğu potansiyel destek değişkeninin toplam varyasyonun %22,3'ü açıklanabilmektedir ($R^2 = \%22,3$).

Yapılan uluslararası bir çalışmada, İngiltere'deki devlet dairelerinin ne zaman içinde belgelerini arşive transfer edecekleri sorulduğunda, kurumların arşive transferi ile ilgili bilinçlerinin var olduğunu, bazı kurumların arşive transfer işlemlerini başlattığını,

bazılarının çalışmaları sürdürdüğü ve yine bazı kurumların transfer için tarihlerinin belirlendiği sonucuna ulaşılmıştır. Bu durumun İngiltere’de Milli Arşivin kurumlarla bağlantıya geçmesinden, denetim ve kontrol yapılmasından, konu ile ilgili Milli Arşivin yine çalışmalar yapıp bu çalışmaları kendi sayfalarında erişime açmasından, yasal zemini (politika, strateji) doldurmasından kaynaklı olduğu görülmektedir (Özdemir, 2018, s. 231-232). Bu sebeple Milli arşivlerin kendi içlerinde yaptığı çalışmalar, kurumlarla iletişim ve iş birliği halinde olmaları, kurumlardaki milli arşive transferini etkilemektedir.

H7: Dijital belge yönetimine dair eğitimler, EBYS yeterliliğini artırmaktadır.

Yorum: Kurumlarda dijital belge yönetimine dair verilen eğitimler ile uygulama aşamasında personelin EBYS kullanımı arasında istatistiki açıdan anlamlı bir ilişki olduğu görülmektedir ($F=20,695$; $p<0,01$). Normalde de böyle bir ilişkinin olması arzu edilir. Kurumlarda verilen her türlü arşiv ve belge yönetimi eğitimi, süreçlerdeki etkinliği ve farkındalığı da artıracaktır. Yapılan regresyon analizi sonucunda kurumlarda verilen eğitimlerin uygulama aşamasında EBYS kullanımını anlamlı bir şekilde etkilediği ortaya çıkmaktadır ($p<0,01$). Test sonuçlarına göre H7 hipotezi ($F=20,695$; $p<0,01$) kabul edilebilir görülmektedir. EBYS yeterliliği değişkenindeki toplam varyasyonun %14,9’u açıklanabilmektedir ($R^2 = \%14,9$).

Sakarya Üniversitesi’nde kullanılan EBYS’nin oradaki personel tarafından kabul edilebilirliğine yönelik yapılan bir çalışmada, personelin EBYS kullanım düzeyleri işle ilgililik, algılanan kullanım kolaylığı, niyet faktörü ve gibi çeşitli faktörlerle ölçülmüştür. Çalışma sonucu ilgili faktörlerin personelin EBYS kullanımı üzerinde olumlu etkisi olduğu ortaya çıkmıştır. Bu faktörler içerisinde en çok etkiyi gösteren ise algılanan fayda olarak ortaya çıkmıştır (Cibaroğlu ve Turan, 2018, s.215). Bakıldığından kurumlarda verilen dijital belge yönetimine dair eğitimlerin ilgili faktörlerle doğrudan bağlantısı olduğunu söylemek mümkündür. Çünkü kurumlarda verilen eğitimler, personelin algılanan faydasını, niyeti, algılanan kullanım kolaylığını doğrudan etkilemektedir.

H8: Devlet arşivlerinin kurumlara desteği, kurumların dijital belgeleri arşive (Milli Arşiv) devretme yükümlülüğün farkında olmasını anlamlı ve olumlu yönde etkilemektedir.

Yorum: Kurumların sahip oldukları dijital belgelerin arşive transferi için devlet arşivleri ile bağlantıya geçilmesinin, kurumların devlet arşivlerine belgeleri devretme yükümlülüğü üzerindeki regresyon sonuçları incelendiğinde, devlet arşivlerinin

kurumlara desteğinin kurumların devlet arşivlerine belgeleri devretme yükümlülüğü üzerindeki etkisini sınavan hipotez istatistiki olarak ($F=13,808$; $p<0,01$) anlamlı görülmektedir. Bu bağlamda H8 hipotezi desteklenebilir niteliktedir. Sonuç olarak devlet arşivlerinin kurumlara desteği, kurumların devlet arşivlerine belgeleri devretme yükümlülüğünün farkında olmasını anlamlı ve olumlu yönde etkilemektedir. Basit bir mantıkla; devlet arşivlerinin kurumlara dijital transfer için bir denetleme/destek görevini ifa etmesi, kurumları cesaretlendirebilir ve hatta somut bir çalışma başlatılmasını sağlayabilir. Kurumların dijital belgeleri arşive (Milli Arşiv) devretme yükümlülüğü değişkenindeki toplam varyasyonun %10,5'i açıklanabilmektedir ($R^2 = \%10,5$).

Ülkenin arşiv konusunda en yetkili birimi olan milli arşivler belgelerin tüm süreçlerinde ve erişiminden sorumludur. Bu sorumluluk kurumlardaki işleyişi denetleme, yasal zemini doldurma, yol gösterici olma, rol ve sorumluluklarını yerine getirme, kurumlara rehber olma gibi eylemlerle desteklenmelidir. Yapılan bir çalışmada kurumların dijital belgelerini transfer edebilmeleri için milli arşiv tarafından kurumlara tavsiye, rehberlik, teknoloji destekli süreçlere teşvik etmek gibi eylemleri sağlamaları gerektiğinin altı çizilmiştir (Özdemir, 2019, s.237).

H12: Kurumların uzun vadeli korumadaki kaygısı, EBYS'yi değiştirme politikaları üzerinde etkilidir.

Yorum: Kurumların EBYS kullanımını ve belgelerin uzun süre korunmasını etkileyecek çeşitli kaygılar (mevcut yazılım ve donanımın güncel tutulması ve korunmasının zor olması, içerik biçimlerinin karmaşık ve kırılgan olması, yasal ve politik risklerin var olması, hacim veya karmaşıklık kapsamında içerik toplamının zor olması, yetersiz personele sahip olmak, içeriğin yetersiz tanımlanması kullanımını ve keşfedilmesini zorlaştırabilmesi ve dosya formatlarının hızlı değişiklik göstermesi ve eski dosya formatlarının okunamaması) ile EBYS uygulamasının çeşitli etkenler neticesinde değiştirilmesi (maliyet, işlevsellik, üst yönetim kararı) üzerinde etkili olduğunu (daha doğrusu pozitif ve doğrusal) tahmin eden H12 reddedilmiştir ($F=3,818$; $p>0,01$). Normalde de kurumların uzun süreli koruma kaygısı neticesinde EBYS'yi değiştirmemeleri beklenir. EBYS'nin aralıklarla değiştirilmesi demek, zaten uzun süreli koruma konusunda bir farkındalığın olmadığı anlamına gelmektedir. Ayrıca genel anlamda bilişim sistemleri yatırımlarının maliyet unsuru olarak görülmemesi gerektiği de burada ortaya çıkmaktadır.

Kurumlarda EBYS'nin değişmesi eski sistem ve yeni sistem arasında hemen uyum sürecine girememe, personel alışkanlıklar sebebiyle değişimlere ayak uyduramama gibi sebepler bulunmaktadır. EBYS'deki başarısızlıkların sebeplerini araştıran bir çalışmada, problemlerin “yeniliğe ve değişime karşı direnç, geleneksel alışkanlıkları terk edememe, mevcut statüyü koruma, elektronik sistemlere ve teknolojiye olan güvensizlik, uygulama yazılımının kullanıcı dostu olmaması ve doğru öğretim metotlarının seçilmemesi” sebebi olduğunu ortaya çıkmıştır. Bunun sorunun aşılmasının çözümü olarak ise EBYS'de personel farkındalığının artırılması olduğu savunulmuştur (Saydam, 2015, s. 24-25). EBYS sürecinin devamlılık uzun vadeli korumayı da artırıcı sebeplerden biri olacaktır. Bu anlamda çeşitli sebeplerle kurumlardaki EBYS'lerin sıklıkla değiştirilmemesi gerekmektedir. Zira bu değişim uzun vadeli korumayı da olumsuz yönde etkileyecek bir unsur olarak karşımıza çıkacaktır.

6.3.3. Bağımsız Örneklem T Testi Analizleri ve Yorumları

Parametrik analiz tekniklerinden biri olan T testi, sosyal bilimlerin birçok alanında yaygın olarak kullanılan testlerden biridir. T testi iki grup arasında incelenen konu açısından anlamlı bir fark olup olmadığını ya da konunun öngörülen bir değerden farklı olup olmadığını ölçmek için kullanılır (Coşkun, Altunışık ve Yıldırım, 2019, s.214-215). Tablo 61'de t testi analiz sonuçları gösterilmektedir.

Tablo 61. H2 ve H4 hipotezleri T testi analizi sonuçları

t-Testi	Cevap	n	Ortalama	Standart Sapma	Levene's	Serbestlik (df)	t	p
S12>S36	Evet	15	1,13	,352	,000	25,350	-3,239	,003
	Hayır	105	1,48	,556				
S36>S20	Evet	15	3,60	,737	,001	23,153	2,861	,009
	Hayır	105	2,98	1,056				

H2: Dijital belgelerin bir bilgi varlığı olarak görülmesi (S12) ile kurumsal politika oluşturma (S36) arasında anlamlı bir ilişki vardır.

Yorum: Kurumlarda her bir birimin bilgi varlığı envanterine sahip olması ile kurumsal politika oluşturma arasındaki ilişki için yapılan t testi sonrasında her bir kurumun bir bilgi varlığı envanterine sahip olması ile kurumsal bir belge yönetim politikasına sahip olma arasında anlamlı bir fark bulunmuştur ($p<0,05$). Bu sebeple H2 hipotezi kabul edilmiştir. Kurumlarında bir belge yönetim politikasına sahip olmayanlar

($\bar{x}=1,48$) belge yönetim politikasına sahip olanlara göre bilgi varlığı envanterine sahip olma ile kurumsal bir belge yönetim politikasına sahip olma arasındaki anlamlı ilişkinin daha farkındadır ($\bar{x}=1,13$).

Kurumlarda bilginin varlık olarak kabul edilmesi kurumsal bilgi süreçlerinin de düzgün işlemesine katkı sağlayacaktır. Aksi taktirde o kurumdaki bilginin sürekliliğinin sağlanması mümkün değildir. Bu sebeple de kurumlarda bilgi varlık envanterlerinin olması gerekir. Kurumlarda bilginin varlık olarak kabul edilmesi, bilgi envanterlerinin oluşturulması süreci ile devam etmelidir. Bilgi varlık envanterleri sayesinde eğer kurumda bir bilgi güvenlik olayı meydana gelirse, bilgilerin bütünlüğü, erişilebilirliği ve gizliliği korunacaktır (Özdemir, 2017, s. 49). Özellikle dijital çağda kurumlarda karşılaşılan dijital zorluklara karşı bilgi varlıklarının belirlenmesi ve düzgün şekilde yönetilmesinin önemi dikkat çekmektedir (Aydın ve Saydam, 2019, s. 4). Tüm bu sürecin düzgün işleyebilmesinin bir ayağı da her kurumun bir belge yönetim politikasına sahip olması gerekliliğidir. Personelin her ne kadar kurumun sahip olduğu bilgi varlıkları bilmesi, varlık envanteri oluşturması bu bilincin farkında olması önemli olsa da tek başına yeterli olmayacaktır. Kurumsal bilgi yönetim sürecinin düzgün işlemesi için belge yönetim politikaları, kurumsal politikalar bu kapsamda hayati rol oynayacaktır. Politikalar yasal zorunluk barındırdığı ve izlenecek adımlar konusunda yol gösterdiği için belge yönetim süreçlerinin ilerlemesine büyük katkı sağlamaktadırlar. Bu sebeple dijital belgelerin bir bilgi varlığı olarak görülmesi ile kurumsal politika oluşturma arasında anlamlı bir ilişki vardır hipotezi desteklenmektedir.

H4: *Belge yönetim politikasına sahip olmak (S36) dijital belgelerin oluşturulmasında "gizlilik" (S20) unsurunu olumlu ve pozitif yönde etkilemektedir.*

Yorum: Kurumlarda dijital belge oluştururken dikkat edilen gizlilik unsuru ile bir belge yönetimi politikasına sahip olma arasındaki ilişkiyi ölçen t testi sonrasında bir kurumun belge yönetimi politikasına sahip olması ile dijital belge oluştururken dikkat ettiği gizlilik unsuru arasında anlamlı bir ilişki bulunmuştur ($p<0,05$). Bu sebeple H4 hipotezi kabul edilmiştir. Kurumlarında bir belge yönetim politikasına sahip olanlar ($\bar{x}=3,60$) belge yönetim politikasına sahip olmayanlara göre ($\bar{x}=2,98$) bir dijital belge oluştururken gizlilik unsuruna önem bilincine daha çok sahiptirler.

Bir belge yönetimi politikası oluştururken öncelikle belgenin yapısını bilmek gerekmektedir. Belge yönetim politikası hali hazırda belgenin yaşam döngüsü içerisinde

belge yönetim süreçlerini kurumsal anlamda belirlemeye yardımcı olur. Belgeyi oluşturan birtakım unsurların içerisinde ise gizlilik faktörü önem kazanmaktadır. Bir belgeyi oluştururken gizlilik derecesi alanlarının (Hizmete Özel, Gizli, Çok Gizli) belirtilmesi önemlidir. Gizlilik unsuru bir belgenin hassasiyet değerlendirmesinden milli arşive transferine kadar birçok süreci etkilemektedir. Bu sürecin düzgün ilerleyişinde yine kurumun belge yönetim politikasına sahip olması etkili olmaktadır. Belge yönetim politikalarında hassas belge yönetim süreçleri gibi bir başlık altında belgenin gizlilik dereceli alanları ile ilgili maddelerin belirlenmesi bu sürecin başlı başına düzgün ilerlemesini sağlayacaktır. Bunu ancak belge yönetim politikası gibi kurumsal politikalarla, yönetmeliklerle yapmak mümkündür. Dolayısıyla bir kurumun belge yönetim politikasına sahip olması dijital belgelerin oluşturulmasında “gizlilik” faktörünü olumlu ve pozitif yönde etkilemektedir.

6.3.4. ANOVA Testi Analizleri ve Yorumları

“Anova testi ya da tek yönlü varyans analizi, k bağımsız ya da k bağımlı gruptan elde edilen verilerin grup ortalamalarının ya da işlem ortalamalarının farklılığını test etmek için yararlanılan bir yöntemdir” (Özdamar, 1997, s.275). Anova testi ikiden fazla grubun karşılaştırılması için kullanılmaktadır. Farkın hangi gruptan kaynaklandığını bulmak için ise Post-hoc testi uygulanır. Çalışmada, homojen dağılan veriler için post-hoc testlerinden Tukey testi, homojen dağılmayan veriler için ise Tamhane testi kullanılmıştır. Anova testi parametrik bir testtir. Toplamda çalışma için belirlenen altı hipotez Anova testi ile ölçülmüştür. Aşağıdaki tablolarda Anova testlerine ait sonuçlar gösterilmektedir.

Tablo 62. H3 hipotezi anova testi sonuçları

e-ayıklama	N	Ortalama	Standart Sapma	Varyans Kaynağı	Kareler Toplamı	Df	Kareler Ortalaması	F	P	Homojenlik
Geleneksel	9	1,8889	1,36423	Gruplar Arası	57,008	2	28,504			
Yapmayanlar	102	3,7549	,89483							
Fikri olmayanlar	9	5,4444	1,66667	Grup İçi	117,984	117	1,008	28,266	,000	,015*
Toplam	120	3,7417	1,21265	Toplam	174,992	119				

*0.05 düzeyinde anlamlıdır (p>0,05)

H3: e-değerlendirme ve e-ayıklama arasında anlamlı ve pozitif yönlü bir ayrışma bulunmaktadır.

Yorum: Tablo 62’de kurumlarda e-değerlendirme ve e-ayıklama arasındaki farkı gösteren Anova sonuçlarını sunulmaktadır. Yapılan Anova testi sonucuna göre e-değerlendirme ve e-ayıklama arasında anlamlı ve pozitif yönlü bir ayrışma olduğu bulunmuştur ($p=0,000<0,05$). Bu sebeple H3 hipotezi kabul edilmiştir. Bir belge üzerinde değerlendirme ve ayıklama süreçleri birbiriyle iç içe geçen süreçlerdir. Anova sonucuna göre e-değerlendirme ve e-ayıklama arasında bağlantı çıkması da bu durumu kanıtlar niteliktedir. Çünkü bir belgenin değerlendirme sürecinde belgenin arşivsel bağlamda değerine bakarken, ayıklama sürecinde arşive gidecek ve gitmeyecek materyallerin belirlenip çeşitli yöntemlerle ayıklanmasının bakılmaktadır. Bakıldığında süreçler birbiri ile iç içedir.

Tablo 62 varyansların homojen olmadığını ($p<0,05$) göstermektedir. Bu nedenle hangi gruplar arasında anlamlı fark olduğunu bulabilmek için post hoc testlerinden heterojen varyanslı dağılımlarda kullanılan Tamhane’s T2 tekniğine başvurulmuştur.

Tablo 63. H3 hipotezi Tamhane’s T2 testi sonuçları

		Ortalama fark	Standart hata	(Sig) P
e-değerlendirme				
Geleneksel değerlendirme yapanlar	e-değerlendirme yapmayanlar	-1,86601*	,46329	,010
	Fikri olmayanlar	-3,55556*	,71794	,000
e-değerlendirme yapmayanlar	Geleneksel değerlendirme yapanlar	1,86601*	,46329	,010
	Fikri olmayanlar	-1,68954*	,56258	,047
Fikri olmayanlar	Geleneksel değerlendirme yapanlar	3,55556*	,71794	,000
	e-değerlendirme yapmayanlar	1,68954*	,56258	,047

Tablo 63’te görüldüğü üzere, Tamhane’s T2 test sonucuna göre e-değerlendirme ve e-ayıklama ile ilgili gruplar arasında anlamlı ve pozitif yönlü bir ayrışma olduğu görülmektedir. Geleneksel değerlendirme yapanlar e-değerlendirme yapmayanlar ($p<0,05$) ve fikri olmayanlara ($p<0,05$) göre daha azdır ve anlamlı bir şekilde ayrılmaktadır. E-değerlendirme yapılmıyor diyenler ile geleneksel değerlendirme yapanlar ($p<0,05$) ve fikri olmayanlar ($p<0,05$) arasında anlamlı farklılık bulunmaktadır. Yine bir fikrim yok diyenlerle geleneksel değerlendirme yapanlar ($p<0,05$) ve e-değerlendirme yapmayanlar ($p<0,05$) arasında anlamlı farklılık vardır. Değerlendirme ve

ayıklama arşivlerin hayati işlevleri olarak görülmektedir. Bu değerlendirme ve ayıklama üzerine daha fazla araştırma ve uygulama yapmak önemli görülmektedir (Lee, 2018, s. 2724).

Tablo 64. H5 hipotezi Anova testi sonuçları

Standart dosya planına uyum	N	Ortalama	Standart Sapma	Varyans Kaynağı	Kareler Toplamı	df	Kareler Ortalaması	F	P	Homojenlik
Belgeyi üretirken	32	3,69	,859	Gruplar Arası	13,596	5	2,719	3,104	,012	,428*
Üretmeden önce	7	3,29	1,254							
Son işlem yapıldıktan sonra	12	3,58	1,084							
Arşivlerken	15	4,00	,756	Grup İçi	99,871	114	,876			
Yapılmıyor	47	3,26	,966							
Diğer	7	3,29	1,254							
Toplam	120	3,57	,976	Toplam	113,467	119				

* 0.05 düzeyinde anlamlıdır ($p>0,05$)

H5: Dijital belgelerin saklama sürelerinin belirlenmesi, standart dosya planına uyumunu olumlu ve pozitif yönde etkilemektedir.

Yorum: Tablo 64'te yapılan Anova testi sonucuna göre kurumlarda dijital belgelerin saklama sürelerinin belirlenmesinin standart dosya planına uyumunu olumlu ve pozitif yönde etkilediği görülmektedir ($p<0,05$). Yani, kurumların dijital belgelerini saklama süreleri belirlemeleri ile standart dosya planına uymaları arasında anlamlı bir ilişki bulunmaktadır. Bu sonuca bağlı olarak H5 hipotezi kabul edilebilir görülmektedir. Tablo 64 varyansların homojen olduğu ($p>0,05$) göstermektedir. Bu nedenle hangi gruplar arasında anlamlı fark olduğunu bulabilmek için post hoc testlerinden homojen varyanslı dağılımlarda kullanılan Tukey testi tekniğine başvurulmuştur.

Standart dosya planı, belgelerin konuları bakımından ilgili yerlerinde olmalarını sağlar. Bunun dışında belgelerin saklama sürelerinin belirlenmesinde bir dayanaktır. Standart dosya planı sayesinde belgelerin saklama süresi sonunda ayrıca milli arşive devredilip devredilmeyeceği de belirlenmektedir. Bu bağlamda dijital belgelerin saklama sürelerinin belirlenmesi, standart dosya planına uyumu olumlu ve pozitif yönde etkilemektedir hipotezini destekler niteliktedir.

Tablo 65. H5 hipotezi Tukey testi sonuçları

Saklama Süreleri		Ortalama	Standart	P
		Fark	Hata	
Belgeyi üretirken	Belgeler oluşturulmadan önce	.402	.391	.907
	Belge üzerinde son işlem yapıldıktan sonra	.104	.317	.999
	Belgeyi arşivlerken	-.313	.293	.893
	Belirlenmemektedir.	.432	.215	.341
	Diğer	-.741	.391	.409
Belgeler oluşturulmadan önce	Belgeyi üretirken	-.402	.391	.907
	Belge üzerinde son işlem yapıldıktan sonra	-.298	.445	.985
	Belgeyi arşivlerken	-.714	.428	.556
	Belirlenmemektedir.	.030	.379	1.000
	Diğer	-1.143	.500	.209
Belge üzerinde son işlem yapıldıktan sonra	Belgeyi üretirken	-.104	.317	.999
	Belgeler oluşturulmadan önce	.298	.445	.985
	Belgeyi arşivlerken	-.417	.363	.859
	Belirlenmemektedir.	.328	.303	.887
	Diğer	-.845	.445	.408
Belgeyi arşivlerken	Belgeyi üretirken	.313	.293	.893
	Belgeler oluşturulmadan önce	.714	.428	.556
	Belge üzerinde son işlem yapıldıktan sonra	.417	.363	.859
	Belirlenmemektedir.	.745	.278	.087
	Diğer	-.429	.428	.917
Belirlenmemektedir.	Belgeyi üretirken	-.432	.215	.341
	Belgeler oluşturulmadan önce	-.030	.379	1.000
	Belge üzerinde son işlem yapıldıktan sonra	-.328	.303	.887
	Belgeyi arşivlerken	-.745	.278	.087
	Diğer	-1.173*	.379	.029
Diğer	Belgeyi üretirken	.741	.391	.409
	Belgeler oluşturulmadan önce	1.143	.500	.209
	Belge üzerinde son işlem yapıldıktan sonra	.845	.445	.408
	Belgeyi arşivlerken	.429	.428	.917
	Belirlenmemektedir.	1.173*	.379	.029

Hipotez 5 için anlamlı bir farklılık saptanmış ve farklılığın hangi gruplardan kaynaklandığını belirlemek için Tukey testine başvurulmuştur (Tablo 65). Tukey testi sonucuna göre p değerleri diğer seçeneğini işaretleyenler hariç 0,05'ten büyük olduğu için gruplar arasında dijital belgelerin saklama sürelerini belirleme konusunda anlamlı bir fark bulunamamıştır ($p>0,05$). Kurumlarda bulunan personelden dijital belgeler için saklama süresi belirlenmemektedir diyenler ve diğer seçeneğini işaretleyenler arasında bir ilişki bulunmaktadır ($p<0,05$). Diğer seçeneğini işaretleyenler dijital belgeler için

saklama sürelerinin devlet arşivleri yönetmeliğine göre belirlendiğini, konunun standartlaşması için çalışmaların devam ettiğini belirtmişlerdir. Kurumlarda dijital belgeler için saklama sürelerinin belirlenmemesi de konu hakkında farkındalık eksikliği olduğunu işaret etmektedir. Aynı zamanda dijital ortamda oluşturulan tüm belgeler fiziksel ortamdaki belgeler gibi dosya bütünlüğü içinde olmalıdır (Dede ve Akbayır, 2017, s. 290). Dosya bütünlüğü için ise hem belgelerin standart dosya planına uyması hem de saklama sürelerinin belirlenmesi elzemdir.

Tablo 66. H6 hipotezi Anova testi sonuçları

Eğitime Duyulan İhtiyaç	Varyans Kaynağı	Kareler Toplamı	df	Kareler Ortalaması	F	P	Homojenlik
Ayıklama	Gruplar Arası	9,876	4	2,469	5,590	,000	,518*
	Grup içi	50,791	115	,442			
	Toplam	60,667	119				
Hassasiyet değerlendirmesi	Gruplar Arası	6,323	4	1,581	3,699	,007	,725*
	Grup içi	49,144	115	,427			
	Toplam	55,467	119				

* 0.05 düzeyinde anlamlıdır (p>0,05)

H6: Kurumsal bilgi yönetim süreçlerinin zorluğu eğitime ihtiyaç duyulan alanları artırmaktadır.

Yorum: Tablo 66’da yapılan Anova testi sonucuna göre kurumsal bilgi yönetim süreçlerinin zorluğu eğitime ihtiyaç duyulan alanları artırdığı görülmektedir (p<0,05). Doğal olarak kurumlarda bilgi yönetim süreçlerinde eğitime ihtiyaç duyulan alanlarla bilgi yönetim süreçlerinde zorluk çekilen alanlar arasında anlamlı bir ilişki bulunmaktadır. Bu sonuca bağlı olarak H6 hipotezi kabul edilebilir görülmektedir. Tablo 66 varyansların homojen olduğunu (p>0,05) göstermektedir. Bu nedenle hangi gruplar arasında anlamlı fark olduğunu bulabilmek için post hoc testlerinden homojen varyanslı dağılımlarda kullanılan Tukey testi tekniğine başvurulmuştur.

Tablo 67. H6 hipotezi Tukey testi sonuçları

Bilgi Yönetim Süreçleri			Ortalama	Standart	
			Fark	Hata	P
Dijital belgelerin ayıklanması	,17	,33	,458	,214	,212
		,50	-,226	,194	,770
		,67	,208	,285	,949
		,83	-,372	,165	,168
	,33	,17	-,458	,214	,212
		,50	-,685*	,216	,017
		,67	-,250	,301	,921
		,83	-,830*	,191	,000
	,50	,17	,226	,194	,770
		,33	,685*	,216	,017
		,67	,435	,287	,555
		,83	-,145	,167	,908
	,67	,17	-,208	,285	,949
		,33	,250	,301	,921
		,50	-,435	,287	,555
		,83	-,580	,268	,201
	,83	,17	,372	,165	,168
		,33	,830*	,191	,000
		,50	,145	,167	,908
		,67	,580	,268	,201
Hassasiyet Değerlendirmesi	,17	,33	,375	,211	,392
		,50	-,147	,191	,939
		,67	,375	,281	,670
		,83	-,245	,162	,559
	,33	,17	-,375	,211	,392
		,50	-,522	,213	,109
		,67	,000	,296	1,000
		,83	-,620*	,188	,011
	,50	,17	,147	,191	,939
		,33	,522	,213	,109
		,67	,522	,282	,351
		,83	-,098	,165	,975
	,67	,17	-,375	,281	,670
		,33	,000	,296	1,000
		,50	-,522	,282	,351
		,83	-,620	,264	,137
	,83	,17	,245	,162	,559
		,33	,620*	,188	,011
		,50	,098	,165	,975
		,67	,620	,264	,137

Hipotez 6 için anlamlı bir farklılık saptanmış ve farklılığın hangi gruplardan kaynaklandığını belirlemek için Tukey testine başvurulmuştur (Tablo 67). Tablo 67'deki 17'lik dilim dijital belgelerin ayıklanması, 33'lük dilim dijital belgelerin değerlendirilmesi, 50'lik dilim dijital belgelerin hassasiyet değerlendirmesi, 67'lik dilim dijital sürekliliği, 83'lük dilim ise dijital belgelerin korunmasını ifade etmektedir. Tablo 67'de dijital belgelerin ayıklanması ve hassasiyet değerlendirmesi eğitimi için iki ayrı Tukey testi sonucu verilmiştir.

Dijital belgelerin ayıklanması eğitimi için yapılan Tukey testi sonucuna göre 33'lük dilimde yer alan cevaplar (Dijital belgelerin değerlendirilmesi), 50'lik dilimde yer alan cevaplara (Hassasiyet değerlendirmesi aşaması) göre anlamlı bir şekilde ayrılmaktadır ($p=,017$; gösterim: $p<0,05$; ortalama fark $-,685^*$). Her iki soru ve cevapların tümü bağlamında düşünüldüğünde kurumlar; hassasiyet değerlendirmesi aşamasında, dijital belgelerin değerlendirilmesi aşamasına göre daha çok zorlanacaklarını düşünüyor olabilirler. - yönlü farklılık, ilişkinin negatif yönlü olduğunu gösteriyor. Böylece 39. soruya dijital belgelerin ayıklanması şeklinde cevap verenler; ayıklama eğitimi bağlamında düşünüldüğünde değerlendirme ve hassasiyet değerlendirmesinde daha çok zorlanacaklarını düşünüyorlar. Tablo 67'ye göre 33'lük dilimde yer alan cevaplar (Dijital belgelerin değerlendirilmesi), 83'lük dilimde yer alan cevaplara (Dijital belgelerin korunması) göre anlamlı bir şekilde ayrılmaktadır ($p=,000$; gösterim: $p<0,05$; ortalama fark $-,830$). Elde edilen bulgulara göre dijital belgelerin değerlendirilmesi aşaması, korunması aşamasına göre daha hoş görülebilir gözükmektedir. Bu bağlamda, katılımcılar dijital belgelerin korunması konusunda daha çok zorlanacaklarını düşünmektedirler.

Dijital belgelerin hassasiyet değerlendirmesi eğitimi için yapılan Tukey testi sonucuna göre 33'lük dilimde yer alan cevaplar (Dijital belgelerin değerlendirilmesi), 50'lik dilimde yer alan cevaplara (Hassasiyet değerlendirmesi aşaması) göre anlamlı bir şekilde ayrılmaktadır ($p=,011$; gösterim: $p<0,05$; ortalama fark $-,620^*$). Her iki soru ve cevapların tümü bağlamında düşünüldüğünde kurumlar; dijital belgelerin değerlendirilmesi aşamasında, dijital belgelerin hassasiyet değerlendirilmesi aşamasına göre daha çok zorlanacaklarını düşünmektedirler. - yönlü farklılık, ilişkinin negatif yönlü olduğunu göstermektedir. Böylece 39. soruya dijital belgelerin hassasiyet değerlendirmesi şeklinde cevap verenler; hassasiyet değerlendirmesi eğitimi bağlamında düşünüldüğünde dijital belgelerin değerlendirmesinde ve hassasiyet değerlendirmesinde

(ayrı ayrı olarak) daha çok zorlanacaklarını düşünmektedirler. Genel olarak tablo kısaca yorumlandığında, dijital belgelerin değerlendirilmesi ve hassasiyet değerlendirilmesi aşamaları yani bu iki adım en fazla zorlanılacak bilgi yönetim süreçlerinin başında geldiği düşünülmektedir. Dijital belgelerin ayıklanması dijital belgelerin hassasiyet değerlendirmesi eğitimlerini tetiklediği anlaşılmaktadır.

Tablo 68. H9 hipotezi Anova testi sonuçları

Farkındalık	N	Ortalama	Standart Sapma	Varyans Kaynağı	Kareler Toplamı	Df	Kareler Ort.	F	P	Homojenlik
Evet	32	1,25	,568	Gruplar Arası	4,149	2	2,074	3,950	,022	,000*
Hayır	64	1,67	,736							
Planlanıyor	24	1,67	,868	Grup İçi	61,443	117	,525			
Toplam	120	1,56	,742	Toplam	65,592	119				

* (p>0,05)

H9: Dijital süreklilik farkındalığı dijital belgelerin uzun vadede erişilebilir olması çalışmalarını artırmaktadır.

Yorum: Tablo 68’de kurumlarda dijital süreklilik farkındalığı ve dijital belgelerin uzun vadede erişilebilir olması arasındaki ilişkin Anova sonuçlarını görmekteyiz. Bu sonuca göre kurumlarda var olan dijital süreklilik farkındalığının dijital belgelerin uzun vadede erişilebilir olmasını artırdığı doğrulanmaktadır (p<0,05). Bu sonuca göre H9 hipotezi kabul edilebilir niteliktedir. Tablo 68 varyansların homojen olmadığını (p<0,05) göstermektedir. Bu nedenle hangi gruplar arasında anlamlı fark olduğunu bulabilmek için post hoc testlerinden heterojen varyanslı dağılımlarda kullanılan Tamhane’s T2 tekniğine başvurulmuştur.

Tablo 69. H9 hipotezi Tamhane’s T2 testi sonuçları

Uzun Vadede Erişilebilirlik		Ortalama Fark	Standart Hata	P
Evet	Hayır	-,422*	,136	,008
	Çalışmalar planlanmaktadır.	-,417	,204	,137
Hayır	Evet	,422*	,136	,008
	Çalışmalar planlanmaktadır.	,005	,200	1,000
Çalışmalar planlanmaktadır.	Evet	,417	,204	,137
	Hayır	-,005	,200	1,000

Tamhane testi sonucuna göre uzun vadede erişebilirlik çalışmalarına evet diyenler ile hayır diyenler arasında anlamlı bir fark vardır ($P<0,05$). Yani kurumlarda dijital belgelerin uzun vadede erişilebilir olması için çalışma olanlar olmayanlara göre dijital sürekliliğin daha farkındadır (Tablo 69). Dijital süreklilik demek ihtiyaç duyduğun anda o bilgiye ulaşmak, onunla çalışmak, ona güvenmek demektir. Bu bağlamda dijital süreklilik kavramı doğrudan dijital ortamda üretilen ve saklanan bilginin korunması ile bağlantılıdır. Dijital süreklilik bir kurumda ne kadar önemsenirse, bilgiye ulaşma, onunla çalışma, onu, bulma, ona güvenme çok daha kolay olacaktır. Dijital ortamda üretilen bilgi ve belgelerin dijital süreklilik açısından bakıldığında kullanılabilir olması dijital korumanın yapılması ile ilgilidir (Özdemir ve Cengiz, 2019, s. 273).

Tablo 70. H11 hipotezi Anova testi sonuçları

Dijital Süreklilik Farkındalığı	N	Ortalama	Standart Sapma	Varyans Kaynağı	Kareler Toplamı	Df	Kareler Ort.	F	P	Homojenlik
Üniversite	67	4,27	,327	Gruplar Arası	,529	3	,176	1,666	,178	,085*
Bakanlık	10	4,45	,222							
Belediye	31	4,19	,299		12,285	116	,106			
Diğer	11	4,22	,442	Grup İçi						
Toplam	120	4,26	,328	Toplam	12,815	119				

H11: Kurum türüne göre dijital süreklilik farkındalığı anlamlı ve pozitif yönde ayrılmaktadır.

Yorum: Tablo 70'te kurum türüne göre dijital süreklilik farkındalığı varyans sonuçları görülmektedir. Bu sonuca göre kurum türünde dijital süreklilik farkındalığı anlamlı ve pozitif yönde ayrılmamaktadır ($p>0,05$). Bu sonuca göre H11 hipotezi kabul edilememektedir. Elde edilen bulgulara göre dijital süreklilik konusu bakanlıklarda, üniversitelerde, belediyelerde ve diğer kamu kurum ve kuruluşlarında birbirinden anlamlı bir şekilde farklılaşmamaktadır. Yani, diğer kurumlarla kıyaslandığında belediyelerde dijital süreklilik farkındalığı daha az ya da çok gibi bir yorum yapılamamaktadır. Ankete dâhil olan tüm kurumlarda dijital süreklilik farkındalığı benzer oranlarda görülmektedir.

Tablo 71. H13 hipotezi Anova testi sonuçları

Varyans Kaynağı	Kareler Toplamı	Kareler Ort.				
		df		F	P	Homojenlik
Gruplar Arası	2,461	9	,273			
				,567	,821	,015*
Grup İçi	53,006	110	,482			
Toplam	55,467	119				

H13: Dijital belgelerin saklandığı formatın çeşitliliği, uzun vadede erişim çalışmalarını artırmaktadır.

Yorum: Tablo 71’de kurumlarda kullanılan format çeşitliliğine göre uzun vadede erişim çalışmana ait varyans sonuçları gösterilmektedir. Bu sonuca göre kurumlarda dijital belgelerin saklandığı formatın çeşitliliğinin uzun vadede erişim çalışmalarını artırmadığı görülmektedir ($p>0,05$). Bu sonuca göre H13 hipotezi kabul edilememektedir. Kurumlarda dijital belgeler için bilinçli ya da bilinçsiz olarak kullanılan çeşitli formatlar bulunmaktadır. Format çeşitliliğinin uzun vadede erişim çalışmalarını artırmaması beklenen bir sonuç olarak karşımıza çıkmaktadır. Buna karşın belgelerin format çeşitliliğinden ziyade kullanılan format yapısının dijital belgelerin uzun vadede erişimi daha destekleyici olduğu da bilinmektedir. Yani kullanılan formatların çeşitliliğinden ziyade koruma için uygun formatı kullanmak önemlidir. Bazı milli arşivler dijital belgelerin arşive transferi için çeşitli format yapıları kullanmaktadırlar. Buna karşın örneğin; İngiliz Milli Arşivi ilk zamanlarda transfer işlemlerinde tüm formatları kabul etmeyip belirli format yapılarını kabul kullanıyordu fakat son yıllarda format türünde ayırım yapmaksızın tüm formatları kabul etmektedirler (Sheridan, 2021). Bu durum da yine format çeşitliliğinin uzun vadeli koruma için belirli bir ölçüt olmadığının altını çizmektedir.

Tablo 72. H14 hipotezi Anova testi sonuçları

Varyans Kaynağı	Kareler Toplamı	df	Kareler Ort.	F	P	Homojenlik
Gruplar Arası	5,127	10	,513			
				,924	,514	,053*
Grup İçi	60,465	109	,555			
Toplam	65,592	119				

H14: Dijital süreklilik farkındalığı, dijital sürekliliğin iyi yönetilmesini olumlu ve pozitif yönde etkilemektedir.

Yorum: Tablo 72’de kurumlarda personelin dijital süreklilik hakkındaki farkındalığı ile ilgili dijital sürekliliğinin iyi yönetilmesine ait varyans sonuçlarını gösterilmektedir. Bu sonuçlara göre kurumlardaki personelin dijital sürekliliği daha önce duymalarının kurumlarda dijital sürekliliğin iyi yönetilmesini olumlu ve pozitif yönde etkilemediği ortaya ($p>0,05$) çıkmıştır. Bu sonuca göre H14 hipotezi kabul edilememektedir. Burada kurumlardaki personelin daha önce dijital süreklilik terimini duyması ya da bu konu ile ilgili farkındalık sağlaması kurumlarda dijital sürekliliğin iyi yönetilmesine başlı başına yeterli gelecek bir unsur değildir. Kurumlarda dijital sürekliliğin iyi yönetilmesi için sadece personelin farkındalığı yeterli değildir. Öncelikle kurumlarda çalışan personelin kurumda var olan bilgi varlıklarını iyi bilmesi gerekir. Çünkü dijital sürekliliğin sağlanması ve yönetilmesi bilgi varlıklarına bağlıdır. Bu kapsamda kurumlar öncelikle sahip oldukları bilginin farkında olmalıdırlar. Bu unsur da tek başına dijital sürekliliğin iyi yönetilmesine yetmemektedir. Kurumlarda dijital sürekliliğin iyi yönetilebilmesi için daha önce çalışmanın dördüncü bölümünde bahsedilen adımların yerine getirilmesi önem arz etmektedir. Kısaca kurumlarda dijital sürekliliğin iyi yönetilmesi için, kurumun konu hakkında bir eylem planına sahip olması, dijital süreklilik gereksinimlerinin tanımlanması, dijital süreklilik risklerini değerlendirme ve yönetme, dijital sürekliliğin sağlanması adımlarının yerine getirilmesi gerekmektedir (*Managing Digital Continuity*, 2017, s. 6).

6.3.5. Mann-Whitney U Testi Analizleri ve Yorumları

Mann-Whitney U testi parametrik olmayan test türlerindendir. Parametrik testler için gerekli şartları sağlamayan durumlarda veri dağılımı ön şartı koşmayan analiz tekniklerine ihtiyaç vardır. Bu tekniklerden biri de Mann Whitney U testidir. Bu test, t testinin parametrik olmayan eşdeğeri olarak kullanılmaktadır. Mann Whitney U testi ile bağımsız iki grubun aynı dağılıma sahip ana kitlelerden geldiği hipotezi test edilebilmektedir (Coşkun, Altunışık ve Yıldırım, 2019, s.237).

Tablo 73. H10 hipotezi Mann-Whitney U testi analizi sonuçları

Grup	N	Sıra Ortalaması	Sıralar Toplamı	U	Z	p
e-arşivi olan	32	49,59	1587,00	1059,000	-2,279	,023
e-arşivi olmayan	85	62,54	5316,00			

H10: Kurumlarda e-arşiv sistemi bulunması ile hassasiyet değerlendirmesinin etkinliği arasında anlamlı ve pozitif yönlü bir ilişki bulunmaktadır.

Yorum: Veriler normal dağılım göstermediği için de T-Testinin parametrik olmayan karşılığı Mann Whitney U-Testi de uygulanmıştır. Mann Whitney U testi, kurumlarda e-arşiv sistemi bulunmasının hassasiyet değerlendirme üzerinde etkisini ortaya çıkarmak için yapılmıştır. Analiz sonucunda, kurumlarda e-arşiv sistemi bulunması ile hassasiyet değerlendirmesi etkinliği arasında anlamlı ve pozitif yönlü bir ilişki bulunmuştur (U=1661,000; Z=-2,279; p<0,05). Bu sebeple H10 hipotezi kabul edilmiştir. Kısaca, kurumlarda hassasiyet değerlendirmesi süreci, e-arşiv sistemine sahip olanlar ile olmayanlar arasında farklılık göstermektedir (Tablo 73). E-arşiv sistemine sahip olmak dijital belgelerin bilgi yönetim süreçlerinin sağlıklı ilerlemesi için önemli bir faktördür. E-arşive sahip bir kurum sahip olmayan bir kuruma göre dijital belgelerini düzenlenme, koruma, milli arşive transfer etme ve transfer sürecinde gerçekleşecek olan hassasiyet değerlendirmesi süreçlerinde daha sağlıklı adımlarla yürütecektir.

YEDİNCİ BÖLÜM

7. SONUÇ VE ÖNERİLER

“Born-dijital records” olarak adlandırılan doğuştan dijital belgeler fiziksel belgelerden farklıdır. Tam da bu sebeple bu tip belgelere fiziksel belgelere yapılan işlemler yapılmamalıdır. Teknoloji odaklı dijital çağda bilgi ve belgelerin yönetim süreçleri de değişiklik göstermiştir ve öyle de olmalıdır. Dijital belgelerin doğası farklıdır ve onlara doğası gereği müdahale edilmelidir. Bu çerçevede öncelikle dijital belgelere ve yönetim süreçlerine yönelik birtakım unsurların belirlenmesi, yol haritasının çıkarılması ve atılacak adımların belirlenmesi son derece elzemdir. Bu konuda Devlet Arşivleri Başkanlığına büyük ve önemli roller düşmektedir. Dijital belgelerin bilgi ve belge yönetim süreçleri; dijital belgenin yaşam döngüsü sürecinden itibaren geçirdiği evrelerin yanı sıra, dijital değerlendirme, dijital ayıklama, hassasiyet değerlendirmesi, belge yönetimi politikaları, dijital süreklilik, dijital koruma konularını da kapsamaktadır. Bu kapsamda dijital belgelerin bilgi ve belge yönetim süreçlerinin ulusal ve uluslararası boyutta planlanması ve yapılandırılması, yasal ve politik düzenlemelerin hayata geçirilmesi, konu kapsamında kurumlarda uygulamaların başlamasına yönelik strateji, plan, program ve rehberlerin hazırlanması büyük önem taşımaktadır. Türkiye’de doğuştan dijital belgelerin arşive transfer süreçleri değerlendirildiğinde, dünyanın birçok ülkesinde bu süreçlerin yıllar önce başlamasına karşın ülkemizde konu ile ilgili süreçlerin henüz başlamadığını söylemek mümkün. Bu bağlamda doğuştan dijital belgelerin bilgi ve belge yönetimi süreçlerine yönelik öncelikle yasal ve politik düzenlemelerin olmayışı, konuya ait uygulamaların başlamamış olması ve bunlara yönelik sorumlu idare tarafından yayımlanmış çalışmaların var olmayışı, kurumlarda çalışan personelin konu hakkındaki farkındalık eksiklerinin bulunması dikkati çekmekte ve konuyu üzerinde çalışılması gereken bir alan haline getirmektedir.

Çalışmamızda Türkiye’de doğuştan dijital belgelerin bilgi ve belge yönetim süreçlerini ortaya çıkarabilmek amacıyla 120 kurum incelenmiştir. Bu kurumlar, Türkiye’de dijital belgelerin bilgi yönetim süreçlerine dair veri sağlayabilecek kamu kurum ve kuruluşları ile Devlet Arşivleri Başkanlığı tarafından yayımlanan 2020-2024 stratejik planında yer alan dış paydaşlar olarak iş birliği yapılan kurumlardır. Yapılan analizler sonucu Türkiye’de doğuştan dijital belgelerin bilgi ve belge yönetimi süreçlerine

yönelik ortaya çıkan sonuçlar aşağıdaki gibi belirtilmiştir. Özel kurumlar örnekleme dâhil edilmeyip, araştırma kamu kurum ve kuruluşları ile sınırlandırılmıştır.

Analiz sonuçlarına göre kurumların yarısından fazlasının belgelerini hem fiziksel hem de dijital (hibrit) halde sakladıkları ortaya çıkmıştır. Kurumlardan bazıları ise EBYS'ye güvenmedikleri için belgelerin sistemden çıktısını alıp saklayarak kendilerine ikinci bir güvenlik alanı oluşturmaktadırlar. Buna göre kurumlar tam olarak uygulamada dijital çalışmamakta ve dijitale güvenmemektedirler. Kurumların büyük bir çoğunluğunun fiziksel belgelerini dijitalleştirdikleri ortaya çıkmıştır. Bununla birlikte fiziksel belgelerin dijital ortamda bulunup bulunmadığına bakıldığında kurumların fiziksel belgelerini dijital ortamda tutması dağınık bir yapıdadır. Analizlerden çıkan sonuçlara göre kurumlarda dijitalleştirme aktif olarak gerçekleşmesine rağmen dijital ortama güvensizlik vb. sebeplerden ötürü kurumlarda hibrit ortamda belge yönetimi hâkimdir.

EBYS kurumlarda kullanılan bir bilgi yönetim sistemidir. Kurumların geneli EBYS'yi hem bir arşiv hem de bir bilgi yönetim sistemi olarak görmektedirler. Bu durum kurumlarda bir e-arşiv sisteminin olmamasından kaynaklanmaktadır. Analiz edilen kurumların büyük bir bölümünün e-arşiv sistemlerinin de olmadığı sonucuna erişilmiştir. Bu sebeple kurumlar kullandıkları EBYS içerisindeki e-Arşiv modülünü arşiv olarak kullanmakta ve EBYS'yi de arşiv olarak algılamaktadırlar. Bununla birlikte kurumların ağırlıklı olarak 7-9 yıldır EBYS kullandıkları sonucuna erişilmiştir. Kurumların yarıya yakını işlevsellik, üst yönetim kararı, maliyet gibi sebeplerle kullandıkları EBYS'yi değiştirirken, yarısı da EBYS değişikliği yapmamışlardır.

Kurumlarda bilginin sürekliliğinin sağlanması ve kurumsal süreçlerin düzgün ilerlemesinin yollarından biri, her bir bilgi varlığının bilgi envanterinin olmasından geçmektedir. Analiz edilen kurumların genel anlamda bahsi geçen bilgi envanterlerine sahip olmadıkları, olanların ise profesyonel anlamda bir bilgi varlığı envanter kaydı tutmadıkları sonucuna erişilmiştir. Bununla birlikte kurumların büyük bir bölümünün bu iş ile ilgilenecek bilgi varlık sorumlularının da olmadığı sonucu karşımıza çıkmaktadır.

Kurumların çok büyük bir bölümü, dijital belge oluştururken bir saklama süresi belirlemediklerini belirtmektedirler. Bu durum kurumların bu konuda farkındalık olarak eksik kaldıklarının bir göstergesidir. Bununla birlikte kurumlar dijital belgeler için bir dosyalama sistemi (standart dosya planı) kullanmakta yetersiz oldukları görülmüştür.

Kurumların standart dosya planına uyma konusunda da yetersiz oldukları dikkatleri çekmektedir. Bu durumun geniş perspektifte belge yönetim süreçlerinde ve arşive transfer süreci ve daha sonrası için büyük sorunlara yol açacağı aşikârdır.

Araştırmaya göre kurumların önemli bir bölümünün kullandıkları sistem içerisinde birden fazla nüshası bulunmaktadır. Analiz edilen kurumların EBYS içerisinde bir belgenin birden fazla nüshası olmasına karşı çoğunlukla hiçbir çalışma yapmadıkları sonucuna erişilmiştir. Bu durumun kurumlarda sistem içerisinde aranılan belgeyi bulmakta zorluk çekileceği, sonradan kullanılacak ve üstünde işlem yapılacak belge ya da arşive aktarılacak belgeler konusunda bir karmaşa oluşturacağı düşünülmektedir.

Kurumlar bir dijital belge oluştururken özgünlüğe, güvenilirliğe, birlikte çalışabilirliği, tekrar kullanılabilirliği, tanımlama ve onaylama kolaylığını, gizliliği ve bütünlüğü önemli görmektedir. Birlikte Çalışabilirlik Rehberi'ne uyulması kamu kurumlarında zorunludur ve bu rehberde kurumlar tarafından uyulması gereken format yapıları belirlenmiştir. Aynı zamanda TS 13298 Standardında da dosya formatları belirlenmiştir. Bunun yanı sıra kurumlar sistem içerisinde dijital belgelerini saklanması önerilen formatlardan ziyade bir standarda uymadan çeşitli formatlarda saklamaktadır. Genel anlamda kurumlardan belirlenen ve kullanılan format yapısı ile ilgili dağınık bir yapılanma olduğu görülmektedir.

Kurumlarda bilginin dijital olarak yönetilmesi ve bilgi, sistemler ve süreçlerin birlikte çalışabilmesi dijital sürekliliğin kurumlarda var olmasıyla gerçekleşebilir. Analiz edilen kurumlarının yarısının dijital süreklilik farkındalığının eksik olduğu sonucu ortaya çıkmıştır. Bununla birlikte kurumlar, dijital sürekliliğin iyi yönetilemediğinde bilgi kaybı gerçekleşmesi, etkili ve verimli çalışmanın olumsuz etkilenmesi, çeşitli formatlarda oluşturulmuş belgelerin açılmak ve kullanılmak istendiğinde donanım ve yazılımın desteklememesi, veri göçünün gerçekleştirilememesi, üst veri eksikliğinden ötürü çeşitli destek ödeneklerinin sağlanamamasına yol açması, kritik bir proje için gerekli olan bilginin bulunamaması gibi olumsuz etkilerinin ortaya çıkacağı endişelerini belirtmişlerdir.

Kurumlarda genel olarak dijital belgelerin uzun vadeli erişebilir olması için bir çalışma yapılmamaktadır. Bu bağlamda kurumlar; depolama ortamlarının sürekliliği sağlanması, kurumda bilgi varlık envanteri oluşturulması ve sorumluların belirlenmesi, konu kapsamında politika, strateji, rehber vb. oluşturulması, dijital sürekliliğin tüm

kurum bünyesinde önemsenmesi ve uygulanması, standartlara uygun üst veri oluşturulması, bir risk planlaması yapılması, konu kapsamında düzenli aralıklarla eğitimler verilmesi, uygun veri formatlarının kullanılması unsurlarına uzun vadede erişilebilirlik için ihtiyaç duymaktadır. Bununla birlikte kamu kurumlarının, dijital belgelerin uzun vadeli korunması ile ilgili içerik biçimlerinin karmaşık ve kırılgan olması, mevcut yazılım ve donanımın güncel tutulması ve korunmasının zor olması, yasal ve politik risklerin var olması, hacim veya karmaşıklık kapsamında içerik toplamanın zor olması, dosya formatlarının hızlı değişiklik göstermesi ve eski dosya formatlarının okunamaması, yetersiz personele sahip olmak, içeriğin yetersiz tanımlanması kullanımını ve keşfedilmesinin zorlaştırabilmesi konularında kaygı düzeyleri oldukça yüksektir. Analiz edilen kurumların yarısından fazlasında dijital belgelerin uzun vadeli korumasından sorumlu birim Bilgi İşlem Daire Başkanlığı'dır. Burada alanımızın disiplinler arası çalışma imkânına sahip olması olumlu bir durumdur. Bilgi İşlem biriminin kurumun bilgi yöneticilerine, arşivcilere danışarak birlikte hareket etmesi ancak süreçlerin sağlıklı ilerlemesine katkı sağlayacaktır. Kurumların geri kalanında ise dijital belgelerin uzun vadeli korumasından sorumlu bir birim yoktur. Kurumların tamamına yakını ise uzun vadeli koruma için bir politikasının (strateji belgesi, plan, program, yönetmelik vb.) olmadığı sonucuna erişilmiştir. Öte yandan kurumların önemli bir bölümünün dijital belgelerin kurumsal bilgi yönetim süreçleri ile ilgili politikaya ihtiyaç duyduklarını belirtmektedir.

Analiz edilen kurumların genel olarak dijital belgelerin kurumsal bilgi yönetim süreçlerinde görev yapan personelin farkındalık düzeylerinin yeterli olmadığı sonucuna ulaşılmıştır. Bu bağlamda, Türkiye'de kamu kurumlarında dijital belgelerin değerlendirmesi, ayıklanması, hassasiyet değerlendirmesi, dijital sürekliliği gibi konularda genel bir farkındalık eksikliği bulunmaktadır sonucunu ortaya çıkarmaktadır. Birçok kurumun bu konuda tecrübeleri yok çünkü henüz dijital transfer işlemlerini yapmakla karşı karşıya gelmediler. Önemli olan yakın zamanda farkındalığın artırılmasıdır. Bu durum ise Milli arşiv altyapısı oluşturulması ve eğitim verilmesine bağlıdır. Bunun yanı sıra dijital belgelerin kurumsal bilgi yönetim süreçlerinde görev yapan nitelikli personel sayısının da yeterli olmadığı kurumlar tarafından belirtilmiştir. Kamu kurumlarında dijital belgelerin kurumsal bilgi ve belge yönetim süreçlerinde daha fazla personele ihtiyaç duyulduğu ve var olan personelin de farkındalık düzeyinin yeterli olmadığı sonucu ortaya çıkmaktadır. Bu bağlamda kamu kurumlarında kurumsal bilgi ve

belge yönetim süreçlerinde farkındalık düzeyi yüksek yeterli sayıda personele ihtiyaç ortaya çıkmaktadır.

e-değerlendirme, e-ayıklama, hassasiyet değerlendirmesi süreçleri dijital çağda dijital belgelerin arşive transfer aşamasında geçirmesi gereken evrelerdir. Bu süreçlerin bulunduğu çağ itibari ile manuel tekniklerden ziyade teknolojik adımlarla ilerlemesi gerekmektedir. Araştırmaya göre kurumların tamamına yakını, dijital belgeler için e-değerlendirme, e-ayıklama ve hassasiyet değerlendirmesi yapmamaktadır. Kurumların çok az bir kısmı ise bu süreçleri manuel olarak yürütmektedir. Bunun yanı sıra kurumlarda EBYS içerisinde dijital belgelerin hassasiyet değerlendirmesi için üst veri tanımlaması da yapılmadığı sonucuna ulaşılmıştır. Dijital belgelerin milli arşivlere transferi birçok ülkede başarı ile gerçekleşirken, henüz Türkiye’de bu adımların dahi gerçekleştirilememesi ve bunun yanı sıra hala manuel yöntemlerle işlemlerin yürütülmeye çalışılması son derece düşündürücü bir tablo olarak karşımıza çıkmaktadır.

Araştırmaya katılan kurumların neredeyse tamamının bir belge yönetim politikasını sahip olmadıkları önemli bir sorun olarak karşımıza çıkmaktadır. Bunun yanı sıra analiz edilen kurumlar; elektronik belgelere erişim, belge yönetimi politikasının amacı ve kapsamı, roller ve sorumluluklar, dosya planı, ayıklama politikası, dijital belgelerin transferi, koruma, imha politikası, arşive uygun materyal türünün belirlenmesi, üst veri standardında uygunluk, hesap verebilirlik ve şeffaflık, eğitim ve farkındalık, hassas belgelerin süreçleri, fiziksel ve dijital belgelerin için saklama unsurlarının bir belge yönetimi politikasında mutlaka olması gereken unsurlar olarak görmektedirler. Bununla birlikte kurumların neredeyse tamamına yakını belge yönetim politikasına ihtiyaç duyduklarına belirtmişlerdir. Diğer yandan, kurumlar dijital belgelerin kurumsal bilgi ve belge yönetim süreçlerine yönelik politikanın T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı tarafından hazırlanmış örnek bir metin üzerinden kurumların kendilerine göre uyarlayarak hazırlanması gerektiğini düşündüklerini belirtmişlerdir.

Analiz edilen kurumların tamamına yakınında dijital süreklilik, dijital belgelerin değerlendirilmesi, dijital belgelerin ayıklanması, dijital belgelerin hassasiyet değerlendirmesi, uzun süreli koruma, risk yönetimi konularında neredeyse hiç eğitim verilmediği ortaya çıkmıştır. Bunun yanı sıra bazı kurumlarda EBYS kullanımı, bilgi iletişim teknolojileri, bilgi güvenliği konularında eğitim verilmektedir. Bazı konularda eğitim almalarına karşın kurumlar sırasıyla; uzun süreli koruma, dijital süreklilik, dijital belgelerin hassasiyet değerlendirmesi, dijital belgelerin değerlendirilmesi, dijital

belgelerin ayıklanması, bilgi güvenliği, risk yönetimi konularında eğitime ihtiyaçları olduğunu belirtmişlerdir. Genel anlamda kurumlar, kendilerine verilen eğitimlerin yetersiz kaldığını belirtmişlerdir. Kurumlar dijital belgelerin ayıklanması ve değerlendirilmesi, hassasiyet değerlendirmesi, dijital süreklilik ve dijital koruma konularında ileride zorlanacaklarını düşünmektedirler. Bu bağlamda kurumların dijital bilgi ve belge yönetim süreçlerinin tüm aşamaları hakkında eksik hissettikleri anlaşılmaktadır.

Araştırmaya göre kurumların önemli bir bölümü dijital belgelerin milli arşive transferi düşünüldüğünde teknik altyapılarını bütünüyle yeterli görmemektedirler. Bu bağlamda kurumların teknik altyapı ihtiyaçlarının giderilmesi gerekliliği sonucu ortaya çıkmaktadır. Bu sonuçlara dayanarak Türkiye’deki kamu kurumlarında konu ilgili teknik altyapının eksikliği bulunduğu ve bu eksikliğin Devlet Arşivlerinin konu ile ilgili resmi bir belge henüz yayımlamamış olmasından ve kapsamlı bir yol haritasının oluşturulamamasından kaynaklı olduğu görülmektedir.

Kurumların büyük çoğunluğunun dijital belgelerini arşive devretme yükümlülükleri ile ilgili bilinçlerinin yeterli olmadığı görülmektedir. Bunun yanı sıra kurumların yarısından fazlasında transfer edilecek materyallerle ilgili de bir bilinç olmadığı sonucu ortaya çıkmıştır. Öte yandan kurumlarda genel olarak milli arşive transfer için bir Devlet Arşivleri ile bir bağlantıya geçilmemiştir. Kurumların kendi içlerinde milli arşive transfer ile ilgili de bir çalışmalarının da olmadığı sonucuna erişilmiştir. Kurumların neredeyse tamamına yakınının dijital belgelerini transfer etmek için belirlenmiş bir tarihleri yoktur. Bu bağlamda kurumların dijital belgelerini transfer aşaması konusunda kendilerini geliştirmeleri gerektiği ortaya çıkmaktadır. Kurumlar dijital transfer sürecinin denetleme işleminin Devlet Arşivleri Başkanlığı tarafından yapılması gerektiğini düşünmektedirler.

Kurumların geneli Devlet Arşivleri Başkanlığı kurumların elektronik arşivleme süreçleri ile ilgili yeterli düzeyde takip ve denetleme yaptığını düşünmemektedir. Bunun yanı sıra kurumlar Devlet Arşivleri Başkanlığı’nın kurumların dijital milli hafızasını koruyup ileriki kuşaklara aktaracağına olan inançları genel anlamda kararsızdır. Öte yandan kurumlar, Devlet Arşivleri Başkanlığı’nın gerekli yasal düzenlemeler (arşiv kanunu, politika) konusunda yeterli hizmeti sağladığını düşünmemektedirler. Kurumların büyük çoğunluğu Devlet Arşivleri Başkanlığı’nın görev ve sorumluluklarını yerine getirdiği konusunda da kararsız kalmaktadırlar.

Çalışmada yukarıda sıralanan sonuçlar doğrultusunda; “Türkiye’de kamu kurumlarında doğuştan dijital belgelerin kurumdan arşive transfer aşamasına kadar gerekli olan bilgi ve belge yönetimi süreçlerinin teknik ve hukuksal altyapısı yeterli/beklenen düzeyde değildir” şeklinde belirlenen temel hipotez doğrulanmıştır.

Çalışmada ortaya çıkan sonuçlar ayrıca:

- “Dijital belgelerin milli arşive transfer sürecine dair bilinç ile Devlet Arşivleri Başkanlığı etkinliği arasında anlamlı ve pozitif yönlü bir ilişki bulunmaktadır.
- Dijital belgelerin bir bilgi varlığı olarak görülmesi ile kurumsal politika oluşturma arasında anlamlı ve pozitif yönlü bir ilişki vardır.
- e-değerlendirme, e-ayıklamayı doğrudan ve pozitif olarak etkilemektedir.
- Belge yönetim politikasına sahip olmak, dijital belgelerin oluşturulmasında "gizliliği" olumlu ve pozitif yönde etkilemektedir.
- Dijital belgelerin saklama sürelerinin belirlenmesi, standart dosya planına uyumu olumlu ve pozitif yönde etkilemektedir.
- Kurumsal bilgi yönetim süreçlerinin zorluğu, eğitime ihtiyaç duyulan alanları artırmaktadır.
- Dijital belge yönetimine dair eğitimler, EBYS yeterliliğini artırmaktadır.
- Devlet arşivlerinin kurumlara desteği, kurumların dijital belgeleri arşive devretme yükümlülüğün farkında olmasını anlamlı ve olumlu yönde etkilemektedir.
- Dijital süreklilik farkındalığı dijital belgelerin uzun vadede erişilebilir olması çalışmalarını artırmaktadır.
- Kurumlarda e-arşiv sistemi bulunması ve hassasiyet değerlendirmesinin etkinliği arasında anlamlı ve pozitif yönlü bir ilişki bulunmaktadır “şeklinde belirlenen alt hipotezler de doğrulanmıştır.

Araştırmada elde edilen sonuçlar kapsamında Türkiye’de doğuştan dijital belgelerin bilgi ve belge yönetim süreçlerine yönelik geliştirilen öneriler aşağıda sıralanmıştır:

- Tüm süreçlerin sağlıklı ilerlemesi için öncelikle “Milli Arşiv Kanunu” oluşturulup yayımlanmalıdır.

- Devlet Arşivleri Başkanlığı öncülüğünde doğuştan dijital belgelerin bilgi ve belge yönetim süreçlerine yönelik yasal düzenlemeler oluşturulmalıdır. İlk olarak “Dijital Strateji” metni oluşturulmalı ve tüm kurumlara ülke genelinde iletilmelidir. Strateji hazırlanırken bakanlıklar, üniversiteler, belediyeler ve iş birliği yapılabilecek özel ve kamu kurumları, meslek örgütleri ve alanında uzman akademisyenler içerisinde görüşler alınmalı, bir araya gelinerek tartışma ortamı sağlanmalıdır.
- Dijital korumada kullanılacak özel stratejileri özetleyen ve özellikle altyapı, biçim, medya sürdürülebilirliği ve standartları, veri bütünlüğü ve bilgi güvenliği gibi konuları ele alan “Dijital koruma politikası” oluşturulmalıdır.
- Her kurumun kendi bünyesinde e-arşivi olmalıdır.
- Devletin tüm süreçleri ile entegre bir dijital bilgi yönetimini sağlamak için dijital süreklilik politikası oluşturulmalıdır.
- Kurumlarda dijital süreklilik farkındalığı artırılmalıdır.
- Her kurumun bir bilgi varlığı envanteri olmalı ve bu envanterden sorumlu bilgi varlık sorumluları belirlenmelidir.
- Kurumların dijital belge oluştururken saklama süresini belirlemeleri ve standart dosya planına uymaları gerekmektedir.
- EBYS içerisinde bir belgenin birden fazla nüshanın oluşmasını önlemek için sistem içerisinde otomatik tetikleyicilerin oluşturulması sağlanarak fazla nüshaların sistem içerisinde oluşması önlenmelidir.
- Kurumlar dijital belge oluştururken Birlikte Çalışabilirlik Rehberi’nde ve TS 13298 Standardında belirtilen dosya formatlarına uymalıdır.
- Dijital belgelerin uzun vadeli korumasından sorumlu bir birim oluşturulmalıdır.
- Dijital belgeleri milli arşive aktarmak için bir altyapı hazırlanmalı, adımlar belirlenmeli, rehberler oluşturulmalıdır.
- Milli arşivde çalışan personele eğitim verilmeli, bu eğitim yurtdışındaki benzer tecrübeyi yaşamış uzmanlar aracılığıyla sağlanmalı ve onlarla yakından çalışılmalıdır.
- Kurumlara alanında uzman kişiler tarafından dijital değerlendirme, dijital ayıklama, hassasiyet değerlendirmesi, dijital süreklilik, dijital koruma, risk yönetimi, bilgi güvenliği, EBYS konularında eğitimler verilmeli ve uygulama

üzerinde gösterilmelidir. Kurumlarda çalışan personelin konu hakkında farkındalığı artırılmalıdır.

- Dijital belgelerin bilgi yönetimi ve transferi aşamalarında kurumlar teknolojik anlamda kendi oluşturacakları programları ya da PRONOM, DROID, JHOVE vb. gibi programları kullanarak süreçleri mümkün olduğunca otomatikleştirilmelilerdir.
- Kurumlardaki nitelikli ve dijital becerilere sahip personel sayısı artırılmalıdır.
- Her kurum bir belge yönetim politikasına sahip olmalıdır. Oluşturulacak politikadaki unsurların bazıları Devlet Arşivleri Başkanlığı tarafından standart haline getirilmeli ve kurumlar bu standart üzerinden hareketle kendi politikalarını yaratabilmelidir.
- Dijital belgelerin milli arşive transferi için kurumlarda Devlet Arşivleri Başkanlığı tarafından denetleme yapılmalı, düzenli eğitimler verilmeli, bilinç oluşturulmalıdır. Bu süreçte uzman kişiler ve üniversitelerin Bilgi ve Belge Yönetimi Bölümlerinden destek alınarak adımlar ilerletilmelidir.
- Kurumların dijital belgelerin transferi için Devlet Arşivleri Başkanlığı ile iletişime geçmeleri gerekmektedir. Transfer sürecinin başlaması için iki taraf açısından aktarım için bir tarih belirlenmelidir.
- Devlet Arşivleri Başkanlığı tarafından dijital belgelerin milli arşive transferi için gerekli olan adımların, aşamaların tüm ayrıntılarının belirlenmesi, yazılı hale getirilmesi Devlet Arşivleri Başkanlığı web sitesinde yayımlanması gerekmektedir. Bununla birlikte Devlet Arşivleri Başkanlığı tarafından kurumlara resmi yazı ile süreçler ve işleyiş gönderilmelidir.
- Dijital belgelerin milli arşive transferi sürecinde kurumların ve milli arşivin teknik altyapısının geliştirilmesi ve hazır olması gerekmektedir.
- Türkiye’deki kurumların hepsi Devlet Arşivleri Başkanlığı tarafından elektronik arşivleme süreçleri ile ilgili yeterli düzeyde takip ve denetlemeye tabi tutulmalılar.
- Kurumlar içerisinde örnek kurumlar (üniversite, bakanlık, belediye, diğer kamu kurum ve kuruluşları) seçilmeli ve bu kurumlar üzerinden dijital belgelerin milli arşive transferi pilot uygulama olarak başlatılmalıdır.
- Kurumlarda süreçlerin sağlıklı ilerlemesi adına personel güncel konuları takip etmeli, personele düzenli eğitimler verilmeli ve aynı zamanda iş takibi açısından personel denetlenmelidir. Bu süreç için uzman kişilerden destek alınmalıdır.

Doğuştan dijital belgelerin milli arşive transfer süreçleri, birçok ülkede aktif şekilde yürütülmektedir. Dijital dönüşüm ile birlikte dijital verinin yönetilmesi, yeniden kullanılabilmesi, onunla çalışılabilmesi, ona güvenilebilmesi, ona erişilebilmesi, şeffaf olması son derece önem kazanmıştır.

Türkiye’de henüz doğuştan dijital belgelerin milli arşive transferi gerçekleşmemiştir ancak önümüzdeki yıllarda yasal olarak transfer sürecinin büyük bir ivedilikle başlaması gerekecektir. Türkiye’de doğuştan dijital belgelerin bilgi ve belge yönetim süreçlerinin sağlıklı ilerlemesi, yaşam döngüsü sonucunda dijital belgelerin uluslararası standartlarda milli arşive transfer edilebilmesi için çalışmaların modellenmesi ve başlatılması son derece elzemdir. Doğuştan dijital belgelerin bilgi ve belge yönetim süreçlerini ele alan bu çalışmanın dijital belgelerin bilgi yönetim süreçleri ve milli arşive transfer sürecinde kurumlara yol gösterici olması beklenmektedir. Konu ile ilgili ileride yapılacak araştırmalarda doğuştan dijital belgelerin bilgi yönetim süreçleri ve milli arşive transferi ile ilgili yazılımlar üretilebilir, teknik boyut çalışılabilir, örnek pilot projeler gerçekleştirilebilir.

KAYNAKÇA

- Akdoğan, Z. ve Özdemirci, F. (2016). Dijitalleştirme ve e-arşivlemede izlenecek yol ve yöntemler. F. Özdemirci, N. Özel, T. Çakmak, Z. Akdoğan ve B. Yalçinkaya, (Yay. Haz.), BEYAS 2015 Sempozyumu Kurumsal Belleklerin Geleceği: Dijitalleştirme-ElektronikArşiv-ElektronikBelge Yönetimi” (21-22 Ekim 2015, Gölbaşı-Ankara), içinde (ss. 195-198), Ankara: Ankara Üniversitesi Belge Yönetimi ve Arşiv Sistemi Koordinatörlüğü.
- Al, H. (2007). *Bilimsel araştırma yöntemleri : akademik yazım kuralları*. Sakarya: Sakarya Yayıncılık.
- Allan, Alex. (2014). *Records Review*. Erişim tarihi ve adresi: (3 Mart 2019) [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/370930/RECORDS_REVIEW - Sir Alex Allan.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/370930/RECORDS_REVIEW_-_Sir_Alex_Allan.pdf)
- Ankara Üniversitesi Belge Yönetimi ve Arşiv Sistemi. (2009). Ankara Üniversitesi Belge Yönetimi ve Arşiv Sistemi Politikası. (Doküman No: BEYAS-DK-01). Erişim adresi: http://beyas.ankara.edu.tr/wpcontent/uploads/beyas/dosyalar/Politika_strateji/politika_metni.pdf
- Archives Act. (2012). Riigikogu (Sayı: 181). Erişim adresi: <https://www.riigiteataja.ee/en/eli/ee/504032016002/consolide/current>
- Archives Nationales. (2018). *ADAMANT: A project for the future*. Erişim tarihi ve adresi: (3 Mart 2019) <http://www.archives-nationales.culture.gouv.fr/web/guest/archiver-les-donnees-numeriques-adamant>
- Archives Nationales. (2020, 5 Mayıs). *L'archivage numérique aux Archives nationales*. Erişim tarihi ve adresi: (3 Mart 2019) <http://www.archives-nationales.culture.gouv.fr/web/guest/l-archivage-numerique-aux-Archives-nationales>
- Archives New Zealand. (2009). *Digital Continuity Action Plan*. Erişim tarihi ve adresi: (3 Mart 2019) <https://web.archive.org/web/20110812032007/http://archives.govt.nz/sites/default/files/ActionPlanDoc.pdf>
- Arhives New Zealand. (2012). *Digital Preservation Policy Manual* Erişim tarihi ve adresi: (3 Mart 2019) <https://natlib.govt.nz/files/digital-preservation/digital-preservation-policy-manual.pdf>

- Archives New Zealand. (2016). *High value and high risk*. Erişim tarihi ve adresi: (3 Mart 2019) <https://archives.govt.nz/manage-information/resources-and-guides/systems/high-value-and-high-risk>
- Archives New Zealand. (2017). *Digital transfer case study*. Erişim tarihi ve adresi: (3 Mart 2019) <https://archives.govt.nz/files/Case%20Study:%20First%20end-to-end%20born-digital%20transfer>
- Archives New Zealand. (2017). *The importance of checksums*. Erişim tarihi ve adresi: (3 Mart 2019) <https://archives.govt.nz/manage-information/resources-and-guides/transfer/the-importance-of-checksums>
- Archives New Zealand. (2018). *File formats for digital transfers*. Erişim tarihi ve adresi: (10 Mayıs 2020) <https://archives.govt.nz/manage-information/resources-and-guides/transfer/file-formats-for-digital-transfers>
- Archives New Zealand. (2018). *Digital transfer - overview*. Erişim tarihi ve adresi: (3 Mart 2019) <https://archives.govt.nz/files/Digital%20transfer%20-%20overview>
- Archives New Zealand. (6 Haziran 2020). *Disposal process*. Erişim tarihi ve adresi: (3 Mart 2019) <https://archives.govt.nz/manage-information/your-responsibilities/disposal-process>
- Archives New Zealand. (2020). *Appraisal process*. Erişim tarihi ve adresi: (3 Mart 2019) <https://archives.govt.nz/manage-information/your-responsibilities/appraisal-process>
- Archivematica. (2020). Erişim tarihi ve adresi: (5 Şubat 2020) <https://www.archivematica.org/en/>
- Arlı, M. ve Nazik, M. H. (2003). *Bilimsel araştırmaya giriş*. Ankara: Gazi Kitabevi. http://www.bilgitoplumu.gov.tr/wpcontent/uploads/2014/04/Birlikte_Calisabilirlik_Esas_lari_Rehberi_2.1.pdf
- Arısoy, Y. (2018). Elektronik Arşivlere Yönelik Uluslararası Yaklaşımlar Çerçevesinde Türkiye Değerlendirmesi. *Bilgi Yönetimi*, 1(1), 63-77 . DOI: 10.33721/by.415166
- Arısoy, Y. E. (2018). Türkiye'de elektronik belge yönetiminde milli arşiv politikalarının geliştirilmesi. (Doktora Tezi, Ankara Üniversitesi, Ankara). Erişim adresi: <https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp>
- Arısoy, Y. E. ve Özdemirci, F. (2017). Kurum ve Kuruluşların Bakış Açısından E-Belgelerin Arşivlenmesi. *DTFC Dergisi*, 57(2), 1250-1270. Erişim adresi: <http://dtcfdergisi.ankara.edu.tr/index.php/dtcf/article/view/2332/3688>

- Arslankaya, S. (2017). *Kurumsal bilgi yönetimi modeli*. (Doktora Tezi, Sakarya Üniversitesi, Sakarya). Erişim adresi: <https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp>
- Aydın, F. ve Saydom, V. (2019). Elektronik Belge Yönetimi Sistemlerinde Bilgi Varlıklarının Kullanımı. *Bilgi Yönetimi Dergisi*, 2(1), 1-8. Erişim adresi: <https://dergipark.org.tr/tr/download/article-file/735215>
- Baron, J.R. ve Borden, B.B. (2016). Opening up dark digital archives through the use of analytics to identify sensitive content. Proceedings of the 2016 IEEE International Conference on Big Data, Washington, DC, 5-8 December 2016, pp. 3324-3229. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7840978>
- Barons, M., Bhatia, S., Double, J., Fonseca, T., Green, A., Krol, S., Merwood, H., Mulinder, A., Ranade, S., Smith, J. Q., Tamara Thornhill, T. and Underdown, D. H. (2021). Safeguarding the nation's digital memory: towards a Bayesian model of digital preservation risk. *Archives and Records*, 42(1), 58-78, DOI: 10.1080/23257962.2021.1873121
- Barutçugil, İ. (2002). *Bilgi yönetimi*. İstanbul: Kariyer Yayıncılık.
- Başbakanlık Devlet Arşivleri Genel Müdürlüğü. (2005). Standart Dosya Planı. Erişim tarihi ve adresi: (24.01.2021) <https://www.resmigazete.gov.tr/eskiler/2005/03/20050325-10.htm>
- Bilgi Edinme Hakkı Kanunu. (2003). Resmi Gazete (Sayı: 25269). Erişim adresi: <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4982.pdf>
- Birlikte Çalışabilirlik Esasları Rehberi. (2012). Resmi Gazete (Sayı: 27155). Erişim adresi: <https://www.resmigazete.gov.tr/eskiler/2005/08/20050805-11.htm>
- Bilgi toplumu. (2020). Erişim tarihi ve adresi: https://tr.wikipedia.org/wiki/Bilgi_toplumu
- Brown, A. (2013). *Practical digital preservation : a how-to guide for organizations of any size*: Facet Publishing.
- Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş. ve Demirel, F. (2012). Bilimsel araştırma yöntemleri. Ankara: Pegem Akademi.
- CCSDS. (2012). *Reference Model For An Open Archival Information System (OAIS)*. Erişim tarihi ve adresi: (3 Mart 2019) <https://public.ccsds.org/pubs/650x0m2.pdf>
- Cengiz Mater, E. ve Özdemir Şahin, L. (2022). Türkiye'deki Kamu Kurum ve Kuruluşlarında Belge Yönetimi Politikası Gerekliği Üzerine Bir Çalışma. *Bilgi Yönetimi*, 5(2). 224-238. <https://doi.org/10.33721/by.1092587>

- Cıbaroğlu, M. O. ve Tıran, A. H. (2018). Elektronik Belge Yönetim Sistemlerinin Genişletilmiş Teknoloji Kabul Modeli Temelinde Kullanımı: Ampirik Bir Değerlendirme. *Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 5(2). 204-217. Erişim adresi. <https://dergipark.org.tr/tr/download/article-file/529433>
- Community Archives and Heritage Group. (2018). *Digital Preservation for Community Archives*. Erişim tarihi ve adresi: (3 Mart 2019) <https://www.communityarchives.org.uk/wp-content/uploads/2018/02/Digital-Preservation-for-Community-Archives-V1.4-2018.pdf>
- COPTR (Community Owned digital Preservation Tool Registry (2020).Erişim tarihi ve adresi: (8 Mayıs 2019) https://coptr.digipres.org/Main_Page
- COVID-19. (2020).Erişim tarihi ve adresi: 06.11.2020 <https://tr.wikipedia.org/wiki/COVID-19>
- Cox, R. J. (2011). Appraisal and the Future of Archives in the Digital Era. In *The Future of Archives and Recordkeeping: A Reader* (s. 213 - 245). Facet, London.
- CTR Uluslararası Belgelendirme ve Denetim. (2021). ISO 27001 Bilgi Güvenliği Yönetim Sistemi.Erişim tarihi ve adresi: (25 Ocak 2021) <https://belgelendirme.ctr.com.tr/iso-27001.html>
- Coşkun, R., Altunışık, R. ve Yıldırım, E. (2019). *Sosyal Bilimlerde Araştırma Yöntemleri: SPSS Uygulamalı*. Sakarya Yayıncılık. Sakarya.
- Çakmak, T. (2011). *Kurumsal içerik yönetimi kapsamında elektronik bilgi ve belge sistemlerinin bir kurum örneğinde değerlendirilmesi*. (Yüksek Lisans, Hacettepe Üniversitesi, Ankara). Erişim adresi: <https://tolgacakmak.net/tez/kurumsal-icerik-yonetimi-kapsaminda-elektronik-bilgi-ve-belge-sistemlerinin-bir-kurum-orneginde-degerlendirilmesi>
- Çakmak, T. (2016). *Türkiye’de Kültürel Bellek Kurumlarında Dijitalleştirme ve Dijital Koruma Politikaları: Bir Model Önerisi*. (Doktora Tezi, Hacettepe Üniversitesi, Ankara). Erişim adresi: <https://tolgacakmak.net/yayinlar>
- Çıngı, H. (1990). *Örnekleme Kuramı*. Ankara: Hacettepe Üniversitesi.
- Çiçek, N. (2015). *Kurumsal Bilgi ve Belge Yönetimi*. İstanbul: Marmara Belediyeler Birliği Kültür Yayınları.
- Çiçek, N. (2016). Elektronik Belge Yönetimi Uygulamalarında Bir Alt Sistem Olarak Dosya Yönetimi. *Türk Kütüphaneciliği*, 30(3). 434-448. Erişim adresi: <http://www.tk.org.tr/index.php/TK/article/view/2692>

- Çiçek, N. (2020). E-Devlet Stratejisi Bağlamında Elektronik Belge Yönetimi İçin “Yazılı Politika” Gereksinimi: Türkiye’deki Uygulamalar Üzerine Bir İnceleme. *Türk Kütüphaneciliği*, 34(3), 377-405. doi:10.24146/tk.739591
- Debons, A., Horne, E. ve Cronenweth, S. (1988). *Information Science: An Integrated View*. Boston, Mass. : G.K. Hall.
- Dede, H. ve Akbayır, A. (2017). Kamu Kurum ve Kuruluşlarında EBYS’nin Durumu F. Özdemirci ve Z. Akdoğan (Yay. haz.). Bilgi Sistemleri ve Bilişim Yönetimi Beklentiler ve Yeni Yaklaşımlar, e-BEYAS 2017 Sempozyumu, 19-20 Ekim 2017, Ankara, Türkiye, Bildiriler içinde (s.285-292), Ankara: Ankara Üniversitesi, BEYAS Koordinatörlüğü.
- Devlet Arşivleri Başkanlığı. (2019). 60 milyon tarihi belge dijital ortama aktarıldı. Erişim tarihi ve adresi: (20.02.2020) <https://www.devletarsivleri.gov.tr/Sayfalar/Haberler/Haber.aspx?ID=2142>
- Devlet Arşivleri Başkanlığı. (t.y.). Sıkça sorulan sorular. Erişim tarihi ve adresi: (25.03.2021) <https://www.devletarsivleri.gov.tr/Sayfalar/Sayfa.aspx?icerik=3&h=934515957719AB25DF388559A8E86A767FD99E56CFFDE08AE38B07C4F6D43854>
- Devlet Arşivleri Başkanlığı. (t.y.). Misyon ve vizyon. Erişim tarihi ve adresi: (20.06.2021), <https://www.devletarsivleri.gov.tr/Sayfalar/Sayfa.aspx?icerik=7&h=7063361CB AAC3C421E5402D9EED43F9CEE1A60EAAC5D7F217A7EB3D3F589CC15>
- Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi. (2018). Resmi Gazete (Sayı: 30480). Erişim adresi: <https://www.mevzuat.gov.tr/MevzuatMetin/19.5.11.pdf>
- Devlet Arşiv Hizmetleri Hakkında Yönetmelik. (2019). Resmi Gazete (Sayı: 30922). Erişim adresi: <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=33899&MevzuatTur=7&MevzuatTertip=5>
- Devlet Planlama Teşkilatı. (2005). *e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı*. Erişim tarihi ve adresi: (17 Ocak 2021) https://sbb.gov.tr/wp-content/uploads/2018/11/eDonusum_Turkiye_Projesi_Kisa_Donem_Eylem_Plani_Degerlendirme_Raporu_4.pdf

- Digital Preservation Management Workshop (2003). Erişim adresi:
<http://dpworkshop.org/dpm-eng/conclusion.html>
- Digital Preservation Coalition. (2008). What is digital preservation? Erişim tarihi ve adresi: (15 Ekim 2020) <https://www.dpconline.org/digipres/what-is-digipres>
- Digital Preservation Coalition and The National Archives. (2020). Selecting Digital Content. Novice to Know-How: Digital Preservation Skills for Beginners.
- Digital Preservation Coalition and The National Archives. (2020). Why is Digital Preservation Important?. Novice to Know-How: Digital Preservation Skills for Beginners.
- Digital records – strategies and requirements. (2020). Erişim tarihi ve adresi: (8 Mayıs 2019) <https://www.sa.dk/en/appraisal-and-transfer/digital-records-strategies-and-requirements/>
- Dişli, M. (2019). *Üniversitelerde Elektronik Belge Yönetim Sistemlerinin Birlikte Çalışabilirlik Açısından Değerlendirilmesi*. (Yüksek Lisans Tezi, Hacettepe Üniversitesi, Ankara). Erişim adresi:
<http://bby.hacettepe.edu.tr/yayinlar/%C3%9CN%C4%B0VERS%C4%B0TELE RDE%20ELEKTRON%C4%B0K%20BELGE%20Y%C3%96NET%C4%B0M %20S%C4%B0STEMLER%C4%B0N%C4%B0N%20B%C4%B0RL%C4%B0 KTE%20%C3%87ALI%C5%9EAB%C4%B0L%C4%B0RL%C4%B0K%20A %C3%87ISINDAN%20DE%C4%9EERLEND%C4%B0R%C4%B0LMES%C4%B0.pdf>
- Duranti, L. (2001). The impact of digital technology on archival science. *Archival Science*, 1(1), 39-55. Erişim adresi:
<https://link.springer.com/article/10.1007/BF02435638>
- Eastwood, T. (2007). Digital appraisal: variations on a theme (Yay. haz.). The Conference on Appraisal in the Digital World, 15-16 November 2007, The University of British Columbia, Rome, Italy.
- Elektronik Belge Standartları Hakkında Genelge. (2008). Resmi Gazete (Sayı: 26938). Erişim adresi: <http://www.resmigazete.gov.tr/eskiler/2008/07/20080716-7.htm>
- Elektronik İmza Kanunu. (2004). Resmi Gazete (Sayı: 25355). Erişim adresi:
<http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf>
- Elem, B. (2020). Dünyada her gün ne kadar veri hangi kaynaklardan üretiliyor? Erişim tarihi ve adresi: (8 Mayıs 2019) <https://2ladd.com/2019/05/dunyada-her-gun-ne-kadar-veri-hangi-kaynaklardan-uretiliyor/>

- Endüstri 4.0. (2020).Erişim tarihi ve adresi: (8 Mayıs 2019)
https://tr.wikipedia.org/wiki/End%C3%BCstri_4.0
- Eroğlu, Ş. (2017). *Türkiye'de Kamu Verilerinin Açık Devlet Uygulamaları ve Belge Yönetimi Çerçevesinde Değerlendirilmesi : Bir Model Önerisi*. (Doktora Tezi, Hacettepe Üniversitesi, Ankara). Erişim adresi:
<http://www.bby.hacettepe.edu.tr/yayinlar/dosyalar/10149938.pdf>
- E-GÜVEN. (2013). *E-imza Kullanım Alışkanlıkları Araştırması*. Erişim tarihi ve adresi: (10 Ocak 2021) http://e-guven.com/Documents/EGUVEN_Eimza_Kullanim_Aliskanliklari_Arastirmasi.pdf
- Federal Act on Archiving (Archiving Act, ArchA). (1998).(Sayı: Erişim adresi:
<https://www.admin.ch/opc/en/classified-compilation/19994756/201305010000/152.1.pdf>
- File profiling tool (DROID). (2020). Erişim tarihi ve adresi: (8 Mayıs 2020)
<https://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/file-profiling-tool-droid/>
- Freedom of Information Act. (2000). UK Public General Acts (Sayı: Erişim adresi:
<http://www.legislation.gov.uk/ukpga/2000/36/contents>
- Garland, M. (2019). The Importance of Records Management Policy. Erişim tarihi ve adresi: (07.03.2020) <https://blog.netwrix.com/2019/09/26/the-importance-of-records-management-policy/#:~:text=At%20the%20center%20of%20your,for%20ensuring%20their%20security%20destruction>
- Gibson, C. (2009). ‘How Many Different Ways Can You Spell ‘Gaddafi’? Erişim adresi: <https://nj1015.com/how-many-different-ways-can-you-spell-khadafi-let-me-count-the-ways/>
- Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik. (2022). Resmî Gazete (Sayı: 31821). Erişim adresi:
<https://www.resmigazete.gov.tr/eskiler/2022/04/20220426-11.pdf>
- Gollins, T. (2009). Parsimonious preservation: preventing pointless processes! *Online Information*, 75-78. Erişim adresi:
<http://www.nationalarchives.gov.uk/documents/information-management/parsimonious-preservation.pdf>

- Harvey, R. ve Thompson, D. (2010). Automating the appraisal of digital materials. *Library Hi Tech*, 28(2), 313-322. doi:10.1108/07378831011047703
- Harvey, R. ve Weatherburn, J. (2018). *Preserving Digital Material* (Third ed.): Rowman-Littlefield.
- Higgins, S. (2008). The DCC Curation Lifecycle Model. *The International Journal of Digital Curation*, 3(1). Eriřim adresi: <http://www.ijdc.net/article/view/69/48>
- Hollier, A. (2001). The archivist in the electronic age. HEP Libraries Webzine (3). Eriřim adresi: <https://webzine.web.cern.ch/3/papers/5/>
- Holschuh, J. and Nist, S. (2000). Active learning: Strategies for college success. Massachusetts: Allyn & Bacon.
- Hutchinson, T. (2020). Natural language processing and machine learning as practical toolsets for archival processing. *Records Management Journal*, 30(2), 157-161. <https://doi.org/10.1108/RMJ-09-2019-0055>
- InterPARES Project. ([t.y.]). Appraisal task force report. Eriřim tarihi ve adresi: (15 Mayıs 2020) http://www.interpares.org/book/interpares_book_e_part2.pdf
- Ipinge, A. ve Nengomasha, C.T. (2018). An Investigation into the Records Management Profession in the Public Service of Namibia. *Information and Learning Science*, 119(7/8), 377-388. doi: 10.1108/ILS-11-2017-0123
- ISO 15489-1. (2001). Enformasyon ve dokümantasyon – Belge yönetimi. Türk Standartları Enstitüsü.
- ISO 19005-1. (2005). Document management - Electronic document file format for long-term preservation — Part 1: Use of PDF 1.4 (PDF/A-1). Cenevre [İsviçre].
- ISO 27001. (2013). Information Security Management Systems: Requirements, Cenevre [İsviçre].
- ISO 21496. (2018). Appraisal for Managing Records. Cenevre[İsviçre].
- İngiliz Milli Arřivi (The National Archives) (2010). Belge yönetimi politikası. Eriřim adresi (12 Mart 2021):<https://www.nationalarchives.gov.uk/documents/information-management/rm-code-guide3.pdf>
- İngiltere Adalet Bakanlığı (Ministry of Justice). (2018). Belge yönetimi politikası. Eriřim adresi (12 Mart 2021):<https://www.gov.uk/government/publications/records-information-management-policy-psi-042018-pi-022018>

- İngiltere Başsavcılık Ofisi (Attorney General's Office). (2015). Belge yönetimi politikası. Erişim adresi (12 Mart 2021): <https://www.gov.uk/government/publications/records-management-policy>
- İngiltere Çalışma ve Emeklilik Bakanlığı (Department for Work and Pensions). (2021). Belge yönetimi politikası. Erişim adresi (12 Mart 2021): <https://www.gov.uk/government/publications/dwp-information-management-policies/dwp-information-management-policy>
- İngiltere Çevre, Gıda ve Tarım Bakanlığı (Department for Environment, Food and Rural Affairs). (2012). Belge yönetimi politikası. Erişim adresi (12 Mart 2021): <https://cdn.nationalarchives.gov.uk/documents/information-management/defra-ima-report.pdf>
- İngiltere Galler Hükümeti (The Welsh Government). (2018). Belge yönetimi politikası. Erişim adresi (12 Mart 2021): <https://gov.wales/sites/default/files/publications/2018-10/information-management-and-governance-policy.pdf>
- İngiltere Sağlık ve Sosyal Bakım Bakanlığı (Department of Health and Social Care). (2021). Belge yönetimi politikası. Erişim adresi (12 Mart 2021): <https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care>
- İngiltere Savunma Bakanlığı (Ministry of Defence). (2014). Belge yönetimi politikası. Erişim adresi (12 Mart 2021): https://data.parliament.uk/DepositedPapers/Files/DEP2014-1256/JSP_441_Version_4.3-FINAL-U%5B1%5D.pdf
- İngiltere Şirketler Sicil Ofisi (Companies House). (2021). Belge yönetimi politikası. Erişim adresi (12 Mart 2021): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/317573/Companies_House_Records_Management_Policy_-_Online_version.pdf
- İngiltere Topluluklar ve Yerel Yönetimler Bakanlığı (Department for Communities and Local Government). (2021). Belge yönetimi politikası. Erişim adresi (12 Mart 2021): <https://www.gov.uk/government/publications/mhclg-records-and-information-management-policy>

- İngiltere Ulaştırma Bakanlığı (Department for Transport). (2020). Belge yönetimi politikası. Erişim adresi (12 Mart 2021): <https://www.transportation.gov/digitalstrategy/policyarchive/Records-Management>
- İngiltere Ulusal Ölçüm ve Düzenleme Ofisi (National Measurement and Regulation Office). (2011). Belge yönetimi politikası. Erişim adresi (12 Mart 2021): <https://www.gov.uk/government/publications/electronic-records-management-policy>
- İslamoğlu, A. H. (2003). *Bilimsel araştırma yöntemleri*. İstanbul: Beta.
- JHOVE (2020). JHOVE -Harvard Object Validation Environment. Open Preservation Foundaiton. Erişim adresi: <https://jhove.openpreservation.org/>
- Kandur, H. (2011). Türkiye’de Kamu Kurumlarında Elektronik Belge Yönetimi: Mevcut Durum Analizi ve Farkındalığın Artırılması Çalışmaları. *Bilgi Dünyası*, 12(1), 2-12. Erişim adresi: <https://www.bd.org.tr/index.php/bd/article/view/218/214>
- Kaptan, S. (1998). *Bilimsel araştırma ve gözlem teknikleri*. Ankara: Tekışık Matbaası.
- Kenney, A. R. ve McGovern, N. Y. (2003). The Five Organizational Stages of Digital Preservation. In *Digital Libraries: A Vision for the Twenty-first Century*.
- Kişisel Verilerin Korunması Kanunu. (2016). Resmi Gazete (Sayı: 6698). Erişim adresi: <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf>
- Kişisel Verileri Koruma Kurumu. (2018). *Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular*. KVKK Yayınları, Ankara. Erişim tarihi ve adresi: (26 Ocak 2021) <https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular>
- Külcü, Ö. (2012).Türkiye’de Kurumsal Elektronik Bilgi ve Belge Yönetimi Uygulamalarına Dönük Koşulların Değerlendirilmesi: 57 Örnek Kurumun Analizi. *Türk Kütüphaneciliği*, 26(1), 30-52. Erişim adresi: <https://dergipark.org.tr/tr/download/article-file/811856>
- Külcü, Ö. (2018). *Kurumsal Bilgi Sistemleri ve Belge Yönetimi: Organizasyonlarda Bilgi ve Belge Yönetimi Sistemlerinin Temel İlkeleri*. Hiperlink Yayınları: İstanbul.
- Lavoie, B. (2014). *The Open Archival Information System (OAIS) Reference Model: Introductory Guide (2nd ed.)*. DPC Technology Watch Report: Digital Preservation Coalition.

- Lee, C. A. (2018). Computer-Assisted Appraisal and Selection of Archival Materials. IEEE International Conference on Big Data, 2721-2724. Eriřim adresi: <https://ieeexplore.ieee.org/document/8622267>
- MacKenzie, G. (2000). Searching for solutions: electronic records problems world-wide. *Managing Information*, 7, 59-65.
- Man, E. (2010), "A functional approach to appraisal and retention scheduling", *Records Management Journal*, Vol. 20 No. 1, pp. 104-116.
- McDonald, G., Macdonald, C., and Ounis, I. (2017). Enhancing sensitivity classification with semantic features using word embeddings. in *Advances in Information Retrieval*, 39th European Conference on IR Research, Aberdeen, UK, 8–13 April 2017, ed. Joemon M. Jose, Claudia Hauff, Ismail Sengor Altıngovde, Dawei Song, Dyaa Albakour, Stuart Watt, and John Tait (Springer, 2017): pp. 450–63, available at: <http://eprints.gla.ac.uk/135030>
- McDonald, G. (2019). *A framework for technology-assisted sensitivity review: using sensitivity classification to prioritise documents for review*. (PhD thesis, University of Glasgow, Scotland). Eriřim adresi: <http://theses.gla.ac.uk/41076/>
- McDonald, G., Macdonald, C., Ounis, I. ve Gollins, T. (2014). Towards a Classifier for Digital Sensitivity Review. T. K. Maarten de Rijke, Arjen P. de Vries, ChengXiang Zhai, Franciska de Jong, Kira Radinsky, Katja Hofmann (Yay. haz.). 36th European Conference on IR Research, ECIR 2014, Amsterdam, The Netherlands, April 13-16, 2014. Proceedings, Amsterdam.
- McDonald, G., Macdonald, C. ve Ounis, I. (2019a). The FACTS of Technology-Assisted Sensitivity Review. arXiv . Eriřim adresi: <https://arxiv.org/pdf/1907.02956.pdf>
- McDonald, G., Macdonald, C. ve Ounis, I. (2019b). How Sensitivity Classification Effectiveness Impacts Reviewers. Proceedings of the 2019 Conference on Human Information Interaction and Retrieval. s.337-341. Eriřim adresi: <http://www.dcs.gla.ac.uk/~graham/publications/McDonaldetal-CHIIR19.pdf>
- McDonald, G., Macdonald, C. ve Ounis, I. (2020). How the Accuracy and Confidence of Sensitivity Classification Affects Digital Sensitivity Review. *ACM Transactions on Information Systems (TOIS)*. 39 (1). S.1-34. Eriřim adresi: <http://www.dcs.gla.ac.uk/~graham/publications/TOIS-McDonaldetal.pdf>

- McLeod, J. (2015). *Access to information: Challenges and opportunities for the records profession*. (Yay. haz.). Records Management and Access to Information: challenges and guidelines for institutions of teaching and reseach, 7th Conference on Scientific Archives, 24 - 26 June 2015, Rio de Janeiro, Brazil, in (p.221-233). Rio de Janeiro : Northumbria University, UK.
- McLeod, S. (2019). What is a case study research method?Eriřim tarihi ve adresi: (6 Mayıs 2019) <https://www.simplypsychology.org/case-study.html>
- Milli Arřiv Kanun Tasarısı. (2006). Eriřim tarihi ve adresi: (8 Mayıs 2019) <https://www.memurlar.net/haber/44086/milli-arsiv-kanunu-tasarisi.html>
- Moss, M. ve Thomas, D . (2020). The four corners of the page and the digital record. *Arřiv D nyası* , 7(2),139-150 . Eriřim adresi: <https://dergipark.org.tr/tr/pub/ad/issue/58522/837284>
- Muhafazasına L zum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun H km nde Kararnamenin Deęiřtirilerek Kabul  Hakkında Kanun. (1988). Resmi Gazete (Sayı: 3473). Eriřim adresi: <http://www.mevzuat.gov.tr/MevzuatMetin/1.5.3473.pdf>
- National Records of Scotland (NRS). (2014). *The Digital Preservation Strategy*. Eriřim tarihi ve adresi: (3 Mart 2019) <https://webarchive.nrscotland.gov.uk/20170203215456/https://www.nrscotland.gov.uk/files//record-keeping/nrs-digital-preservation-strategy.pdf>
- Neuman, W. L. (2013). Toplumsal arařtırma y ntemleri: Nitel ve nicel yaklařımlar (6. bs). Ankara: Yayınodası.
- NDIIPP. (2011). *Preserving our digital heritage: National Digital Information Infrastructure and Preservation Program*. Washington, D.C.: Library of Congress.
- Niu, J. (2014). Appraisal and selection for digital curation. *School of Information Faculty Publications*, 9(2), 65–82. doi:doi:10.2218/ijdc.v9i2.272
- N.O. Sadiku, M., E. Shadare, A. ve M. Musa, S. (2017). Digital preservation. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(4), 4-7. Eriřim adresi: <http://www.ijarcsse.com/index.php/ijarcsse>
- Odabař, H. (2003). Kurumsal bilgi y netimi. *T rk K t phanecilięi*, 17(4), 357-368. Eriřim adresi: <http://www.tk.org.tr/index.php/TK/article/view/302/294>

- Open Preservation Foundation (OPF). (2020). Eriřim tarihi ve adresi: (8 Mayıs 2020)
<https://openpreservation.org/about/>
- Önal, H. İ. (1993). Bilgi ve bilgi gereksinimleri. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, 10(1). Eriřim adresi:
<https://dergipark.org.tr/tr/download/article-file/607054>
- Özdamar, K. (1997). Paket Program ile İstatistiksel Veri Analizi I. Eskiřehir: Anadolu Üniversitesi Yayınları.
- Özdamar, K. (2004). Paket Program ile İstatistiksel Veri Analizi II. Eskiřehir: Kaan Kitabevi.
- Özdemir, L. (2016). *An Insight into the Transfer of Digital Records to Archives*. G. Güneř ve diğeri (Yay. haz.). Bilgi Sistemleri Platformlar Mimariler ve Teknolojiler, ÜNAK 2013 Konferansı, 19-21 Eylül 2013, , İstanbul, Türkiye, Bildiriler içinde (s.121-126), İstanbul : Marmara Üniversitesi, Üniversite ve Arařtırma Kütüphanecileri Derneđi.
- Özdemir, L. (2017). *İngiliz Milli Arřivi'nin Yeni Stratejilerinin Gözden Geçirilmesi: Yenilikçi (Disruptive*) Arřiv Modeli* F. Özdemirci ve Z. Akdoğan (Yay. haz.). Bilgi Sistemleri ve Biliřim Yönetimi Beklentiler ve Yeni Yaklařımlar, e-BEYAS 2017 Sempozyumu, 19-20 Ekim 2017, Ankara, Türkiye, Bildiriler içinde (s.47-55), Ankara: Ankara Üniversitesi, BEYAS Koordinatörlüğü.
- Özdemir, L. (2019). The inevitability of digital transfer: How prepared are UK public bodies for the transfer of born-digital records to the archives?. *Records Management Journal*, 29(1/2),224-239. Eriřim adresi:
<https://www.emeraldinsight.com/doi/abs/10.1108/RMJ-09-2018-0040>
- Özdemir, L. ve Cengiz, E. (2019). *Türk Kamu Sektöründe Dijital Süreklilik Ne Kadar Mevcut: Teorik Bir Çerçeve*. B. Yalçınkaya ve diğeri (Yay. haz.). Bilgi Yönetimi ve Bilgi Güvenliđi : eBelge-eArřiv-eDevlet-Bulut Biliřim-Büyük Veri-Yapay Zeka, e-BEYAS 2019 Sempozyumu, 10-11 Ekim 2019, Ankara, Türkiye, Bildiriler içinde (s.273-294), Ankara: Ankara Üniversitesi, BEYAS Koordinatörlüğü.
- Özdemir řahin, L . (2020). Archives in the Digital Age: is the Turkish Generation Z Equipped for the Challenge?. *Arřiv Dünyası*, 7(1), 1-14. Eriřim adresi:
<https://dergipark.org.tr/tr/pub/ad/issue/55174/746935>

- Özdemir Şahin L. ve Saydam, V. (2022). Digital Continuity Practices in Municipalities: A Study on Municipalities in Istanbul . *Bilgi Yönetimi* , 5(1) , 131-146 . DOI: 10.33721/by.932771
- Özdemirci, F. (2001). *Belge Üretimi ve Kurumsal Bilgi Yönetimi* T. Fenerci ve O. Gürdal (Yay. haz.). 21. Yüzyıla Girerken Enformasyon Olgusu Sempozyumu, 19-20 Nisan 2001, Hatay, Türkiye, Bildiriler içinde (s.179-186). Ankara: Türk Kütüphaneciler Derneği.
- Özdemirci, F. (2003). İlk Uluslararası Belge Yönetim Standardı: Ülkemiz Açısından Bir Değerlendirme. *Türk Kütüphaneciliği*, 17(3), 225-246. Erişim adresi: https://fahrettinozdemirci.com.tr/wp-content/uploads/2018/09/ilk_uls_blg_ynt_standardi-1.pdf
- Özdemirci, F. (2004). Bilgi Edinme Hakkı Kanunu: Kamu Belgelerinin Yönetimi ve Arşivler. In D. Atılgan (Ed.), *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Bilgi ve Belge Yönetimi Bölümü'nün Kuruluşunun 50. Yılına Armağan* (s. 65-77). Ankara: Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Bilgi ve Belge Yönetimi Bölümü.
- Özdemirci, F. (2019). *Kurumlar için EBYS ve e-Arşiv Sistemi İdari Yapılanma ve Yönetim Süreci: Bileşenler ve Entegrasyonlar*. B. Yalçınkaya ve diğerleri (Yay. haz.). Bilgi Yönetimi ve Bilgi Güvenliği : eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zeka, e-BEYAS 2019 Sempozyumu, 10-11 Ekim 2019, Ankara, Türkiye, Bildiriler içinde (s.3-9), Ankara: Ankara Üniversitesi, BEYAS Koordinatörlüğü.
- Özdemirci, F. ve Aydın, C. (2007). Kurumsal Bilgi Kaynakları ve Bilgi Yönetimi. *Türk Kütüphaneciliği*, 21(2), 164-185. Erişim adresi: <http://www.tk.org.tr/index.php/TK/article/view/58>
- Öztemiz, S. ve Özel, N. (2019). Dijital Kütürlük: Kavramsal Bir Değerlendirme. *DTCF Dergisi*, 59(2), 1208-1226. doi:10.33171/dtcfjournal.2019.59.2.22
- Pierce-Moses, R. (2005). Dictionary of Archives Terminology. Erişim adresi: <https://dictionary.archivists.org/index.html>
- PRONOM. (2020).Erişim tarihi ve adresi: (8 Mayıs 2020) <https://www.nationalarchives.gov.uk/aboutapps/pronom/default.htm>
- Public Records Act 2005. (2017). The Department of Internal Affairs. (Sayı: 40). Erişim adresi: <http://www.legislation.govt.nz/act/public/2005/0040/latest/DLM345737.html>

- Rahvusarhiivi Juhis (Ulusal Arşiv Rehberi). (2008). Digitaaldokumentide arhiveerimise nõuded/Dijital belgeleri arşivleme gereksinimleri. Erişim tarihi ve adresi: (3 Mart 2019) https://www.ra.ee/wp-content/uploads/2016/12/digidok_arhiveerimine-1.pdf
- Ranade, S. (2018). Access technologies for the disruptive digital archive. In C. Brown (Ed.), Archival Futures. London: Facet Publishing.
- Raosoft. (2004). Sample size calculator. Erişim tarihi ve adresi: (8 Mart 2019) <http://www.raosoft.com/samplesize.html>
- Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik. (2020). Resmî Gazete (Sayı: 31151). Erişim adresi: <https://tccb.gov.tr/assets/dosya/resmiyazisma/dosyalar/yonetmelik.pdf>
- Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik Kılavuzu (2020). Erişim adresi: <https://www.tccb.gov.tr/resmiyazisma/kilavuz/>
- Sanayi devrimi. (2020). Erişim tarihi ve adresi: (8 Mayıs 2018) https://tr.wikipedia.org/wiki/Sanayi_Devrimi
- Sağlık Bakanlığı. (2014). Bilgi Güvenliği Politikaları Kılavuzu. Erişim tarihi ve adresi: <https://bilgiguvenligi.saglik.gov.tr/files/BilgiG%C3%BCvenli%C4%9FiPolitikalar%C4%B1K%C4%B1lavuzu.pdf>
- Sağsan, M. (2006). *Bilgi yönetimi bakış açısından bilgi süreçleri ve bir model önerisi*. A. Yıldızeli ve H. K. Bahşioğlu (Yay. haz.). ÜNAK'06 Bilimsel İletişim ve Bilgi Yönetimi Bildiriler Kitabı içinde, Ankara : ÜNAK.
- Saydam, V. (2015). Elektronik Belge Yönetimi Uygulamalarında Personel farkındalığının Arttırılması: Değişim Yönetimi üzerine Bir İnceleme. *Bilgi ve Belge Araştırmaları Dergisi*, 3, 23-32. Erişim adresi: <https://dergipark.org.tr/tr/download/article-file/454336>
- Shepherd, E. And Yeo, G. (2003). Implementing Records Management: Practical and Managerial Issues. Elizabeth S. and Geoffrey Y. (Ed.), Managing Records: A Handbook of Principles and Practice. (s.246-269) içinde. London. Facet.
- Sheridan, John. (2021). Geleceğin Yapıtaşları: Bilim-Teknoloji ve Bilgi/Belge Yönetimi Bütünleşmesine Doğru Arşivciliğin ve Arşivlerin Rotası Sempozyumu,9 Haziran 2021. Erişim tarihi ve adresi: (13 Haziran 2021) <https://www.youtube.com/watch?v=bym1kfn19Kg>

- Sloyan, V. (2016). Born-digital archives at the Wellcome Library: appraisal and sensitivity review of two hard drives. *The Journal of the Archives and Records Association*, 37(1), 20-36. doi:10.1080/23257962.2016.1144504
- Smith, A. (1999). The future of the past: preservation in American research libraries. Washington, DC: Council on Library and Information Resources.
- Solhan, S. (2015). Fizikselden Elektroniğe; Belge Yönetim ve Arşivleme Sürecinin Sürdürülebilirliği. F. Özdemirci ve diğerleri (Ed.), e-BEYAS 2015 Sempozyumu: Kurumsal Belleklerin Geleceği: Dijitalleştirme-Elektronik Arşiv-Elektronik Belge Yönetimi Sempozyumu, 21-22 Ekim 2015, Ankara, Türkiye, Bildiriler içinde (s. 49-63). Ankara: Ankara Üniversitesi BEYAS Koordinatörlüğü.
- Swiss Federal Archives. (2015). *Federal Archives Strategy 2016 - 2020*. Erişim tarihi ve adresi: (3 Mart 2019) <https://www.bar.admin.ch/bar/en/home/about-us/the-federal-archives/strategy.html>
- Swiss Federal Archives. (2019). *Digital Archiving Policy*. Erişim tarihi ve adresi: (3 Mart 2019) <https://www.bar.admin.ch/bar/en/home/archiving/digital-documents.html>
- Şen, Ş. (2013). ISO 27001 Kurumsal Bilgi Güvenliği Standardı. Erişim tarihi ve adresi: <https://ab.org.tr/ab13/sunum/216.pdf>
- Şişkin, D. Ş. ve Çakmak, T. (2020). Üniversite Kütüphanelerinde Kişisel Veriler: Ankara'daki 15 Üniversite Kütüphanesindeki Uygulamaların Analizi. *Türk Kütüphaneciliği*, 34(3), 458-484. doi:10.24146/tk.754346
- Tarım devrimi. (2020). Erişim tarihi ve adresi: (19 Mart 2019) https://tr.wikipedia.org/wiki/Tar%C4%B1m_devrimi
- T. C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı. (t.y.). Sıkça sorulan sorular. Erişim tarihi ve adresi: (25.03.2021) <https://www.devletarsivleri.gov.tr/Sayfalar/Sayfa.aspx?icerik=3&h=934515957719AB25DF388559A8E86A767FD99E56CFFDE08AE38B07C4F6D43854>
- T. C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı. (t.y.). Misyon ve vizyon. Erişim tarihi ve adresi: (20.06.2021) <https://www.devletarsivleri.gov.tr/Sayfalar/Sayfa.aspx?icerik=7&h=7063361CB AAC3C421E5402D9EED43F9CEE1A60EAAC5D7F217A7EB3D3F589CC15>
- T. C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı. (2019). *2020-2024 Dönemi Stratejik Planı*. Erişim tarihi ve adresi: (30 Ekim 2019)

<https://www.devletarsivleri.gov.tr/varliklar/dosyalar/raporlar/DAB20202024SP.pdf>

T. C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı. (2020). *2020 Yılı Faaliyet Raporu*.

Erişim adresi:

<https://www.devletarsivleri.gov.tr/varliklar/dosyalar/raporlar/devletarsivleri2020faaliyetraporu.pdf>

TBMM. (2013). Bilgi Edinme Hakkı Çalıştayı Sonuç Raporları. Erişim tarihi ve adresi: (17 Ocak 2021)

https://www.tbmm.gov.tr/bilgi edinme/bilgi_edinme_calistay_raporu.pdf

Tecim, V. (2020). Bilginin Hiyerarşisi Piramidi. Erişim adresi:

<https://vahaptecim.com.tr/yonetim-bilisim-sistemleri/>

The Danish National Archives (2013). *Strategy for archiving digital records at the*

Danish National Archives. Erişim tarihi ve adresi: (3 Mart 2019)

<https://www.sa.dk/wp-content/uploads/2014/12/Strategy-for-archiving-digital-records-2013.pdf>

The National Archives. (2013). Best practice guide to appraising and selecting records for The National Archives. Erişim tarihi ve adresi: (5 Haziran 2020)

<https://www.nationalarchives.gov.uk/documents/information-management/best-practice-guide-appraising-and-selecting.pdf>

The National Archives. (2013). What is appraisal? Erişim tarihi ve adresi: (7 Temmuz 2020) [https://www.nationalarchives.gov.uk/documents/information-](https://www.nationalarchives.gov.uk/documents/information-management/what-is-appraisal.pdf)

[management/what-is-appraisal.pdf](https://www.nationalarchives.gov.uk/documents/information-management/what-is-appraisal.pdf)

The National Archives. (2004). *Background paper-the "Grigg System" and beyond*.

Erişim tarihi ve adresi: (7 Haziran 2020)

<https://www.nationalarchives.gov.uk/documents/information-management/background-appraisal.pdf>

The National Archives. (2011). *Digital Preservation Policies: Guidance for archives*.

Erişim tarihi ve adresi: (7 Mayıs 2019)

<https://www.nationalarchives.gov.uk/documents/information-management/digital-preservation-policies-guidance-draft-v4.2.pdf>

The National Archives. (2016). The application of technology assisted review to born-digital records transfer, Inquiries and beyond. Erişim tarihi ve adresi: (7

Temmuz 2019) <https://www.nationalarchives.gov.uk/documents/technology-assisted-review-to-born-digital-records-transfer.pdf>

- The National Archives. (2017). Digital Strategy. Eriřim tarihi ve adresi: (12 Ocak 2019) <https://www.nationalarchives.gov.uk/documents/the-national-archives-digital-strategy-2017-19.pdf>
- The National Archives. (2017). DROID : user guide. Eriřim tarihi ve adresi: (6 Ocak2019) <http://www.nationalarchives.gov.uk/documents/information-management/droid-user-guide.pdf>
- The National Archives. (2017). Managing Digital Continuity. Eriřim tarihi ve adresi: (9 řubat 2019) <https://www.nationalarchives.gov.uk/documents/information-management/managing-digital-continuity.pdf>
- The National Archives. (2017). *Understanding Digital Continuity*. Eriřim tarihi ve adresi: (7 řubat 2019) <http://www.nationalarchives.gov.uk/documents/information-management/understanding-digital-continuity.pdf>
- The National Archives. (2017). *What is an information asset?* . Eriřim tarihi ve adresi: (8 Mart 2019) <https://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf>
- The National Archives. (2019). *Digital transfer steps*. Eriřim tarihi ve adresi: (15 Mayıs 2020) <https://www.nationalarchives.gov.uk/information-management/manage-information/digital-records-transfer/digital-transfer-steps/>
- The National Archives. (2019). *Steps 1 and 2: Appraisal and selection*. Eriřim tarihi ve adresi: (15 Mayıs 2020) <https://www.nationalarchives.gov.uk/information-management/manage-information/digital-records-transfer/digital-transfer-steps/steps-1-and-2-appraisal-and-selection/>
- The National Archives. (2019). *Step 3: Sensitivity review*. Eriřim tarihi ve adresi: (15 Mayıs 2020) <https://www.nationalarchives.gov.uk/information-management/manage-information/digital-records-transfer/digital-transfer-steps/step-3-sensitivity-review/>
- The National Archives. (2019). *Step 4: Preparation for transfer*. Eriřim tarihi ve adresi: (15 Mayıs 2020) <https://www.nationalarchives.gov.uk/information-management/manage-information/digital-records-transfer/digital-transfer-steps/step-4-preparation-for-transfer/>

- The National Archives. (2019). *Step 5: Packaging and delivery*. Eriřim tarihi ve adresi: (15 Mayıs 2020) <https://www.nationalarchives.gov.uk/information-management/manage-information/digital-records-transfer/digital-transfer-steps/step-5-packaging-and-delivery/>
- The National Archives. (2019). What is Digital Continuity? Eriřim tarihi ve adresi: (20 řubat 2019) <https://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/what-is-digital-continuity/>
- The National Archives. (2018). *Preservation Policy*. Eriřim tarihi ve adresi: (8 Nisan 2019) <https://www.nationalarchives.gov.uk/documents/preservation-policy-june-2018.pdf>
- The National Archives. (2020). 20-year rule. Eriřim tarihi ve adresi: (8 Mayıs 2019) <https://www.nationalarchives.gov.uk/about/our-role/transparency/20-year-rule/#>
- The National Archives and Records Administration (NARA). (2014). *NARA Bulletin 2014-04: Format Guidance for the Transfer of Permanent Electronic Records*. Eriřim tarihi ve adresi: (4 Mayıs 2020) <https://www.archives.gov/records-mgmt/bulletins/2014/2014-04.html>
- The National Archives and Records Administration (NARA). (2015). *Bulletin 2015-04: Metadata Guidance for the Transfer of Permanent Electronic Records*. Eriřim tarihi ve adresi: (5 Nisan 2020) <https://www.archives.gov/records-mgmt/bulletins/2015/2015-04.html>
- The National Archives and Records Administration (NARA). (2018). *2018–2022 Strategic Plan*. Eriřim tarihi ve adresi: (3 Mart 2019) <https://www.archives.gov/files/about/plans-reports/strategic-plan/2018/strategic-plan-2018-2022.pdf>
- The National Archives and Records Administration (NARA). (2019). *Preservation Strategy 2019- 2022*. Eriřim tarihi ve adresi: (15 Mayıs 2020) <https://www.archives.gov/files/preservation/pres-strategy-2019.pdf>
- The National Archives and Records Administration (NARA). (2019). *Transition to Electronic Records*. Eriřim tarihi ve adresi: (3 Mart 2019) <https://www.whitehouse.gov/wp-content/uploads/2019/08/M-19-21-new-2.pdf>

- The National Archives of Australia. (2011). *Digital transition policy*. Eriřim tarihi ve adresi: (10 Mart 2018) <https://www.naa.gov.au/information-management/information-management-policies/digital-continuity-2020-policy/digital-transition-policy#reporting>
- The National Archives of Australia. (2015). *Digital Continuity 2020 Policy*. Eriřim tarihi ve adresi: (3 Mart 2019) http://www.naa.gov.au/Images/Digital-Continuity-2020-Policy_tcm16-93933.pdf
- The National Archives of Australia. (2018). *Digital Preservation Policy*. Eriřim tarihi ve adresi: (7 Mart 2019) <https://www.naa.gov.au/about-us/our-organisation/accountability-and-reporting/archival-policy-and-planning/digital-preservation-policy>
- The National Archives of Australia. (2018). *The Archives 2020 Strategic Plan*. Eriřim tarihi ve adresi: (7 Nisan 2019) <https://www.naa.gov.au/about-us/our-organisation/accountability-and-reporting/archives-2020-strategic-plan>
- The National Archives of Australia. (2020). *Transferring information to the National Archives. (2020, 5 Mayıs)*. Eriřim tarihi ve adresi: (15 Mayıs 2020) <https://www.naa.gov.au/information-management/dispose-information/transferring-information/transferring-information-national-archives>
- The National Archives of Estonia. (2005). *Dijital Arřivleme Stratejisi 2005-2010*. Eriřim tarihi ve adresi: (3 Mart 2019) <https://www.ra.ee/wp-content/uploads/2016/12/digistrateegia.pdf>
- The National Archives of Estonia. (2020, 6 Mayıs). *The universal archiving module (UAM)*. Eriřim tarihi ve adresi: (21 Mayıs 2020) <http://www.ra.ee/en/information-management/universal-archiving-module/>
- The National Archives of Estonia. (2020). Eriřim tarihi ve adresi: (20 Mayıs 2020) <http://www.ra.ee/en/national-archives/about-us/>
- The National Archives of Ireland. (2020, 7 Mayıs). *Responsibilities under legislation*. Eriřim tarihi ve adresi: (3 Mart 2019) <https://www.nationalarchives.ie/services-to-government-and-courts/responsibilities-under-legislation/>
- Tonta, Y. (1999). Bilgi toplumu ve bilgi teknolojisi. *Türk Kütüphanecilięi*, 13(4), 363-375. Eriřim adresi: <http://www.tk.org.tr/index.php/TK/article/view/910/904>
- Townley, C. T. (2001). Knowledge management and academic libraries. *College and Research Libraries*, 62(1), 44-55. doi:10.5860/crl.62.1.44

- TS 13298. (2015). Elektronik Belge Yönetimi. Ankara: Bilgi Teknolojileri ve İletişim İhtisas Grubu Türk Standartları Enstitüsü.
- Türkiye Cumhuriyeti Cumhurbaşkanlığı. (2020). *Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik Kılavuzu*. Erişim tarihi ve adresi: (3 Mart 2019) <https://tccb.gov.tr/assets/dosya/resmiyazisma/dosyalar/kilavuz.pdf>
- Türkiye Kamu Hastaneleri Kurumu. (2017). Hizmet içi eğitim programı-Başbakanlık Devlet Arşivleri Genel Müdürlüğü sunumları. 16.09.2017 tarihinde <http://khgm.saglik.gov.tr/Dosyalar/7b4a600795de406f973e76847b2e23e3.pdf> adresinden erişilmiştir
- Ulusal Meslek Standartlarına Dair Tebliğ (2021, 9 Mayıs). Resmi Gazete (Sayı: 31046 (Mükerrer). Erişim adresi: <https://www.resmigazete.gov.tr/eskiler/2020/02/20200221M1-2.htm>
- VeraPDF (2020). Erişim tarihi ve adresi: (8 Mart 2020) <https://verapdf.org>
- Yalçinkaya, B. (2014). *E-Devlet Üst Veri Standardının Oluşturulması ve Türkiye için Modellenmesi* (Yayımlanmamış doktora tezi). Marmara Üniversitesi, Türkiyat Araştırmaları Enstitüsü, İstanbul.
- Yalçinkaya, B. (2015). Milli Arşivlerin Elektronik Belge Yönetiminde Rolü ve Önemi. F. Özdemirci ve diğerleri (Yay. haz.). Elektronik Belge Yönetimi ve Arşiv Uygulamaları Sempozyumu. e-BEYAS 2014 Sempozyumu, 20-21 Mart 2014, Ankara, Türkiye, Bildiriler içinde (s.151-157), Ankara: Ankara Üniversitesi, BEYAS Koordinatörlüğü.
- Yalçinkaya, B. ve Saydam, V. (2018). Elektronik Belge Yönetiminde Personel Farkındalığının Uygulama Sürecine Etkisi: Bağcılar Belediyesi ile Marmara Üniversitesinin Karşılaştırmalı Analizi. *Bilgi ve Belge Araştırmaları Dergisi*, 9, 1-25. Erişim adresi: <https://dergipark.org.tr/tr/download/article-file/588349>
- Yeo, G. (2018). Can we keep everything? The future of appraisal in a world of digital profusion. In C. Brown (Ed.), *Archival futures*. London: Facet Publishing.
- Yılmaz, H. (2016). TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi. *Denetim* (15), 45-59. Erişim adresi: <https://dergipark.org.tr/tr/pub/denetisim/issue/22466/240291>
- Yükseköğretim Kurulu. (2017). Yükseköğretim Üst Kuruluşları ve Yüksek Öğretim Kurumları Saklama Süreli Standart Dosya Planı. Erişim adresi: https://www.yok.gov.tr/Documents/Universiteler/Standart_Dosya_Plani.pdf

Walliman, N. S. R. (2011). *Research methods: the basics*. USA and Canada: Routledge.

What are born-digital records? (2020).Eriřim tarihi ve adresi: (13 řubat 2020)

<https://www.nationalarchives.gov.uk/information-management/manage-information/digital-records-transfer/what-are-born-digital-records/>

What is PRONOM? (2020).Eriřim tarihi ve adresi: (8 Mayıs 2020)

<http://www.nationalarchives.gov.uk/PRONOM/Default.aspx>



EKLER

EK 1. Dijital Çağda Doğuştan Dijital Belgelerin Bilgi Yönetim Süreçleri Anketi

Değerli Katılımcı,

Bu çalışma Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümü'nde doktora öğrencisi olan Emine CENGİZ'in doktora tezi kapsamında gerçekleştirilmektedir. Çalışma, Türkiye'de dijital çağ ile birlikte kurumsal bilgi yönetim süreçlerinde (dijital belgelerin üretiminden milli arşive transferine giden süreç) yaşanan değişimi ortaya koymak, Türkiye'de kurumsal bilgi yönetim süreçlerinde yaşanan sorunları ve sebeplerini ortaya koymak, Türkiye'de kamu kurum ve kuruluşlarının dijital belge yönetimi konusunda karşılaşılabileceği zorlukları belirlemek, dijital belgelerin kurumsal bilgi yönetim süreçlerini nasıl etkilediğini belirlemek ve mevcut sorunlara çözüm üretmek amacıyla gerçekleştirilmektedir. Çalışma için gerekli etik kurul izni alınmıştır (İzin sayı ve tarih:9/12.05.2020). Anket kamu çalışanlarına uygulanmaktadır. Çalışmada hiçbir şekilde kurumsal ve kişisel veri kullanılmayacaktır. Çalışmanın başarısı ve geçerliliği tamamen sizin katılımınıza bağlıdır. Anket konusunda Marmara Üniversitesi Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümü doktora öğrencisi Öğr. Gör. Emine CENGİZ ile iletişim kurabilirsiniz. Araştırmaya katkılarınız ve ayırdığınız zaman için teşekkür ederiz.

Öğr. Gör. Emine CENGİZ
Marmara Üniversitesi
Bilgi ve Belge Yönetimi Bölümü
Doktora Öğrencisi

Genel Bilgiler

1.Eğitim durumunuz nedir? *

- ☐ Doktora
- ☐ Yüksek Lisans
- ☐ Lisans
- ☐ Ön Lisans
- ☐ Lise ve Dengi Okul
- ☐ Ortaöğretim mezunu
- ☐ İlköğretim mezunu

2. Kurumunuzda yapmış olduğunuz göreviniz nedir? (Kütüphaneci, Arşivci, Bilgi Yöneticisi, EBYS Sorumlusu vb.) *

3. Çalıştığınız kurum türünü lütfen işaretleyiniz. *

- ☐ Üniversite
- ☐ Bakanlık
- ☐ Belediye
- ☐ Diğer:

4. Çalıştığınız sektör nedir? (Örn: Eğitim, Kültür ve Sanat, Enerji, Finans, Ulaşım, Turizm, Ticaret, Sağlık v.b.) *

Dijital Belge ve EBYS

5. Kurumunuzda belgenin hem basılı hem dijital hali (hibrit) saklanmaya devam ediyor mu? *

☐ Evet, yasal sorumluluk olduğu için saklanmaya devam edilmektedir.

☐ Hayır

☐ Bir kısmı saklanıyor bir kısmı saklanmıyor.

☐ Diğer: _____

6. Kurumunuzda fiziksel (kâğıt) belgeler dijitalleştiriliyor mu? *

☐ Evet

☐ Hayır

☐ Diğer: _____

7. Kurumunuzda fiziksel belgelerin ne kadarı dijital ortamdadır? (yaklaşık olarak) *

☐ %10'dan az

☐ %11-20 arası

☐ %21-40 arası

☐ % 41-60 arası

☐ %61- 80 arası

☐ %81-100 arası

☐ Bilmiyorum

☐ Diğer: _____

8. EBYS (Elektronik Belge Yönetim Sistemi) bir arşiv midir yoksa Bilgi Yönetim Sistemi midir? *

☐ EBYS bir arşivdir.

☐ EBYS bir Bilgi Yönetim Sistemi'dir.

☐ EBYS hem arşiv hem de Bilgi Yönetim Sistemi'dir.

☐ Bilmiyorum

☐ Diğer: _____

9. Kurumunuzda kaç senedir EBYS kullanılmaktadır? *

☐ 1-3 yıl

☐ 4-6 yıl

☐ 7-9 yıl

☐ 10+ yıl

☐ Kurumumuzda EBYS (Elektronik Belge Yönetim Sistemi) kullanılmamaktadır.

☐ Diğer: _____

10. Kurumunuz kullandığı EBYS' yi daha önce değiştirdiyse bu değişimin sebebi nedir? *

☐ Maliyet

☐ İşlevsellik

☐ Üst yönetim kararı

☐ Hepsi

☐ EBYS değişikliği yapılmadı.

☐ Bilmiyorum

☐ Diğer: _____

11. Kurumunuzda kaç senedir elektronik/dijital ortamda belge üretiliyor? *

☐ 1-5 yıl

☐ 6-10 yıl

☐ 11-15 yıl

☐ 16-20 yıl

☐ 20+

☐ Diğer: _____

Dijital Belgeler için Bilgi Varlığı, Saklama Planı, Dosya Formatları ve Dijital Süreklilik

12. Kurumunuzdaki her birimin bilgi varlığı (varlığın verimli bir şekilde anlaşılması, paylaşılabilmesi, korunması ve kullanılabilmesi için tek bir birim olarak tanımlanan ve yönetilen bilgi yığınıdır) envanteri var mıdır? Örn. kullanıcı bilgileri envanteri, personel maaş bilgileri envanteri, veritabanları envanteri vb. *

☐ Evet

☐ Hayır

☐ Bilmiyorum

☐ Diğer: _____

13. Kurumunuzda her bir bilgi varlığının bir bilgi varlık sorumlusu var mıdır? *

☐ Evet

☐ Hayır

☐ Bilmiyorum

☐ Diğer: _____

14. Kurumunuzda dijital belgelerin arşivlenmesine yönelik bir e-Arşiv sistemi bulunmakta mıdır? *

☐ Evet

☐ Hayır

☐ Diğer: _____

15. Kurumunuzda dijital belgelerin saklama süreleri ne zaman belirlenmektedir? *

☐ Belgeyi üretirken

☐ Belgeler oluşturulmadan önce

☐ Belge üzerinde son işlem yapıldıktan sonra

☐ Belgeyi arşivlerken

☐ Kurumumuzda dijital belgeler için saklama süresi belirlenmemektedir.

☐ Diğer: _____

16. Dijital belgeleriniz için kullandığınız bir dosyalama sistemi (Standart dosya planı) bulunmakta mıdır? *

☐ Evet

☐ Hayır

☐ Diğer: _____

17. Kurumunuzda standart dosya planına uyulmasını değerlendiriniz. (1- çok yetersiz, 5- çok yeterli) *

[1] [2] [3] [4] [5]

18. Kurumunuzda bir belgenin sistem içerisinde birden fazla nüshasının bulunması sorunu mevcut mudur? *

[] Evet mevcuttur.

[] Hayır mevcut değildir.

[] Diğer: _____

19. Kurumunuzda bir belgenin sistem içerisinde birden fazla nüshasının olmasında neler yapılmaktadır? *

[] Manuel olarak her belge tek tek sistemden kontrol edilip ayıklanmaktadır.

[] Bir yazılım programı tarafından fazla nüsha olan belgeler sistem içerisinde tespit edilmektedir.

[] Hiçbir çalışma yapılmamaktadır.

[] Bir fikrim yok

[] Sistemimizde birden fazla nüsha sorunu yoktur.

[] Diğer: _____

20. Kurumunuzda dijital belge oluştururken aşağıdaki unsurlar ne derece dikkate alınmaktadır? * (1- Aşırı derece, 2- Kısmen, 3- Çok az, 4- Hiç)

Özgünlük	[1]	[2]	[3]	[4]
Güvenilirlik	[1]	[2]	[3]	[4]
Birlikte çalışabilirlik	[1]	[2]	[3]	[4]
Tekrar kullanılabilirlik	[1]	[2]	[3]	[4]
Tanımlama ve onaylama kolaylığı	[1]	[2]	[3]	[4]
Gizlilik	[1]	[2]	[3]	[4]
Bütünlük	[1]	[2]	[3]	[4]

21. Kurumunuzda bulunan dijital belgeler hangi formatlarda saklanmaktadır? (Birden fazla seçenek işaretleyebilirsiniz) *

[] Microsoft Word 97 Binary Document Format (DOC)

[] Microsoft Word Office Open XML (DOCX)

[] Portable Document Format (PDF)

[] Portable Document Format (PDF/A-1a)

[] Portable Document Format (PDF/A-1b)

[] Düz metin (txt)

[] EPUB, Electronic Publication, version 3

[] Hypertext Markup Language (HTML)

[] Rich Text Format (RTF)

[] Bilmiyorum

[] Diğer: _____

22. Kurumunuzda dijital belgeler için belirlenmiş formatlar neye göre/kim tarafından belirlenmektedir? *

- ☐ Kurum kendisi belirlemektedir.
☐ TS 13298 Standardında belirlenen dosya formatları kullanılmaktadır.
☐ Birlikte Çalışabilirlik Esasları Rehberinde belirlenmiş dosya formatları kullanılmaktadır.
☐ Belirlenmiş bir format yapısı yoktur.
☐ Diğer: _____

23. Dijital süreklilik (Bilginin ihtiyaç olduğunda bulunabilir, ihtiyaç olduğunda açılabilir, gerektiği şekilde onunla çalışılabilir, ne olduğu ve ne hakkında olduğu anlaşılabilir, içeriğine güvenilebilir olmasıdır) terimini daha önce duydunuz mu? *

- ☐ Evet
☐ Hayır
☐ Kısmen

24. Sizce bir kurumda dijital sürekliliğin iyi yönetilememesi aşağıdaki unsurların gerçekleşmesini nasıl etkiler? * (1- Kesinlikle katılmıyorum, 5 - Kesinlikle katılıyorum)

Bilgi kaybına yol açabilir.	[1]	[2]	[3]	[4]	[5]
Etkili ve verimli çalışmayı olumsuz etkiler.	[1]	[2]	[3]	[4]	[5]
Üst veri eksikliğinden ötürü çeşitli destek ödeneklerinin sağlanamamasına yol açar.	[1]	[2]	[3]	[4]	[5]
Çeşitli formatlarda oluşturulmuş belgeleri açmak ve kullanmak istendiğimizde donanım ve yazılımın desteklememesi	[1]	[2]	[3]	[4]	[5]
Veri göçünün gerçekleştirilememesi	[1]	[2]	[3]	[4]	[5]
Kritik bir proje için gerekli olan bilginin bulunamaması	[1]	[2]	[3]	[4]	[5]

Uzun Vadede Erişilebilirlik, Koruma, Üst Veri ve Tanımlama Süreçleri

25. Kurumunuzda dijital belgelerin uzun vadede erişilebilir olması için herhangi bir çalışma var mıdır? *

- ☐ Evet
☐ Hayır
☐ Çalışmalar planlanmaktadır.
☐ Diğer: _____

26. Dijital belgelerin uzun vadede erişilebilir olması için kurumunuzun aşağıdaki çalışmalara ne derecede ihtiyacı vardır? * (1- Hiç ihtiyaç yok, 5 - Çok ihtiyaç var)

Depolama ortamlarının sürekliliği sağlanmalı	[1]	[2]	[3]	[4]	[5]
Dijital süreklilik tüm kurum bünyesinde önemsenmeli ve uygulanmalı	[1]	[2]	[3]	[4]	[5]
Kurumda bilgi varlık envanteri oluşturulmalı ve sorumlular belirlenmeli	[1]	[2]	[3]	[4]	[5]
Konu kapsamında politika, strateji, rehber vb. oluşturulmalı	[1]	[2]	[3]	[4]	[5]
Bir risk planlaması yapılmalı	[1]	[2]	[3]	[4]	[5]
Uygun veri formatları kullanılmalı	[1]	[2]	[3]	[4]	[5]
Standartlara uygun üst veri oluşturulmalı	[1]	[2]	[3]	[4]	[5]
Konu kapsamında düzenli aralıklarla eğitimler verilmeli	[1]	[2]	[3]	[4]	[5]

27. Kurumunuzda var olan dijital belgelerin uzun vadeli korunması ile ilgili aşağıdaki kaygı durumlarına ne derecede katılmaktasınız? * (1- Kesinlikle katılmıyorum, 5 - Kesinlikle katılıyorum)

Mevcut yazılım ve donanımın güncel tutulması ve korunmasının zor olması	[1]	[2]	[3]	[4]	[5]
İçerik biçimlerinin karmaşık ve kırılgan olması	[1]	[2]	[3]	[4]	[5]
Yasal ve politik risklerin var olması	[1]	[2]	[3]	[4]	[5]
Hacim veya karmaşıklık kapsamında içerik toplamanın zor olması	[1]	[2]	[3]	[4]	[5]
Yetersiz personele sahip olmak	[1]	[2]	[3]	[4]	[5]
İçeriğin yetersiz tanımlanması kullanımını ve keşfedilmesini zorlaştırabilmesi	[1]	[2]	[3]	[4]	[5]
Dosya formatlarının hızlı değişiklik göstermesi ve eski dosya formatlarının okunamaması	[1]	[2]	[3]	[4]	[5]

28. Kurumunuzda dijital belgelerin uzun vadeli korunmasından hangi birim sorumludur? *

☐ Kütüphane ve Dokümantasyon Daire Başkanlığı

☐ Arşiv Daire Başkanlığı

☐ Belge Yönetimi Daire Başkanlığı

☐ Bilgi İşlem Daire Başkanlığı

☐ İdari İşler Daire Başkanlığı

☐ Dijital belgelerin uzun vadeli korunmasından sorumlu bir birim yoktur.

☐ Dijital belgelerin uzun vadeli korunmasından sorumlu bir birimin kurulması planlanmaktadır.

☐ Diğer: _____

29. Kurumunuzda dijital belgeler için uzun vadeli koruma süreçlerini (belgenin gerçekliği, bütünlüğü, güvenliği, erişilebilir ve yeniden kullanılabilir olması) içeren yazılı bir politika (strateji belgesi, plan, program, yönetmelik vb.) var mı? *

- ☐ Evet, yazılı bir politika bulunmaktadır.
☐ Hayır, yazılı bir politika bulunmamaktadır.
☐ Kurumumuzda yazılı bir politika geliştirilmesi planlanmaktadır.
☐ Diğer: _____

30. Lütfen aşağıdaki unsurları kurumunuz kapsamında değerlendiriniz. * (1- Kesinlikle katılmıyorum, 5 - Kesinlikle katılıyorum)

Kurumumuzda dijital belgelerin kurumsal bilgi yönetim uygulamalarındaki tüm süreçleri içeren yazılı bir politikaya ihtiyaç vardır.	[1]	[2]	[3]	[4]	[5]
Kurumumuzda dijital belgelerin kurumsal bilgi yönetim süreçlerinde görev yapan personelin bu konuyla ilgili farkındalık düzeyi yeterli değildir.	[1]	[2]	[3]	[4]	[5]
Kurumumuzda dijital belgelerin kurumsal bilgi yönetim süreçlerinde görev yapan nitelikli personel sayısı kurumunuz açısından yeterli değildir.	[1]	[2]	[3]	[4]	[5]
Dijital belgelerin uzun vadeli korumaya yönelik yazılı bir politikaya ihtiyacı vardır.	[1]	[2]	[3]	[4]	[5]
Kurumunuzda dijital belgelerin üst veri tanımlanması için politikaya ihtiyaç vardır.	[1]	[2]	[3]	[4]	[5]
Kurumumuzun bir belge yönetim politikasına ihtiyacı vardır.	[1]	[2]	[3]	[4]	[5]

Dijital Belgelerin E-Değerlendirme, E-Ayıklama, Hassasiyet Değerlendirmesi Süreçleri

31. Kurumunuzda dijital platformlarda (kurumun e-arşivi dâhil) saklanan belgeler için e-değerlendirme (dijital belgelerin arşivsel değerini belirleme süreci yani bir bağlamda arşive transfer edilip edilmemesi gerektiğinin belirlenmesi) sürecinde aşağıdakilerden hangilerini yapıyorsunuz? *

- ☐ Kurumumuzda e-değerlendirme personel tarafından el ile tek tek kontrol edilerek (geleneksel değerlendirme) yapılmaktadır.
☐ Kurumumuzda e-değerlendirme için belirli programlar kullanılmaktadır.
☐ Kurumumuzda e-değerlendirme hem personel tarafından el ile hem de belirli programlar ile yapılmaktadır.
☐ Kurumumuzda dijital belgeler için e-değerlendirme yapılmamaktadır.
☐ Kurumumuzda dijital belgeler için makro değerlendirme yöntemi kullanılmaktadır.
☐ Kurumumuzda e-değerlendirme için özel bir yazılım oluşturulmuştur.
☐ Bir fikrim yok
☐ Diğer: _____

32. Kurumunuzda dijital platformlarda (kurumun e-arşivi dâhil) saklanan belgeler için e-ayıklama (kalıcı olarak korunması gereken ve arşivsel değere sahip olan belge ve bilgilerin farklı yazılım ve donanımlarla ayıklanması) sürecinde aşağıdakilerden hangilerini yapıyorsunuz? *

- ☐ Kurumumuzda e-ayıklama personel tarafından el ile tek tek kontrol edilerek yapılmaktadır.
- ☐ Kurumumuzda e-ayıklama için belirli programlar kullanılmaktadır.
- ☐ Kurumumuzda e-ayıklama hem personel tarafından el ile hem de belirli programlar ile yapılmaktadır.
- ☐ Kurumumuzda dijital belgeler için e-ayıklama yapılmamaktadır.
- ☐ Kurumumuzda e-ayıklama için özel bir yazılım oluşturulmuştur.
- ☐ Bir fikrim yok
- ☐ Diğer: _____

33. Kurumunuzda dijital belgelerin hassasiyet değerlendirmesi (hangi belgelerin erişime kapatılması gerektiği, hangilerinin erişime açılarak Milli Arşive aktarılması gerektiğinin kararının verilmesi aşaması-örn; nitelikli kişisel veri) yapılırken hangi yöntem kullanılmaktadır? *

- ☐ Hassasiyet değerlendirmesi için oluşturulan özel bir yazılım programı kullanılmaktadır.
- ☐ İşlemler uzman/uzmanlar tarafından tek tek gözden geçirilerek yapılmaktadır.
- ☐ Bu işlem için bir komisyon kurulmuştur ve verilen karara göre süreç ilerlemektedir.
- ☐ Hem bir uzman tarafından hem de özel bir yazılım kullanılarak yapılmaktadır.
- ☐ Kurumumuzda dijital belgelerin hassasiyet değerlendirmesi yapılmamaktadır.
- ☐ Bir fikrim yok
- ☐ Diğer: _____

34. Kurumunuzda dijital belgelerin e-değerlendirme, e-ayıklama, hassasiyet değerlendirmesi yapılırken özel bir yazılım ya da program kullanıyorsanız lütfen diğer kısmına belirtiniz. *

- ☐ Özel bir yazılım ya da program kullanılmamaktadır.
- ☐ Diğer: _____

35. Bir dijital belge sisteme alındığında ya da sistem içinde oluşturulduğunda hassasiyet (nitelikli kişisel veri ya da hizmete özel bilgi v.b) değerlendirmesi için üst veri tanımlaması neye göre oluşturulmaktadır? *

- ☐ Her belge yöneticisi tarafından belgenin konusuna göre anlık oluşturulmaktadır.
- ☐ Kurum tarafından belirlenmiş bir kelime seti içinden seçilerek tanımlanmaktadır.
- ☐ Komisyon tarafından belirlenmektedir.
- ☐ TS 13298 Standardında belirlenen alanlara göre
- ☐ Dublin Core (DC) alanlarına göre
- ☐ Dijital belgelerin hassasiyet değerlendirmesi için üst veri tanımlaması yapılmamaktadır.
- ☐ Bir fikrim yok
- ☐ Diğer: _____

Politika, Eğitim ve Milli Arşive Transfer Süreci

36. Kurumunuz yayımlanmış bir belge yönetim politikasına sahip midir? *

- ☐ Evet
- ☐ Hayır
- ☐ Diğer: _____

37. Kapsamlı bir belge yönetimi politikasında aşağıdaki unsurlardan hangileri yer almalıdır? * (1- Kesinlikle katılmıyorum, 5 - Kesinlikle katılıyorum)

Belge yönetimi politikasının amacı ve kapsamı	[1]	[2]	[3]	[4]	[5]
Roller ve sorumluluklar	[1]	[2]	[3]	[4]	[5]
Arşive uygun materyal türünün belirlenmesi	[1]	[2]	[3]	[4]	[5]
Dosya planı	[1]	[2]	[3]	[4]	[5]
Elektronik belgelere erişim	[1]	[2]	[3]	[4]	[5]
Fiziksel ve dijital belgeler için saklama politikası	[1]	[2]	[3]	[4]	[5]
Ayıklama politikası	[1]	[2]	[3]	[4]	[5]
İmha politikası	[1]	[2]	[3]	[4]	[5]
Dijital belgelerin transferi	[1]	[2]	[3]	[4]	[5]
Üst veri standardına uygunluk	[1]	[2]	[3]	[4]	[5]
Hesap verebilirlik ve şeffaflık	[1]	[2]	[3]	[4]	[5]
Koruma	[1]	[2]	[3]	[4]	[5]
Hassas belgelerin süreçleri	[1]	[2]	[3]	[4]	[5]
Eğitim ve farkındalık	[1]	[2]	[3]	[4]	[5]

38. Kurumunuzda aşağıdaki konulara yönelik eğitimler veriliyor mu? * (1- Evet, 2- Hayır, 3- Bir fikrim yok)

Dijital belgelerin değerlendirilmesi	[1]	[2]	[3]
Dijital belgelerin ayıklanması	[1]	[2]	[3]
Dijital belgelerin hassasiyet değerlendirmesi	[1]	[2]	[3]
Dijital süreklilik	[1]	[2]	[3]
Uzun süreli koruma	[1]	[2]	[3]
Risk yönetimi	[1]	[2]	[3]
Bilgi iletişim teknolojileri	[1]	[2]	[3]
EBYS kullanımı	[1]	[2]	[3]
Bilgi güvenliği	[1]	[2]	[3]

39. Kurumunuzda aşağıdaki konularla ilgili eğitimlere ne derece ihtiyaç vardır? * (1- Hiç ihtiyaç yok, 5 - Çok ihtiyaç var)

Dijital belgelerin değerlendirilmesi	[1]	[2]	[3]	[4]	[5]
Dijital belgelerin ayıklanması	[1]	[2]	[3]	[4]	[5]
Dijital belgelerin hassasiyet değerlendirmesi	[1]	[2]	[3]	[4]	[5]
Dijital süreklilik	[1]	[2]	[3]	[4]	[5]
Uzun süreli koruma	[1]	[2]	[3]	[4]	[5]
Risk yönetimi	[1]	[2]	[3]	[4]	[5]
Bilgi iletişim teknolojileri	[1]	[2]	[3]	[4]	[5]
EBYS kullanımı	[1]	[2]	[3]	[4]	[5]
Bilgi güvenliği	[1]	[2]	[3]	[4]	[5]

40. Kurumunuzda verilen eğitimlerin uygulama aşamasında yeterli olduğunu düşünüyor musunuz? (1-Çok yetersiz, 5-Çok yeterli) *

[1] [2] [3] [4] [5]

41. Dijital belgelerin kurumsal bilgi yönetim süreçlerine yönelik yazılı bir politika sizce kim/kimler tarafından oluşturulmalıdır? *

- ☐ Her kurumun kendisi tarafından,
☐ T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı tarafından hazırlanmış örnek bir metin üzerinden kurumlar kendilerine göre uyarlayarak,
☐ Bilgi Teknolojileri ve İletişim Kurumu
☐ TÜBİTAK
☐ Diğer: _____

42. Kurumunuzda dijital belgelerin kurumsal bilgi yönetim süreçlerinde en çok hangi alanlarda zorlanmaktasınız ya da zorlanacağınızı düşünüyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz) *

- ☐ Dijital belgelerin ayıklanması
☐ Dijital belgelerin değerlendirilmesi
☐ Hassasiyet değerlendirmesi aşaması
☐ Dijital süreklilik aşaması
☐ Dijital belgelerin korunması
☐ Diğer: _____

43. Kurumunuzda dijital belgelerin kurumsal bilgi yönetim süreçlerinden hangi birim sorumludur? *

- ☐ Bilgi İşlem Dairesi Başkanlığı
☐ Strateji Geliştirme Daire Başkanlığı
☐ Kütüphane ve/veya Arşiv Hizmetleri Birimi
☐ İdari ve Mali İşler Daire Başkanlığı
☐ Konu ile ilgili sorumlu bir birim yoktur.
☐ Bir fikrim yok
☐ Diğer: _____

44. Dijital belgelerin Milli Arşive transferi gerçekleşmesinde kurumunuzun teknolojik altyapısının ne derecede yeterli olduğunu düşünüyorsunuz? (1-Çok yetersiz, 5-Çok yeterli) *

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

45. Kurumunuzdaki dijital belgelerinizi Devlet Arşivleri'ne devretme yükümlülüğünüz bulunmakta mıdır? *

☐ Evet ☐ Hayır ☐ Bilmiyorum

46. Kurumunuzdaki hangi materyallerin Devlet Arşivlerine transfer etmekle yükümlü olduğunuzu biliyor musunuz? *

☐ Evet
☐ Hayır
☐ Diğer: _____

47. Dijital belgelerin arşive transferi için Devlet Arşivleri ile bağlantıya geçildi mi? *

☐ Evet
☐ Hayır
☐ Bilmiyorum
☐ Diğer: _____

48. Kurumunuzda, dijital belgelerinizin milli arşive transferi ile ilgili bir çalışma var mıdır? *

☐ Hayır, henüz dijital belgelerin milli arşive transferi ile ilgili bir çalışma yoktur.
☐ Evet, dijital belgelerin milli arşive transferi ile ilgili bir çalışma vardır.
☐ Bilmiyorum
☐ Diğer: _____

49. Dijital belgelerin milli arşive ilk transferini ne zaman gerçekleştirmeyi planlıyorsunuz? *

☐ 2021-2023
☐ 2024-2026
☐ 2027-2029
☐ 2030-2033
☐ Planlanmıyor
☐ Diğer: _____

50. Sizce kurumunuzdaki e-belgelerin Milli Arşive teslim edilip edilmediğinin (veya mevzuat esaslarına uygun olarak sürecin işleyip işlemediğinin) kontrolü hangi kurum tarafından yapılmalıdır? *

☐ T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı
☐ Kamu Kurumlarının İç Denetim Mekanizması
☐ TÜBİTAK
☐ Özel Anlaşmalı Kurumlar
☐ Bilgi Teknolojileri ve İletişim Kurumu
☐ Yazılım şirketleri
☐ Diğer: _____

51. Devlet Arşivleri Başkanlığı ile ilgili aşağıdaki unsurları değerlendiriniz * (1- Kesinlikle katılmıyorum, 5 - Kesinlikle katılıyorum)

Devlet Arşivleri Başkanlığı kurumların elektronik arşivleme süreçleri ile ilgili yeterli düzeyde takip ve denetleme yapmaktadır.	[1]	[2]	[3]	[4]	[5]
Devlet Arşivleri Başkanlığı'nın kurumların milli hafızasını koruyup ileriki kuşaklara aktaracağına inancımız yüksektir.	[1]	[2]	[3]	[4]	[5]
Devlet Arşivleri Başkanlığı görev ve sorumluluklarını yerine getirmektedir.	[1]	[2]	[3]	[4]	[5]
Devlet Arşivleri Başkanlığı gerekli yasal düzenlemeler (arşiv kanunu, politika vb.) konusunda yeterli hizmeti sağlamaktadır.	[1]	[2]	[3]	[4]	[5]

52. Anket hakkında belirtmek istediğiniz görüş ve düşüncelerinizi var ise lütfen aşağıdaki alana yazınız.

Ek 2. Etik Kurul İzni



T.C

MARMARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ARAŞTIRMA ETİK KURULU

Sayı:2020-2...

Tarih: 08.06.2020

PROJENİN ADI: “Dijital Çağda Doğuştan Belgelerin Bilgi Yönetim Süreçleri: Kurumdan Arşive Giden Yol”

PROJE YÜRÜTÜCÜSÜ: Emine Cengiz

PROJEDEKİ ARAŞTIRICILAR:

ONAY TARİHİ VE ONAY SAYISI: 2020-1205

Sayın: Emine Cengiz

2020-5/4. Protokol Nolu

“Dijital Çağda Doğuştan Belgelerin Bilgi Yönetim Süreçleri: Kurumdan Arşive Giden Yol” isimli projeniz Üniversitemiz Sosyal Bilimler Araştırma Etik Kurulu tarafından incelenmiş ve etik yönden uygunluğuna karar verilmiştir.

Prof. Dr. İsmail Taşpınar

Kurul Başkanı

Prof. Dr. Bihterin Dinçkol
ÜYE

Prof. Dr. Kemal Yıldız
ÜYE

Prof. Dr. Nurhan Zeynep Tosun
ÜYE

Prof. Dr. Nafil Ekşi
ÜYE

Prof. Dr. İnci Deniz Ilgın
ÜYE

Prof. Dr. Fatma Ayanoğlu
ÜYE

Prof. Dr. Kemalettin Köroğlu

Prof. Dr. Ahmet Kemal Bayram
ÜYE

Not: 689 sayılı Kişisel Verilerin Korunması Kanunu hükümlerine göre ıslak imzalar maskelenmiştir.

Ek 3. Kavram Haritası

