T.C.

İSTANBUL ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

DOKTORA TEZİ

ELEKTRONİK BELGELERİN VE ELEKTRONİK BELGELERE AİT İŞLEM İZLERİNİN ARŞİV İMHA UYGULAMALARI BAKIMINDAN İNCELENMESİ

Ceyhan GÜLER

2502150532

TEZ DANIŞMANI

Prof. Dr. Mehmet CANATAR

İSTANBUL-2019

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

DOKTORA
TEZ ONAYI

ÖĞRENCİNİN;

Adı ve Soyadı	:	CEYHAN GÜLER	Numarası	:	2502150532
Anabilim Dalı / Anasanat Dalı / Programı	:	BİLGİVE BELGE YÖNETİMİ ANABİLİM DALI	Danışmanı	:	PROF.DR MEHMET CANATAR
Tez Savunma Tarihi	:	23.12.2019	Saati	:	09:00
Tez Başlığı	:	ELEKTRONIK BELGELERİN VE ELEKTRONİK BELGELERE AİT İŞLEM İZLERİNİN ARŞİV İMHA UYGULAMALARI BAKIMINDAN İNCELENMESİ)			

TEZ SAVUNMA SINAVI, İÜ Lisansüstü Eğitim-Öğretim Yönetmeliği'nin **50. Maddesi** uyarınca yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin **KABULÜNE** OYBİRLİĞİ / OY~~ÇOKLUĞUYLA~~ karar verilmiştir.

JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1- PROF.DR MEHMET CANATAR		KABUL
2- PROF.DR A. OĞUZ İÇİMSOY		Kabul
3- -PROF.DR İSHAK KESKİN		Kabul
4--DOÇ.DR BURÇAK ŞENTÜRK		Kabul
5--DR.ÖĞR .ÜYESİ M. FAHRİ FURAT		Kabul

YEDEK JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1- PROF.DR BERAT BİR		
2--DR.ÖĞR. ÜYESİ M. HANEFİ KUTLUOĞLU		

Versiyon: 1.0.0.2-61559050-302.14.06

ÖZ

ELEKTRONİK BELGELERİN VE ELEKTRONİK BELGELERE AİT İŞLEM İZLERİNİN ARŞİV İMHA UYGULAMALARI BAKIMINDAN İNCELENMESİ

CEYHAN GÜLER

Elektronik ortamdaki belgelerin imhası diğer bilgi saklama ortamlarına göre farklı yöntem ve tekniklerin kullanılmasını gerektirir. Elektronik belgelerin yazılım ve donanım izleri bırakmaları ve çok farklı ortamlarda bulunmaları arşiv imha uygulamaları açısından bir problem teşkil etmektedir. Bu nedenle imha edilen elektronik belgelere tekrar erişimin imkânsız hale gelmesini sağlayacak yazılım ve donanım mekanizmaları/araçları arşiv imha teorisinin elektronik ortamdaki belgelere uygulanması açısından büyük önem taşır. Bu mekanizmaların/araçların, elektronik belge ve izlerini sistem ve saklama ortamlarından çıkarması veya yok etmesi beklenmektedir.

Elektronik belgelerin ve bunlara ait izlerin nasıl yok edilmesi gerektiği konusunda ülkemizde tez niteliğinde bir çalışmanın bulunmaması, bu araştırmanın eleştirel literatür taraması, keşifsel bir vaka incelemesi ve tematik analizin bir kombinasyonundan oluşan ve dengeleyici bir nitel araştırma yaklaşımıyla ele alınmasını gerekli kılmıştır. Çalışmada, ABD, Kanada, Avrupa, Avustralya ve Türkiye'deki çalışmalar ve yaklaşımlar değerlendirilmiştir.

Araştırma sonucunda, elektronik belge ve izlerine yönelik farklı devlet veya hükümetlerin imha standartları geliştirdiği, Türkiye'de ise modern arşivcilik için kullanılan imha yöntem ve tekniklerin, elektronik belgeye yönelik hazırlanmış olan resmi standartta da bulunmadığı anlaşılmıştır. Ayrıca, elektronik belgenin ve izlerinin güncel ortam ve güncelliğini yitirmiş (obselete) ortam olarak ikiye ayrılarak imha edilebileceği ve bunların özellikleri bağlamında düşünülmesi gerektiği elde edilen sonuçlardır. Güncel ortamdaki belge ve izlerinin imha edilmesi için çoğunlukla yazılımsal yöntemler kullanılırken, güncelliğini yitirmiş ortam için yazılımsal yöntemler yanında donanımsal yöntemlerin de kullanılabileceği görülmüştür. Yazılımsal yöntemler olarak, tasfiye etme, boşaltma, üzerine yazma, temizleme, manyetiksizleştirme gibi farklı teknikler uygulanmaktadır. Donanımsal yöntemler olarak da erişime kapatma, taşlama

veya fırçalama, çekiçli değirmenle öğütme, parçalama, ufalama, yakma, kesme, eritme gibi teknikler kullanılmaktadır.

Anahtar Kelimeler: Elektronik Belge Yönetim Sistemleri, Arşivsel Değerlendirme, Arşiv İmha Teorisi, Elektronik Belgeler, Elektronik Belge İzleri, İmha Yöntem ve Teknikleri

ABSTRACT

EXAMINATION OF ELECTRONIC RECORDS AND TRACES OF ELECTRONIC RECORDS IN TERMS OF ARCHIVE DESTRUCTION PRACTICES

CEYHAN GÜLER

The destruction of electronic records requires different methods and techniques in comparison with the other data storage environments. Leaving software and hardware traces of electronic documents and being in different environments constitute a problem in terms of archival destruction. Therefore, the software and hardware mechanisms / tools that will make it impossible to re-access the destroyed electronic documents are of great importance for the application of the archival destruction theory to the electronic documents. These mechanisms/tools are expected to remove or destroy electronic records and traces from systems and storage environments.

Since the lack of like a thesis on how to electronic documents and their traces should be destroyed, the study has to be handled with a balancing qualitative research approach that consists of a combination of critical literature review, heuristic case study and thematic analysis. In the study, studies and approaches has been evaluated within the scope of the USA, Canada, Europe, Australia and Turkey.

As a result of research, it has been developed standards by different states or governments for the destruction of electronic documents and their traces. In Turkey, methods and techniques of destruction used for modern archival were not found the official standard that is prepared for the electronic records. In addition, the electronic document and traces of the current and obsolete environment can be destroyed by separating the media and their properties should be considered in the context of the results obtained. While it is mostly used software methods for destroying documents and traces in the current environment, it is seen that hardware methods can be used in addition to software methods for obselete media. As a software methods, different techniques are applied, such as disposal, clearing, overwriting, purge and degaussing. Also, different techniques are used for hardware methods, such as deaccessioning, grinding or scrubbing, hammer-milling, disintegration, shredding, incineration, cutting and smelting.

Keywords: Electronic Records Management Systems, Archival Appraisal, Archival Destruction Theory, Electronic Records, Traces of Electronic Records, Methods and Techniques of Destruction

ÖNSÖZ

Günümüzde bilgi teknolojilerinin sunduğu imkânlar, belgelerin üretilmesi, tanımlanması, düzenlenmesi, kullanılması, korunması ve imha edilmesi gibi işlemlerin elektronik ortamda gerçekleştirilmesini sağlamaktadır. Bu işlemlerin gerçekleştirilmesi, geleneksel uygulamalar gibi elektronik ortamdaki uygulamaların da tam işlevli olarak çalışmasıyla mümkün kılınır. Arşiv imha teorisi, geleneksel anlamdaki ihtiyaçları karşılayabilecek ilke ve uygulamalara sahiptir. Ancak Türkiye'de arşiv uygulamalarının önemli aşamalarından biri olan imhanın elektronik ortamda nasıl yapılacağı ve bunun istenilen şekilde olup olmadığı belirsiz bir konudur. Yine belgelerin ve bu belgelere ait işlem izlerinin elektronik ortamda hangi yöntem ve tekniklerle imha edilebileceği ve bunun geri dönüşü olmayacak şekilde yapılmasına ilişkin herhangi bir çalışmanın olmayışı Türk arşivcilik literatüründe eksikliği hissedilen bir konudur. Bu çalışmanın söz konusu eksikliği doldurması beklenmektedir.

Çalışmada konuya yardımcı kaynakların Türkiye'de henüz olmayışı, başta İngilizce olmak üzere yabancı dillerde hazırlanmış kaynakların ağırlığı ve çevirisi karşılaşılan birinci güçlük olarak ifade edilebilir. İkinci bir güçlük de, Türkiye'de elektronik belge yönetim sistemlerinin (EBYS) yakın geçmişte uygulanmaya başlanması nedeniyle henüz imha süresi gelmiş belgelerin olmayışı ya da bu konu bağlamında henüz zorlayıcı bir durum ile karşılaşılmaması, uygulama noktasında örneklerin eksikliğini hissettirmektedir. Yine Türkiye'de açık kodlu EBYS yazılımlarının olmayışı sistem içinde imha süreçlerinin nasıl olduğunu görmeye imkân vermemektedir. EBYS yazılımlarının, TS 13298[*]'e göre geliştirilmesi, bu standart kriterlerinde elektronik belgelerin imhası ve bu belgelerin işlem izlerine ilişkin açıklayıcı herhangi bir maddenin olmayışı, hazırlanmış olan EBYS'lerde elektronik belgelere ve işlem izlerine dair imha prosedürlerinin nasıl yerine getirilmesi gerektiği sorusunu düşündürmektedir. Türkiye'deki yazılım şirketleriyle görüşülmesine rağmen elektronik belgelerin imhasına ve işlem izlerinin yok edilmesine yönelik net yanıtlar alınamamıştır. Araştırma, tüm

[*] Bu standard, kurumlarda üretilen ve/veya üretilmesi muhtemel elektronik dokümanların belge niteliğinin korunabilmesi için gerekli standartların belirlenmesi konularını kapsamaktadır (Türk Standartları Enstitüsü (TSE): **TS 13298 Elektronik Belge Yönetimi**, 2015, s. 1).

bu güçlüklere rağmen, uluslararası imha standartları ve yazılımları ve bu konuyla ilgili ve ilişkili birçok kaynağın sentezlenmesiyle, hem geleneksel arşivcilik hem de modern arşivcilik uygulamalarına yönelik kaynaklardan alınan bilgilerle tamamlanmaya çalışılmıştır.

Uluslararası düzenlemelerde ve teknik raporlarda söz konusu belgelerin imhası için farklı ülkelerde hazırlanan birçok imha standardı bulunmaktadır. Ayrıca, bu standartlara göre hazırlanmış çeşitli yazılımlar söz konusudur. Bu yazılımlar elektronik belgenin imhasını sağlarken işlem izlerine yönelik imhayı da gerçekleştirmektedir. Konunun daha iyi anlaşılabilmesi için belgeler ve bunlara ilişkin izler güncel ortamdaki belge ve izleri ile güncelliğini yitirmiş (obselete) ortamdaki belge ve izleri olmak üzere ikiye ayrılmıştır.

Güncel ortamdaki belge ve izlerinin imha edilmesi için genellikle yazılımsal yöntemler kullanılırken, güncelliğini yitirmiş ortam için yazılımsal yöntemlerin yanında donanımsal yöntemlerin de kullanılabileceği görülmüştür. Yazılımsal yöntemler olarak, tasfiye etme, boşaltma, üzerine yazma, temizleme, manyetiksizleştirme gibi farklı teknikler uygulanmaktadır. Donanımsal yöntemler olarak da erişime kapatma, taşlama veya fırçalama, çekiçli değirmen, parçalama, ufalama, yakma, kesme, eritme gibi teknikler uygulanmaktadır. İmha yöntem ve teknikleri yanında imhanın adli bilişimle nasıl bir ilişki içinde olduğu da kısmen ifade edilmiştir.

Beş bölümden oluşan çalışmanın giriş kısmında çalışma konusunun önemi, amacı, yöntemi, hipotez ve araştırma soruları, araştırmanın çıktıları ve birincil kaynaklar hakkında bilgi verilmiştir. Tezin birinci bölümünde *Arşivsel Değerlendirme* başlığı altında, arşiv uygulamalarının tümü için temel işlev gören arşivsel değerlendirme ele alınmıştır. Almanya, İngiltere, ABD, Avustralya gibi ülkeler bağlamında değerlendirme yaklaşımlarının tarihi seyri ortaya konmuştur. Çalışmanın ikinci bölümünde dünyada yaygın olan elektronik belge yönetim sistem modelleri *Elektronik Belge Yönetim Sistem Modelleri* başlığı altında incelenmiştir. Bu modellerin üç temel yaklaşım biçiminde olduğu görülmüştür. Bunlar; Avrupa idari modeli, Anglo-Sakson yaşam döngüsü modeli ve Avustralya belge sürekliliği modelidir. Araştırmanın üçüncü bölümünde ise elektronik belgelerin yazılımsal ve donanımsal olarak ne gibi

izler bıraktıkları *Elektronik Belgenin Varlığının Yazılım ve Donanım Yönü ve Bu Yönlere Ait İzler* başlığı altında değerlendirilmiştir. Dördüncü bölümde dünyadaki ve Türkiye'deki elektronik belge ve izlerinin imhasına yönelik düzenlemelerin neler olduğu *Dünyada ve Türkiye'de Elektronik Belge İmha Politikaları, Teorileri ve Uygulamaları* başlığı altında verilmiştir. Beşinci bölümde ise *Elektronik Belgenin (Sanal Nesnenin) İmhasına Yönelik Yöntem ve Teknikler* başlığı altında elektronik belge ve izlerine yönelik imha yöntem ve teknikleri açıklanmıştır. İmha yöntem ve teknikleri açıklanırken bunların iki şekilde incelenmesi uygun görülmüştür. Bunlar; güncel ortam ve güncelliğini yitirmiş ortamdır. Açıklanan yöntem ve teknikler bu iki ortama göre sınıflandırılmıştır.

Türkiye'de elektronik belge ve izlerinin imha edilmesine yönelik herhangi bir çalışmanın olmayışı, hatta dünya örneklerinde de elektronik belge ve izlerini imha etme gibi genel anlamda derleyici bir çalışmanın olmayışı, bu çalışmanın bu konudaki eksikliği giderebileceği ümidini artırmaktadır. Birçok kaynak, rapor, standart, rehber ve diğer kaynakların senteziyle meydana gelen bu tez, arşiv imha teorisini ortaya koymaktadır. Teorik olarak hazırlanan bu çalışmanın arşivsel imha uygulamalarında kaynak olarak kullanılması beklenmektedir.

Bu çalışmanın başlangıç aşamasından mevcut hale gelene kadar desteklerini esirgemeyen danışman Hocam Prof. Dr. Mehmet CANATAR'a şükranlarımı sunmayı borç bilirim. Tez izleme komitesinde yer alan Prof. Dr. Oğuz İCİMSOY'a katkılarından dolayı teşekkür ederim.

Tezin hazırlanıp ortaya konmasında değerli emeklerini esirgemeyen, özverili bir şekilde teze destek veren ve tez konusunun belirlenmesinde önemli katkıları olan ve de bundan sonra da birlikte çalışmalarımızın devamı için desteklerini beklediğim Dr. Öğr. Üyesi M. Fahri FURAT'a ve ayrıca Prof. Dr. İshak KESKİN'e teşekkür ve saygılarımı sunmaktan kıvanç duyarım.

Yine EBYS sistemi kullanmakta olan bazı kurumlarla iletişim kurmama yardımcı olan Dr. Öğr. Üyesi M. Hanefi KUTLUOĞLU'na ve Nizamettin OĞUZ'a, alandaki tecrübe ve bilgisiyle tartışma olanağı bulduğum Sayın Engin TARHAN'a, İstanbul Ticaret Üniversitesi yetkili ve çalışanlarına, İlkay OĞUZ ve Doğukan GÜRAN'a,

kaynak sağlamada yardımcı olan Gökhan USTA, Çiğdem AKYOL, Ekrem ARSLAN, Sümeyye Mine İLTEKİN ve Volkan KURU'ya teşekkür ederim. Ayrıca, İslam Araştırmaları Merkezi (İSAM) Kütüphane yetkili ve çalışanlarına tezin tamamlanmasında sağladıkları imkân ve kolaylıklar için teşekkür ederim.

Son olarak tezin her aşamasında yanımda olan, sabır ve fedakârlık gösteren desteğini her zaman hissettiğim eşim Neslihan ARACI GÜLER'e ve aileme sonsuz teşekkür ederim.

CEYHAN GÜLER

İSTANBUL, 2019

İÇİNDEKİLER

ÜÇÜNCÜ BÖLÜM

ELEKTRONİK BELGENİN VARLIĞININ YAZILIM VE DONANIM YÖNÜ VE BU YÖNLERE AİT İZLER

DÖRDÜNCÜ BÖLÜM

DÜNYADA VE TÜRKİYE'DE ELEKTRONİK BELGE İMHA POLİTİKALARI, TEORİLERİ VE UYGULAMALARI

BEŞİNCİ BÖLÜM

ELEKTRONİK BELGENİN (SANAL NESNENİN) İMHASINA YÖNELİK YÖNTEM VE TEKNİKLER

TABLOLAR LİSTESİ

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR LİSTESİ

a.e.	**:** Aynı eser
a.g.e.	**:** Adı geçen eser
a.g.m.	**:** Adı geçen makale
A.g.y.	**:** Adı geçen yayın
A.Ş.	**:** Anonim şirket
a.y.	**:** Aynı yer
AB	**:** Avrupa Birliği
ABD	**:** Amerika Birleşik Devletleri
AFSSI	**:** United States Air Force System Security Instructions
AIIM	**:** Association for Information and Image Management International
Akt.	**:** Aktaran
AoE	**:** Audio over Ethernet
AR	**:** Army
ARMA	**:** Association of Records Managers and Administrators
ATA	**:** All Advanced Technology Attachment
bkz.	**:** Bakınız
BMP	**:** Bitmap
BSI-VSITR	**:** The German Federal Office for Information Security
BT	**:** Bilgi Teknolojileri
C.	**:** Cilt
CalRIM	**:** California Records & Information Management
CAN/CGSB	**:** Electronic Records as Documentary Evidence
CD-R	**:** Compact Disk-Recordable
CD-ROM	**:** Compact Disk - Read Only Memory
CD-RW	**:** Compact Disc - ReWritable

CESG CPA	**:** The U.K. Government's National Technical Authority for Information Assurance Standard
CGM	**:** Computer Graphics Metafile
CLI	**:** Command Line Interface
CMK	**:** Ceza Muhakemesi Kanunu
CPNI	**:** U.K. Centre for the Protection of National Infrastructure
CPU	**:** Central Processing Unit
CSEC ITSG	**:** Communication Security Establishment Canada Standard
CSU	**:** Channel Service Unit
CSV	**:** Computerized System Validation
Çev.	**:** Çeviren
DAGM	**:** Devlet Arşivleri Genel Müdürlüğü
DAS	**:** Direct Attached Storage
DAT	**:** Digital Audio Tape
DBAN	**:** Darik's Boot And Nuke
DGD	**:** Deutsche Gesellschaft für Datenschutz
DIF	**:** Data Interchange Format
DIRKS	**:** Designing and Implementing Recordkeeping Systems
DLM	**:** Document Lifecycle Management
DNS	**:** Domain Name System
DoD	**:** Department of Defense
DOI	**:** Digital Object Identifier
DOM	**:** Document Object Model
DPI	**:** Dots Per Inch
DRAM	**:** Dynamic Random Access Memory
DSS	**:** Defense Security Service
DSU	**:** Data Service Unit
DVD-R	**:** Digital Versatile Disc-Recordable
DVD-RAM	**:** Digital Versatile Disc-Random Access Memory

DVD-ROM **:** Digital Versatile Disc-Read Only Memory

DVD-RW **:** Digital Versatile Disc-ReadWritable

DXF **:** Drawing Interchange Format

e-BEYAS **:** Elektronik Belge Yönetimi ve Arşiv Sistemi

EBYS **:** Elektronik Belge Yönetim Sistemi

ECC **:** Error-Correction Code

Ed. **:** Editör

EDYS **:** Elektronik Doküman Yönetim Sistemi

EEPROM **:** Electrically Erasable Programmable Read-Only Memory

EPRML **:** Extended Partial-Response Maximum-Likelihood

EPS **:** Encapsulated PostScript

ERMS **:** Electronic Records Management System

ESI **:** Electronically Stored Information

ETSI **:** European Telecommunications Standards Institute

FBI : Federal Bureau of Investigation

FcoE **:** Fiber Channel Over Ethernet

FDD **:** Floppy Disk Drive

FERPA **:** The Family Educational Rights and Privacy Act

FISMA **:** Federal Information Security Management Act of 2002

GIF **:** Graphics Interchange Format

Gnş. **:** Genişleten

GOM **:** Gretech Online Movie

GOST R **:** Russian State Standard

HAVELSAN **:** Hava Elektronik Sanayi

Haz. **:** Hazırlayan

HDD **:** Hard Disk Drive

HD-DVD **:** High Definition Digital Versatile Disc

HHD **:** Hybrid Hard Drive

HMG **:** Her/His Majesty’s Government

HTML : HyperText Markup Language

IaaS : Infrastructure-as-a-Service

ICR : Intelligent Character Recognition

ICA : Internationa Council on Archives

IDE : Integrated Drive Electronics

IE : Internet Explorer

IEEE : Institute of Electrical and Electronics Engineers

IO : Input/Output

IP : Internet Protocol

ISDN : Integrated Services Digital Network

ISM : Information Security Manual

ISO : International Organization for Standardization

JPEG : Joint Photographic Experts Group

JTC : Joint Technology Committee

KEP : Kayıtlı Elektronik Posta

KEPHS : Kayıtlı Elektronik Posta Hizmet Sağlayıcısı

KVKK : Kişisel Verileri Koruma Kurumu

LAC : Library and Archives Canada

LAN : Local Area Network

LTO : Linear Tape-Open

MCRS : MoReq2010 Compliant Records System

MFU : Most Frequently Used

MIT : Massachusetts Institute of Technology

MoReq : Model Requirements for The Management of Electronic Records

MoReq2 : Model Requirements for The Management of Electronic Records

MoReq2010 : Modular Requirements for Records Systems

MP3 : Moving Picture Experts Group Layer-3

MPEG : Moving Picture Experts Group

MRU : Most Recently Used

NAI : National Archives of Iceland

NARA : National Archives and Records Administration

NAS : Network Attached Storage

NASA : National Aeronautics and Space Administration

NAVSO P : Navy Staff Office Publication

NCSC : National Computer Security Center

NFS : Network File Server

NICs : Network Interface Cards

NISP : National Industrial Security Program

NIST : National Institute of Science and Technology

NOS : Network Operating System

NSA : National Security Agency

NZSIT : New Zealand Institute of Science and Technology

OCR : Optical Character Recognition

ODF : Open Document Format

OOXML : Office Open Extensible Markup Language

OS : Operating System

OSB : Organize Sanayi Bölgesi

PaaS : Platform-as-a-Service

PATA : Parallel Advanced Technology Attachment

PC : Personal Computer

PDA : Personal Digital Assistant

PDF : Portable Document Format

PDF/A : Portable Document Format Archive

PNG : Portable Network Graphic

PRML : Partial-Response Maximum-Likelihood

QR : Quick Response

RAID : Redundant Array of Inexpensive Disks

RAM : Random-Access Memory

REDR : Registered Engineers for Disaster Relief

REM : Registered Electronic Mail

ROM : Read-Only Memory

RTF : Rich Text Format

s. : Sayfa

S. : Sayı

SAA : Society of American Archivists

SaaS : Software-as-a-Service

SAN : Storage Area Network

SCSI : Small Computer Standard Interface

SD : Security Deposit

SDP : Standart Dosya Planı

SE : Secure Erase

SEKA : Selüloz ve Kâğıt Sanayii Kurumu

SGML : Standard Generalized Markup Language

SHA : Secure Hash Algorithm

SHP : Shapefiles

SIM : Subscriber Identity Module

SQL : Structured Query Language

ss. : Sayfa Sayısı

SSD : Solid State Drive

SULAIR : Stanford University Libraries and Academic Information Resources

t.y. : Basım tarihi yok

TCP/IP : Transmission Control Protocol / Internet Protocol

TIFF : Tagged Image File Format

TNA : The National Archives

TSE : Türk Standartları Enstitüsü

TÜBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

UDI : Unrestricted Digital Information

UK G-Cloud : United Kingdom Government Cloud

UK : United Kingdom

UNC : The University of North Carolina

URL : Uniform Resource Locator

US : United States

USB : Universal Serial Bus

v. : Version

vb. : ve benzeri

vd. : ve diğerleri

VERBİS : Veri Sorumluları Sicil Bilgi Sistemine

VHS : Video Home System

VPN : Virtual Private Network

W3C : World Wide Web Consortium

WAN : Wide Area Network

WAPSs : Wireless Access Points

WORM : Write Once Read Many

XHTML : eXtensible Hypertext Markup Language

XML : eXtensible Markup Language

y.y. : Basım yeri yok

GİRİŞ

Farklı işlemlerden oluşan arşiv çalışmaları, tarihin ilk arşiv kurumlarının kurulmasından itibaren arşivciler tarafından uygulanmaktadır. Fiziksel herhangi bir ortamda üretilen, düzenlenen, tanımlanan, devredilen, erişilen ve korunan arşiv belgeleri için gerekli mesleki uygulama ilkelerine ilişkin teorik yaklaşımlar zaman içerisinde hem meslektaşlar hem de arşivlerden yararlanan araştırmacılar tarafından geliştirilmiştir. Yüzyılı aşkın bir zamandan beri arşivciler tarafından uygulanmakta olan bu ilkeler günümüz arşivlerinde fiilen yürütülen hizmetler bakımından belirgin bir öneme sahiptir. Ancak kabul görmüş arşiv ilkelerine dayanan bu uygulamalar; arşiv belgelerinin üzerine kaydedildiği bilgi taşıyıcılarının çeşitlenmesiyle birlikte üzerinde yeniden düşünülen uygulamalar haline geldiler. Bu durum, mevcut teorik yaklaşımların söz konusu yeni sorunlar karşısında -kısmen- yeni çözüm yolları ve yeni yaklaşımlar sunmasını da beraberinde getirdi.

Arşivcilik mesleğinin karşı karşıya olduğu güncel ve önemli sorunlardan biri bilgi teknolojileri olarak bilinen yeni teknolojiler tarafından dolaylı olarak üretilen sorunlardır. Farklı türdeki kurumlar ve gerçek kişiler tarafından bilginin üretilmesinde bilgi teknolojilerinin fiilen uygulanmasıyla ve kullanılmasıyla ortaya çıkan bu sorunlar, üretilen bilginin işlenmesiyle ilgili olan her faaliyet (üretim, kontrol altına alma, koruma, düzenleme, tanımlama, değerlendirme, imha, devir ve erişim) aşamasında belirgin problemlerin baş göstermesine yol açtı. Fiziksel ortama ait bilgi taşıyıcıları için üretilen mesleki çözümlerin yeni bilgi taşıyıcıları için de geçerliliği mesleki uzmanlar tarafından çok sayıda tartışmaya ve araştırmaya konu edildi. Böylelikle, sonradan elektronik ortama aktarılan ve doğrudan elektronik ortamda doğan/üretilen (digital born) belgelere yönelik mesleki işlemler tartışmaya açılmış oldu. Bu tartışmalardan birini, elektronik ortamda üretilen belgelerin imhasına ilişkin prosedürlerin değerlendirilmesi oluşturmaktadır.

Belgelerin yaşam döngüsünde önemli bir süreç olan belgelerin değerlendirilmesi ve değerlendirme sonucunda gerekli imha uygulamalarının yapılması, fiziksel olarak üretilen belgeler için kabul görmüş -ve kesin- bazı adımları gerektirmektedir. Bu adımlar önemli bir mesleki yönerge olan saklama planlarıyla belirlenir. Fiziksel

belgelerin imhasında, çeşitli iş ve işlemler sonunda gözle görülür bir sonuca ulaşılabilmekte ve tereddüte izin vermeyen bir işlem gerçekleştirilebilmektedir. Bu formda üretilen belgeler için yürütülen imha işlemi belgelerin kesin şekilde yok edildiğinin garantisidir. Buna karşın, "elektronik belgeler, şekil itibariyle bir forma sahip değildirler. Zamana göre sürekli bir değişiklik içindedirler. Zaman ve mekâna bağlı kalınmaksızın her yerden ulaşılabilirler"[1], yetkilendirme ile veya yetkilendirme olmaksızın yasal olmayan yollarla erişim mümkündür ve belge üzerinde çok yönlü işlem yapılabilmesi söz konusu olabilir. Bu nedenle, elektronik ortamda doğan belgelerin imhası gözle görülemez, somut bir sonuç elde edilmesi güçtür ve birçok karmaşık işlemin takip edilmesi titiz bir çalışma yöntemini gerektirir. Elektronik belgelerin yok edilmesi fiziksel ortamdaki gibi kolay/basit değildir. Fiziksel malzemenin imha edilmesinde -neredeyse tek aşamadan oluşan- bir yöntem uygulanır; buna karşın, elektronik ortamda doğan belgelerin imha işlemleri evrakın üretildiği andan en son imha edileceği ana kadar gerçekleşmiş olan üretim, onay, havale, dosyalama, erişim ve değiştirme aşamalarından oluşmaktadır. Bütün bu işlemlerin elektronik belgeler için dikkate alınmaksızın yönetilmesi imha prosedürünün gerçekleşmesinde hataları beraberinde getirmesi olasıdır. Bu işlemin üretim, onay, havale, erişim, değiştirme ve devir süreçlerinin herhangi birinde özensizlik nedeniyle terk edilmesi, imha edildiği düşünülen belgenin gözden kaçan / ihmal edilen bir izden yakalanıp -muhtemelen eski haliyle- geri getirilmesi ile sonuçlanacağı gözden uzak tutulmamalıdır. Bu sebeple söz konusu elektronik belgelere yönelik imha işleminin ihmali ve hatayı kaldırır bir yanı yoktur.

Elektronik bir belgenin üretimi çeşitli nedenlerden dolayı karmaşıktır. Sanal ortamın kendine has özelliklerinden kaynaklı bu karmaşık yapı, elektronik bir kaydın çeşitli yerlerde (yazılımsal ve donanımsal olarak) bulunabilmesine olanak sağlamaktadır. Özellikle dikkatsizlik nedeniyle oluşturulan elektronik veri izlerinin ve belge

[1] Angelika Menne-Haritz, "Elektronik Kayıtların Değerlendirilmesi, İmhası ve Provenans İlkesi: (Unutmak İçin Değil) Erişim İçin Değerlendirme", **Arşivcilik Metinleri,** Çev. Nurettin Özyakup, Haz. İshak Keskin, İstanbul, Yeditepe, 2008, s. 119.

kopyalarının varlığı, bu varlığın dikkatli bir şekilde belli bir limit ve kontrol mekanizmasına bağlı olmaması, belirgin problemlere yol açmaktadır.[2] Böyle bir durumun olması, elektronik bir belgenin üretiminin, aynı zamanda tek bir belgenin varlığından ibaret olmadığı anlamını taşımaktadır. Her ne kadar gerekli tedbirler alınmış olsa da belge aynı anda birçok kopyasıyla birlikte elektronik ortamda var olabilir. Birçok kopyanın olması, elektronik belgenin oluşum sürecinden sonra onaylanıp havale edilmesinden sonra başlayan yeni süreç ve prosedürler nedeniyle hareket ettiği ortam üzerinde elektronik izler bırakma özelliğinden kaynaklanmaktadır. Bu özellik yazılım programlarının veriyi saklama işlevlerinin olmasından, donanım aracı olan saklama araçlarının ise silinmiş olan verinin tekrar elde edilmesi ihtimalinden dolayı vardır.

Arşivciliğin önemli aşamalarından olan imha uygulamalarının elektronik ortamda da gerçekleştirilmesi, ortamdan kaynaklı problemleri beraberinde getirmektedir. İmha uygulamalarının sadece oluşturulan belgenin varlığına yönelik olması, yukarıda bahsedilen belgenin üretim, onay, havale, dosyalama, erişim, değiştirme ve devir nedenleriyle bıraktığı yazılım ve donanım izlerinin imha edilmemesi veya edilememesi anlamını taşıdığını düşündürmektedir. Geleneksel arşiv imha teorisindeki yaklaşımların, elektronik ortamdaki belgelere uygulanması bu izlerden dolayı mümkün görülmemektedir. "İmha edilmesi gereken bir belgeyi yaşatmak veya yaşaması gereken bir belgeyi imha etmek ciddi problemlere yol açabilir".[3] Bu sebeple elektronik ortamda doğan bir belgenin imhasının gerçekleştirilmesi sadece bizzat belgenin değil aynı zamanda ona ait yazılım izlerinin ve saklama alanlarının yok edilmesine bağlıdır. Bu izlerin belge üretim, onay, havale, dosyalama, erişim, değiştirme ve devir süreçlerinde sistemin bir gereği olarak ve otomatik bir şekilde üretilmiş olabileceği, ancak nerelerde ve sayısının ne olduğunun bilinmemesi, imha edilecek belge izlerinin de tam olarak bilinmemesine neden olmaktadır. Belgenin izlerinin bulunduğu muhtemel yerleri ve imha edilmek istenmesi yanında, nasıl imha edileceğine dair ilkeler de önem

[2] Appraisal and Disposal, (Çevrimiçi) http://www.paradigm.ac.uk/workbook/pdfs/04_appraisal_disposal.pdf, 10 Ekim 2016.

[3] Burçak Şentürk, "Arşivsel Değerlendirme: Arşivciliğin İlk Adımı," **Arşiv Dünyası**, S. 14-15, 2013, s. 38.

arz etmektedir. Nitekim yazılım izerinin yok edilmesi yazılım programlarıyla yapılırken saklama alanlarının sadece yazılımsal değil fiziksel olarak da yok edilmesi gerekebilir.

Türkiye'de üniversitelerde üretilen belgelerin imha edilmesi ile ilgili Henkoğlu'nun yaptığı çalışmanın bulguları, üniversitelerin tamamında fiziksel belgelerin imhasına yönelik çeşitli araçların kullanıldığını, elektronik belgelere yönelik imha uygulamalarının ise göz ardı edildiğini göstermektedir. Ülkemizde, üniversitelerdeki elektronik belgelerin kalıcı olarak silinmesine yönelik hangi tür standarda / standartlara uyulması gerektiği belirlenmemiştir. Aynı şekilde, basit bir sorun olduğu değerlendirilebilecek olan kullanım ömrü dolan sabit disklerin imha sorumluluğunun hangi birimlerce yapılacağı dahi bilinmemektedir.[4] Yine yapılan araştırmaya göre "*üniversite birimlerinde tamamen kullanım dışı kalan bilgi sistemlerinin üzerindeki bilgilerle çöpe atılması, bu sistemler üzerinde işlenmiş olan veriler için silinmiş olsa dahi risk oluşturmaktadır. Bu risklerin tamamen ortadan kalkması, kalıcı silme işlemi ve sonrasında mümkün olması halinde fiziksel imhasının yapılmasıyla sağlanabilmektedir*"[5] şeklinde problem ve çözüm önerisi sunulmaktadır. Üniversitelerde elektronik imha yöntemlerine yönelik politika ve sorumluluk paylaşımının olmadığı, elektronik veri depo alanlarının bilinçsizce çöpe atılmasının kişi hak ve mahremiyeti ile kurumsal gizliliğe zarar vereceği unutulmuş gibidir. Sadece üniversitelerde değil diğer kamu kurum ve kuruluşlarının ve özel şirketlerin nasıl bir imha uygulamasını benimsediği de henüz bilinmemektedir. Bu durumun genelde Türkiye için, özelde ise Türkiye'deki kamu ve özel hukuk tüzel kişilerinin oluşturduğu kurumlar ve gerçek kişiler için ne tür sakıncalar doğabileceğine dikkat çekilmesi bu araştırmayı önemli kılmaktadır.

Fujitsu'nun yaptığı önemli bir araştırmanın sonuçlarına göre, her üç dijital dönüşüm projesinin ikisi risk taşımaktadır. Birleşik Krallık, İspanya, İsveç ve Almanya'da 600'ün üzerinde dijital karar vericinin katıldığı araştırmanın sonucuna göre, dijital dönüşüm hayati öncelikler arasında kabul edilmektedir. Şirketler, dijital başarı-

[4] Türkay Henkoğlu, **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, Ankara, Yetkin Yayınları, 2015, s. 162-165.

[5] **A.y.**

nın önündeki en büyük engelin karmaşa, çatışan öncelikler ve güven eksikliği gibi sebepler olduğunun altını çizmektedirler.[6] Fujitsu'nun araştırmasında öne çıkan bulgular şöyle sıralanabilir:[7]

- Araştırmaya katılanların sadece üçte biri dijital önceliklerin şirketlerine göre belirlendiğini belirtmektedir.
- Her iki yöneticiden biri dijitalleştirmenin BT departmanına bırakılacak bir iş olduğunu düşünmektedir.
- Her üç yöneticiden biri dijital projelere yüksek meblağlar harcamaya hazır olduğunu söylemektedir.
- Araştırmaya katılanların sadece dörtte biri verdikleri tavsiyelerde son derece emin olduğunu ifade etmektedirler.

Büyük şirketlerin dijital dönüşüm projeleriyle ilgili kaygılarının olması, elektronik belgelerle ilgili sistem ve teorilerin ya yaygın bir şekilde bilinmediğini ya da uygulamada ortaya çıkan eksikliği göstermektedir. Bu eksikliğin giderilmesi noktasında elektronik belgelere ilişkin arşiv imha teorilerinin geliştirilmesi ve standart hale getirilmesi, dijital dönüşüm projelerinin hayata geçirilmesinde güven eksikliğini ortadan kaldırabilir. Kurum ve kuruluşların elektronik belge yönetim sistemlerinin kullanılmasını yaygınlaştıracak fiziksel arşiv uygulamalarına muadil sezgisi veren araçların/çözümlerin elektronik ortamda da kullanılması/hayata geçirilmesi arşivcilik mesleği ve uygulamaları açısından gereklidir. Görüldüğü gibi elektronik dönüşüm projelerindeki muhtemel risklerin belirlenmesi çalışmayı bu açıdan da önemli kılmaktadır. Bu çalışmanın temelini oluşturan meselenin elektronik ortamda doğan belgelerin ve bu belgelere ait işlem izlerinin imhasına yönelik olması arşivcilik alanında çok belirgin bir uygulama eksikliğini ortaya koymaktadır. Arşivcilik alanında elektronik imhayı kapsamlı olarak ele alacak temel bir yaklaşımın sergilenmeye çalışılması ve yaklaşımdan sonuçlar elde edilmesi tezin amacını yansıtmaktadır.

[6] Walking The Digital Tightrope, **A Fujitsu Report,** 2016, (Çevrimiçi) http://www.fujitsu.com/global/Images/br-fujitsu-digital-tightrope-report-em-en.pdf, 25 Ekim 2016.

[7] Walking The Digital Tightrope.

Elektronik ortamda üretilen belgelerin imhasıyla ilgili uygulama örneklerine baktığımızda, Yeni Zelanda arşivlerinde, dijital verinin güvenli imhası için yok edilecek belge (üstveri dâhil) üzerine yeniden yazma* yöntemi kullanılmaktadır.[8] Avusturalya'da imha edilmesi gereken bir elektronik kaydın tüm kopyaları, kuruluşun bilgi yedekleme uygulamalarının bir parçası olarak saklanan tüm kopyaları da içerecek ve yeniden erişilmeyecek şekilde silinmelidir şeklinde elektronik imhanın standartlarda yer bulduğu görülmektedir.[9] Amerika Birleşik Devletleri (ABD)'ndeki uygulamalara baktığımızda, Kentucky Eyaletinde elektronik belgelerin imhasına yönelik hazırlanan kılavuzda kabul edilebilir iki yöntemden söz edilmektedir. Bunlar; üzerine yazma ve fiziksel imhadır. Bunun yanı sıra elektronik ortamdaki kayıtların imhasının gelecekteki teknolojilerin kullanımına göre değişebileceği ifade edildikten sonra, yeniden kullanılacak ortam (sabit sürücüler, yeniden yazılabilir diskler vb.) için üzerine yazma işleminin gerçekleştirileceği üzerinde durulur. Çalışır durumda sabit diskler ise tamamen fiziksel olarak tahrip edilmesi ya da sabit disklerin içindeki bilgilerin ayıklanması gerekmektedir. Eğer sabit sürücü çalışamaz durumdaysa veya kullanım ömrünün sonuna gelindiyse fiziksel olarak yok edilmelidir[10] şeklinde açıklanmaktadır.

Fiziksel belgelerin imhası için gerekli yöntemler bilinmektedir. Elektronik ortamdaki ve elektronik ortama aktarılan verinin imhasına yönelik belirlenmiş yöntemler yoktur. Türkiye'de bu konuda yasal bir düzenleme veya kullanılan bir standart bulunmamaktadır. Elektronik belgelerle ilgili uygulanan TS 13298 standardında dahi elektronik belgelerin imhasına ilişkin bir modül veya madde görülmemektedir. Yasal ve prosedür eksikliği yanında elektronik imha yöntemleri noktasında da kurum ve kuruluşlarda uyulacak ilke ve uygulamalar bilinmemektedir. Yasal düzenleme eksikliğine ve uluslararası uygulanan standartlara dikkat çekip, bilgi teknolojilerin getirdiği farklı

---

*Üzerine yazma veri imha yöntemlerinden olup tezin beşinci bölümünde açıklanmıştır.

[8] Archives New Zealand Part of Part of the Department of Internal Affairs, "Methods of Destruction," July 2016/F1, v1.0. (Çevrimiçi) https://records.archives.govt.nz/assets/Guidance-new-standard/16-F1-Methods-of-destruction.docx, 7 Aralık 2017.

[9] Northern Territory Government of Australia, Department of Corporate and Information Services, "Standard 5-Disposal," (Çevrimiçi) http://www.nt.gov.au/dcis/info_tech/records_policy_standards/records_management_standards/standard5_disposal.shtml, 7 Aralık 2017.

[10] Kentucky Department for Libraries and Archives, Public Records Division, "Destruction of Public Records: A Procedural Guide," Version 1.0 – Edition of September 2007, s. 12-15, (Çevrimiçi) https://kdla.ky.gov/records/Documents/Destruction%20Guidelines.pdf, 28 Aralık 2017.

ortama yönelik uygun imha uygulama yöntemlerini belirtmek tezin önemini göstermektedir. Arşivlerin varlığı, arşivsel uygulamaların bilgi teknolojileriyle uyumlu hale getirilmesine bağlıdır. Elektronik ortamdaki belge ve belge süreçlerinde -bir anlamda- doğal olarak oluşan izlerin silinmesine, arşivsel bir çözüm getirilmesi açısından çalışmayı önemli kılmaktadır.

Tezin kapsamı, dijitalleştirme yoluyla elektronik ortama aktarılan dijitalleştirilmiş belgelerin ve doğrudan elektronik ortamda üretilen belgelere ait işlem izlerinin imhasıdır. Bu çerçevede öncelikli olarak belgelerin hangi süreçlerden geçtiği veya iz bıraktığı açıklanacaktır. İkinci olarak; elektronik ortamdaki bilginin imhasına yönelik mevzuat ve standartlara ilişkin yapılan çalışmalar araştırma kapsamında ele alınacaktır.

Elektronik belgelerin ve elektronik belgelere ait işlem izlerinin imhası problemi, bu çalışmada bazı soruların sorulmasıyla ve bu sorulara verilen cevaplarla şekil bulabilecektir. Problemin çözümü için muhtemel sorular şu şekildedir:

- Elektronik bir belge nasıl üretilir?
- Üretilen elektronik bir belge kaç farklı lokasyonda bulunabilir?
- Mevzuat gereği oluşturulan bir belgenin kopyaları dışında, farklı kopyaları var mıdır?
- Sistem gereği üretilen bir belge kaç farklı havale işlemine tabi tutulmaktadır?
- Havale sürecinden sonra belgenin izler bırakabilme olasılığı nedir?
- Elektronik ortamda doğan belgelerin imhası gerekli midir?
- Elektronik ortamdaki belgelerin imhası gerekli görülüyorsa bunun için nasıl bir imha yöntemi takip edilmelidir?
- Elektronik imha uygulamasının kapsamı nasıl olmalıdır?
- Üretilen belgenin aslı temel alınarak yapılan imha yönteminin kapsamı, istenen imha işlemini gerçekleştirmekte yeterli midir?
- Elektronik imha uygulaması nasıl yapılmalıdır?
- Elektronik imha uygulamalarında karşılaşılan riskler nelerdir?
- Günümüzde kullanılan elektronik imha uygulama yazılımları var mıdır?

- Elektronik imha uygulama yazılımı varsa, bu yazılımlarla, imha işlevleri istenildiği gibi yapılabilmekte midir?
- Yeni bir imha yazılımı gerekli midir?
- Yapılan imha uygulamasından sonra, elektronik belge ve izleri başarılı bir şekilde imha edilebilmiş midir?
- İmha edilememişse, elektronik ortamdaki imhadan söz edilebilir mi?
- Elektronik imha prosedürlerinin kapsam ve işleyişi nasıl olmalıdır?
- Elektronik belgelerin imhasında üretim, onay, havale, dosyalama, erişim ve değiştirme prosedürlerinin belirlenmesinin rolü nedir?
- Elektronik belgelere ilişkin işlem adımlarının kesin şekilde başlangıçta tespit edilmesinin yararları nelerdir?
- Elektronik belgelerin kendisiyle ilgili izlerin teknik olarak asıl belge ile ilişkilendirilmesi teknik açıdan mümkün müdür?

Bir belgenin formatı ne olursa olsun, üretilmesinden nihai işlem olan imhasına kadar devam eden belirli bir yaşam döngüsü vardır. Kapsamlı bir belge yönetimi programı, üretimden imhaya kadar elektronik belgelerin yaşam döngüsünü tamamlamasını amaç edinir.[11] Günümüzde teşekküllerini henüz tamamlamaya başlayan elektronik belge yönetim sistemlerinin, belgenin fiziksel ortamdaki yaşam döngüsünü manyetik alanda da sağlaması önemlidir. Nihai işlem olan imha uygulamalarının bütün boyutlarıyla elektronik belge yönetim sistemlerinde yer alıp almadığı, bazı kurum ve kuruluşlar bağlamında da değerlendirilmiştir.

Elektronik belgelere yönelik imha uygulamaları, arşiv imha teorisiyle tam anlamıyla bağdaşmamaktadır. Elektronik ortamdaki belge, farklı yerlerde ve çok fazla sayıda izler bırakabilmektedir. Mevcut elektronik imha uygulamalarının bu izleri kapsamaması, uygulamanın gözden geçirilmesinin gerekliliğini ve elektronik belgelere ilişkin imha uygulamalarının önemini göstermektedir. Arşivsel değerlendirme aracı olarak imha teorisinin, elektronik ortamdaki kayıtların varlığını ve bu varlığa ait izleri de

[11] Joint Technology Committee, "Developing an Electronic Records Preservation and Disposition Plan", Version 1.0, **JTC Resource Bulletin,** 2014, s. 17, (Çevrimiçi) http://www.ncsc.org/~/media/Files/PDF/About%20Us/Committees/JTC/JTC%20Resource%20Bulletins/6JTC%20E%20Records%2010%20FINAL.ashx, 11 Mayıs 2016.

kapsayacak mevcut yaklaşımların, temel bir yaklaşımla geliştirilmesi, söz konusu elektronik belgenin imhasını gerçekleştirebilir.

Günümüzde belgenin daha değerlendirme aşamasında imha sürecine karar verilmesi, bu kararın elektronik ortamda nasıl yapılabileceğini düşündürmektedir. Fiziksel belgelerin imha edilmesinin, somut ve gözle görülebilir nitelikte olması, belge imhasının gerçekleştirilip gerçekleştirilmediğini kuşkuya yer bırakmayacak şekilde göstermektedir. Elektronik ortamdaki belgelerde bu durum söz konusu değildir. Elektronik ortamdaki bir belge imha edilmiş gibi olsa bile, bu belgenin elektronik bir iz veya izler bırakabilmesinin söz konusu olması, belgenin kesin şekilde imhasını zorlaştırmakta hatta kuşkulu hale getirmektedir. Çünkü istenildiğinde belge izlerinden belgeye tekrar erişim sağlanabilmesi, -geleceğe yönelik güçlü bir öngörüde bulunmak bir yana- mevcut teknolojik imkânlar bakımından bile imkânsız değildir.

Adli bilişimin, silinmiş olduğu varsayılan verinin kurtarılmasındaki başarısı, elektronik ortamdaki verinin güvenli bir şekilde imha uygulamalarına ilişkin yeterince araştırma yapılmadığını göstermektedir. Arşivci, istenmeyen daha doğrusu her bakımdan yarar sağlamayacağı belirlenen belgelerin imha edilmesinden sorumludur ve var olan yasal düzenlemeler ve kurumsal politikalar kapsamında saklama planlarına göre belgeleri imha etmelidir.[12] Bu nedenle elektronik bir belgenin tamamen imha edilmesi, belgeye ait izlerin de yok edilmesine bağlıdır. "Tam bir imha için, imha edilecek dosya kopyalarının durumunun (kasıtlı, geçici, silinmiş ve yedek alınmış olanlar dâhil) bilinmesi ve verinin eksiksiz bir şekilde silinmesinin nasıl olacağı iyi anlaşılmalıdır".[13] Bu açıdan "Bir belgenin tamamen imhası nasıl yapılabilir?" sorusunun cevabı bu çalışmanın gerekçesini oluşturmaktadır. Arşivcilere ve belge yöneticilerine, elektronik ortamdaki verinin güvenli bir şekilde imha edilmesi konusunda yardımcı olacak böyle bir araştırmanın alanında özgün olacağı düşünülmektedir.

Elektronik imha teorisinin uygulanmasının arşivcilik ilke ve prensiplerine göre standart hale getirilmesi gerekmektedir. Bu teorinin bilimsel bir nitelik kazanması ve uygulanması arşivcilik alanında yapılan yurt içi ve yurt dışı kaynakların ve uygulama

[12] Appraisal and Disposal, s. 34.
[13] **A.e.**

örneklerinin imha teorisine yaklaşımının bilinmesini zorunlu hale getirmektedir. Elektronik ortamda doğan belgelerin imhası konusunun teorik çerçevesini çizmek bu kaynakların incelenmesini ve yorumlanmasını gerekli kılmaktadır. Hilary Jenkinson ve T. R. Schellenberg'in, arşivsel kayıtların değerlendirmesiyle ilgili kabul görmüş etkin fikirleri, arşiv uygulamaları için önemlidir.[14] Özellikle belgenin kim tarafından imha edilmesi gerektiği ve bunun elektronik ortamla beraber ne şekilde değiştiği söz konusu kişilerin fikirleriyle tartışma imkânı bulmuştur. Schellenberg'in arşivcinin ve belge yönetişinin belgeleri beraber değerlendirmesini öne sürmesi, Jenkinson'ın belgelerin kanıtsal değerinin arşivci ve belge yöneticinin iş birliği ile olmasını düşünmesi önemlidir.[15] Bu nedenle Jenkinson ve Schellenberg'in fikirleri arşivsel değerlendirme kısmında sentez kaynaklarla birlikte aktarılmıştır. Tezin birinci bölümünde özellikle Jane Turner'ın, "*A Study of the Theory of Appraisal For Selection"* adlı değerlendirme teorisi üzerine 1992 yılında yazılan tezinden, Ole Kolsrud'un 1992 yılında ele almış olduğu *"The Evolution of Basic Appraisal Principles - Some Comparative Observations"* adlı değerlendirmeye ilişkin makalesinden ve Luciana Duranti'nin *"The Concept of Appraisal and Archival Theory"* adlı 1994 yılında hazırlamış olduğu makalesinden ve diğer sentez çalışmalardan yararlanılmıştır. Tezin ikinci bölümde, MoReq, MoReq2, MoReq2010 dokümanlarından, ISO 15489 nolu standardından, ICA'nın sistem gereklilikleri dokümanlarından, Jay Atherton'ın, *"From Life Cycle to Continuum: Some Thoughts on the Records Management - Archives Relationship"*, adlı çalışması, Frank Upward'ın *"Structuring the Records Continuum - Part One: Postcustodial Principles and Properties"* adlı 1996 yılında yayımlanmış olduğu makale ve 1997 yılında önceki çalışmanın ikinci adımı olan makaleden yoğun şekilde yararlanılmıştır. Üçüncü bölümde dünyadaki ulusal arşivlerin, üniversitelerin ve konuya ilişkin ürün geliştiren özel sektör temsilcilerinin perspektifinden belgelerin yazılım ve donanım izleri tartışılmıştır. Bu bölümde özellikle ifade edilmesi gereken ABD Ulusal Teknoloji ve Standartlar Enstitüsü (NIST) ve Yeni Zelanda Bilgi ve İletişim Teknolojileri

[14] Richard Stapleton, "Jenkinson ve Schellenberg: Bir Karşılaştırma", M. Fahri Furat (Çev.), **Arşiv Dünyası**, S.14-15, 2013, s. 45.

[15] Reto Tschan, "Jenkinson ve Schellenberg'in Değerlendirmeye Dair Görüşlerinin Karşılaştırılması," **Prof. Dr. Şevki Nezihi Aykut Armağanı** (ss. 355-372**)**, Erkan Keser (Çev.), Gülden Sarıyıldız, Niyazi Çiçek, İshak Keskin, Sevil Pamuk (Haz.), İstanbul, Etkin Kitaplar, 2011. s. 371.

(NZSIT) önemli iki kurum olarak söylenebilir. Tezin dördüncü bölümünde yararlanılan kaynaklar ise ABD ordusu, hava kuvvetleri, donanma ve diğer ulusal teknolojik kurumlarının hazırlamış olduğu veri imha standartlarından, Almanya, Avustralya, İngiltere, Kanada, Rusya ve Yeni Zelanda devlet veya hükümet dokümanlarından yararlanılmıştır. Türkiye'de ise TS 13298 nolu standarttan, Kişisel Verileri Koruma Kurumunun hazırlamış olduğu düzenlemeler ve rehberlerden yararlanılmıştır. Tezin son bölümünde ise çok çeşitli kaynaklardan yararlanılmıştır. Bunlardan bazıları şunlardır: NIST 800-88 Ortam Temizleme Rehberi, Birleşik Krallık Ulusal Altyapı Koruma Merkezi CPNI Hassas Verilerin Güvenli Silinmesi Standardı, Tazmanya Arşiv ve Miras Ofisi, Otago Üniversitesi, Kentucky Arşiv ve Kütüphane Departmanı Kamu Belgelerinin İmha Etme Rehberi, Florida, North Carolina eyalet arşiv uygulamaları rehberleri, Craig Wright, Dave Kleiman ve Shyaam Sundhar R.S.'ın *"Overwriting Hard Drive Data: The Great Wiping Controversy"* adlı çalışmaları, Gordon F. Hughes, Daniel M.Commins ve Tom Coughlin'nın *"Disposal of Disk and Tape Data by Secure Sanitization"* adlı çalışmaları. Bunlar haricinde ulusal ve uluslararası arşiv kurumlarının elektronik belgelerin imhasına yönelik uyguladığı imha yöntemleri ve elektronik belgelerin imhasını vurgulayan standartlar ve politikalar da çeşitli ülke ve kurumlar bağlamında değerlendirilmiştir.

Elektronik ortamdaki bilgi silinebilir ve tekrar kullanılabilir, fakat en üst düzey güvenlik için, elektronik belgelerin tekrar kullanılmasına olasılık vermeden iz bırakmış olduğu ortamdaki her yerden silinmesi gerekmektedir. Elektronik belgelerin imhası, çok zor olabilir. Çünkü kurumun, sistem yöneticisi tarafından bile erişilemeyen ve birçok lokasyonda bulunan dosya örnekleri olabilir. Bu itibarla, elektronik belge ve dosyalarının silinmesi için belli prosedürlerin olması önemlidir. Bazı kurumların, sunucularındaki belgeler için, periyodik silme işlemlerini devreye sokması tedbir amaçlı atılacak adımlar olarak görülebilir. Bahsedilen periyodik, bir hafta veya daha az bir zaman dilimi için dahi düşünülebilir.[16] Belgelerin manyetik ortamda bulunma süresi

[16] Geof Huth, "Retention and Disposition of Records: How Long to Keep Records and How to Destroy Them", **Archives Technical Information Series,** 41, 2002, s. 18, (Çevrimiçi) www.archives.nysed.gov/common/archives/files/mr_pub41.pdf, 5 Mayıs 2016.

dahi, belgenin bilinmeyen yerlerde kopyalarının oluşmasına neden olabilir. Belge üretim aşamasında, elektronik belge imha uygulama araçlarını devreye sokmak ve bunu zorunlu kılacak prosedürlerin geliştirilmesi, teorik bir çerçevenin oluşturulmasında yararlı olacaktır.

Arşiv malzemesinin fiziksel ortamdan elektronik ortama doğru bir seyir izlemesi, elektronik ortama yönelik arşiv uygulamalarının metodolojisinin anlaşılmasını gerektirmektedir. Metodolojinin bilinmesi, arşivcilik tarihinde, fiziksel arşiv teorilerinin nasıl oluşturulduğunun ve günümüze kadar hangi evrelerden geçtiğinin bilinmesi, günümüz elektronik ortamdaki belgelerin nasıl bir yaklaşımla ele alınması gerektiğini göstermek açısından önemlidir. Özellikle belgelerin değerlendirilmesine ilişkin teorilerin nasıl ortaya atıldığı ve bu teorilerin ne kadar başarılı olduğunu bilmek, her ne kadar belgenin bulunduğu ortam farklılık arz etse de, yaklaşımların belirlenmesinde takip edilmesi gereken adımlardır.

Arşivcilik tarihinde, imha teorisinin gelişimine bakıldığında, 1930'lu yıllara kadar belgelerin imha edilmesinin arşivcilik yaklaşımıyla yapılmadığı görülmektedir. Söz konusu tarihten önce yapılan ayıklama ve imha uygulamaları, belgelerin önemli veya önemsiz olmalarına göre ya saklanılmış ya da tamamen yok edilmiştir. Lağvedilen kurumlara ait belgelerin imha edilmesi bu durumu açıkça göstermektedir. Bu dönem içinde kurumsal olarak ihtiyaç duyulan belgelerin korunduğu, ihtiyaç duyulmayan belgelerin de imha edildiği veya korunmasına özen gösterilmediği görülmektedir.[17]

1930'lu yıllardan başlamak üzere 1960'lı yıllara kadar, siyasal, hukuksal, ekonomik ve toplumsal açıdan önemli sayılan bilgi kaynaklarının araştırma ihtiyacı için kullanıldığı bilinmektedir. Toplum/devlet hayatında önemli olaylara, etkin öznelere ve araçlara ilişkin kayıtların korunması eğilimi bu dönemin temel karakterine işaret etmektedir. Bilgi kaynaklarının araştırma ihtiyacı için kullanılmaya başlanması, önemli evrakların tutulması yanında araştırma için korunan evrakın da tutulduğunu göstermektedir. "Özellikle 1950'lere doğru teknik gelişmelerin etkisiyle, belge sayılarındaki

[17] 10 Nisan 2016 tarihinde Dr. İshak Keskin ile yapılan görüşme.

artış, arşivcilerin imha teorisini benimsemelerine neden olmuştur".[18] Bunun sonucunda saklama planlarının önemi ortaya çıkmış ve evrakların saklanıp korunmasına ilişkin planlar geliştirilmiştir.

Belgelerin gün geçtikçe önemliler yanında önemsiz sayılan belgelerin arasından bazı örneklerin ayıklanarak korunması durumu, 1960-1970 yılları arasında gelişmiş bir evrim olarak karşımıza çıkmaktadır. Bunun nedeni söz konusu İkinci Dünya Savaşı'ndan sonra önemsenmeye başlanan kültür tarihinin baskısıdır. Yeni bir araştırma sahası olan kültür tarihi / sosyal tarih / yerel tarih çalışmaları toplum / devlet hayatı bakımından etkin olamayanlarla da ilgilenmektedir ve bilim dalına ilişkin temel ilgi yeni kaynakların kullanımına ihtiyaç duyulmasına yol açmıştır. Geleneksel imha teorisine göre imha edilmesi gereken belgeler arasından örneklemenin yapılması eğilimi böylelikle ortaya çıkmıştır. Üretilen her belgenin kurum imkânları ve araştırma sürecinin hızlandırılması nedeniyle korunmaması, belgelerin bir kısmının ilkesel olarak imha edilmesi bir kısmının da sürekli olarak korunması uygulaması devam ettirilmiştir.[19] Bu süreçler belgelerin değerlendirilmesini iki temel yaklaşım üzerinden şekillendiğini göstermektedir. Bu yaklaşımlardan biri belgenin ispatlayıcı vasfının olmasıdır. İkinci yaklaşım ise belgelerin araştırma hizmetlerinde yardımcı olacak nitelikte olmasıdır. Bu iki nitelik belgelerin fiziksel ortamda saklanılmasını zorlaştırmış, ayrıca arşiv kurumlarını araştırma hizmetlerini yerine getiremez duruma sokmuştur. Bu nedenle arşivciler, belgelerin söz konusu hizmetlerde aksaklıkları ortadan kaldırmak için yeni yöntem ve beceriler araştırmışlardır. Arşivlerdeki imha uygulamalarını bir gereklilik olarak benimsemeleri ve bu işlemin uygulanması, belgelerin depolanması ve araştırma sürecinde karşılaşılan problemlerin azalmasına ve arşivlik malzemenin istenildiği şekilde korunmasına yardımcı olmuştur.

Bilgi teknolojilerinin arşivcilik alanında yaygın olarak kullanılması, günümüzde elektronik belge yönetim sistemlerinin kurumlarda hızla işlerlik kazanması, elektronik ortamda arşivlemeyi gündeme getirmiştir. Elektronik belgelerin saklanması

[18] İshak Keskin, "Osmanlı Bürokrasisinde Evrak İmha Uygulamalarına Dair Gözlemler," **Türk Devlet Yönetimi Geleneği**, Ed. Cengiz Buyar, Mehmet Kıldıroğlu, Murat Kocobekov, Bişkek, 2016, s. 315.

[19] İshak Keskin, "Arşivcinin Efemerası," (Yayına hazır makale).

metodolojisi, fiziksel ortamdaki belgelerin saklanma metodolojisiyle temelde benzerlikler göstermektedir. Arşivci veya belge yöneticisi, öncelikle, elektronik ortamdaki bilginin varlığını tanımlamalıdır. Gruplara göre saklama planları ve bu saklama planlarına uygun talimatları uygulamalıdır. Daha sonra, saklama planlarının imhayı da içerecek şekilde pratikte uygulanmasını sağlamakla sorumludur. Bu işlemler, elektronik belgenin saklanma planlarının özünü oluşturur.[20] Görüldüğü gibi, elektronik belgelerin saklanma planları, fiziksel ortamdaki belgelerin saklanma planlarıyla benzerlik taşımaktadır. Bu da bize göstermektedir ki, aynı metodoloji kullanılabilir olmakla beraber asıl farklılığın imha uygulama yöntem ve becerisinde olduğudur. İşte bu çalışmanın özünü oluşturan elektronik belgeler ve bu belgelere ait işlem izlerinin imhası konusu, geleneksel arşivsel yaklaşımların yanında, elektronik ortamda doğan belgelere yönelik yeni prensiplerin de ortaya çıkışını tetiklemiştir. Geçmişten günümüze belgelerin değerlendirilmesi sorununda, imha uygulamalarının önemi açıktır. Elektronik ortamdaki belgelerin fiziksel belgeler gibi ispat edici vasfı ve araştırma niteliğinde başvurulan kaynaklar olması için çeşitli bilgi teknolojileri araçları kullanılmaktadır.

Donanım ve yazılım eskimesinden dolayı, elektronik ortamdaki belgelerin belirli zamanlarda taşınması, belgelerin korunmasında maliyeti artırabilmektedir.[21] Arşivcilik metodolojisi açısından imha edilmesi gereken bir belgenin imha edilememesi bu gibi çeşitli sorunlara da neden olabilir. Fiziksel belgelerdeki imha yöntemlerinin elektronik ortamdaki belgeler için kullanılamaması, arşiv imha teorilerinin yerine getirilememesi sorununu ortaya çıkarmaktadır. Çünkü elektronik ortamdaki belge, farklı birçok alanda izler bırakabilmektedir. Bu izlerin belirlenmesi ve imha teorisinin bu izleri de kapsaması arşivcilik imha metodolojisi ve teorisi açısından önemlidir.

Betimsel yöntemle ortaya konulacak çalışmanın verilerinin değerlendirilmesi yanı sıra konuya ilişkin ulusal ve uluslararası sentez eserlerin de içerik analizi yöntemiyle incelenmesi çalışmaya nitelik kazandıracaktır. Bu alanda doğrudan mevcut tez

[20] David O. Stephens and Roderick C. Wallace, "Electronic Records Retention: Fourteen Basic Principles". **Information Management,** 34, 4, 2000, ARMA International, s. 41, (Çevrimiçi) http://www.umiacs.umd.edu/~oard/teaching/708x/spring12/readings/stephens.pdf, 14 Mayıs 2017.

[21] Joint Technology Committee, s. 17.

niteliğinde hiçbir çalışma olmadığından, bu araştırma eleştirel literatür taraması, keşifsel bir vaka incelemesi ve tematik analizin bir kombinasyonundan oluşan dengeleyici bir nitel araştırma yaklaşımıyla ele alınmıştır.

Tezden beklenen sonuçlar aşağıda sıralanmıştır:

- Arşivsel değerlendirmenin farklı ülkeler bağlamında tarihi seyri ve imhanın ihtiyaçlara göre nasıl şekillendiği görülmüş olacaktır.
- Günümüzde uluslararası kabul edilebilir elektronik belge yönetim sistemlerinin hangi yaklaşımlarla ele alındığı ve elektronik belge yönetim modellerinin nasıl geliştirildiği bilinmiş olacaktır. Ayrıca bu modellerde elektronik belgeye yönelik imhanın nasıl olduğu da anlaşılmış olacaktır.
- Elektronik belgenin yazılımsal ve donanımsal olarak izlerinin ne şekilde ve hangi ortamlarda olduğu ortaya konulacaktır.
- Dünyada ve Türkiye'de elektronik belgenin imhasına yönelik standartlar, yasal ve kurumsal düzenlemelerin neler olduğu bilinmiş olacaktır. Ayrıca imhaya yönelik standartlar bağlamında geliştirilen elektronik belge imha yazılımları ve özellikleri bilinmiş olacaktır.
- Çalışmanın sonunda, elektronik bir belgenin üretimi, sonrasında arşivlik malzeme olması sürecinde ne gibi izler bıraktığı bilinecektir.
- Güncel ortamdaki belgelerin imhası için başvurulan yöntem ve tekniklerin neler olduğu açıklanmış olacaktır.
- Güncelliğini yitirmiş ortamdaki belgelerin imhası için kullanılan yöntem ve tekniklerin neler olduğuna dikkat çekilecektir.
- Yazılımsal ve donanımsal olarak imha edilmiş bir belgenin istenilen imha işlemin gerçekleştirilip gerçekleşmediği ortaya konmuş olacaktır.
- Elektronik ortamdaki belgelerin imhasında fiziksel imhanın önemi ortaya konulacaktır.
- Özellikle donanımın imha edilmesinin geri dönüşüm ve ileriye yönelik eski bilgi kaynaklarının sunumundaki etkisi tartışılmış olacaktır.

Kamu kurum ve kuruluşlarında imha algısının imha sürecindeki etkisine değinilmiş olunacaktır.

BİRİNCİ BÖLÜM
ARŞİVSEL DEĞERLENDİRME

1.1. ARŞİVSEL DEĞERLENDİRMENİN (ARCHIVAL APPRAISAL) TANIMI

Değerlendirme, Amerika Arşivciler Derneğinin sözlüğünde[1], (1) arşivlenecek materyallerin tespit edilmesi için yeterli değeri olan materyallerin belirlenmesi süreci ve (2) saklanacak belgelerin yasal gereklilikler kapsamında mevcut ve potansiyel kullanışlılığa dayalı belgelerin saklanması olarak ifade edilmektedir. Aynı kaynakta, kavramın arşivsel bağlamda anlamının şu şekilde ifade edilebileceği de belirtilmektedir: Değerlendirme, belgelerin ve diğer materyallerin kalıcı (arşivsel) değere sahip olup olmadığını belirleme sürecidir. Değerlendirme kararlarının temelinde, birçok neden olabilir. Bunlar; belgelerin provenans, içerik, özgünlük, güvenirlik, düzen, bütünlük, durum ve durumun korunma maliyetleri ve gerçek değer gibi nedenlerdir. Değerlendirme, genellikle daha büyük bir kurumsal toplama politikası ve misyon beyanı içinde gerçekleşmektedir.[2] Yine İskoçya değerlendirme politikasında değerlendirme, belge ihtiyacını tanımlayan bir süreç olarak ifade edildikten sonra tüm personelin belirtilen arşivsel iş ve işlemlere mevzuat, standartlar ve hesap verebilirlik şartlarına uymak zorunda oldukları bildirilmektedir. Bunlar; belge üretimi, saklama, bakım, belgelerin imhası veya transferidir.[3] Bir diğer önemli tanım da Carol Couture tarafından yapılmıştır. Couture'a göre, değerlendirme; "belirli bir kurum (veya kişi) ile onların faaliyetleri sırasında oluşturdukları belgeler arasındaki temel bağlantıya saygılı bir bağlamda belgelerin birincil ve ikincil değerlerini yargılama ve bu değeri korudukları zamanın uzunluğunu belirleme eylemidir".[4]

---

[1] Richard Pearce-Moses, **A Glossary of Archival and Records Terminology**, Chicago, The Society of American Archivists (SAA), 2005, s. 22.

[2] **a.e.**

[3] Irene E O'Brien, **Appraisal and Disposal Policy**, Preserving the Archival and Historic Memory of Glasgow, 2011, v.5, s. 2, (Çevrimiçi) https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/element7-GCA.pdf, 11 Mayıs 2016.

[4] Carol Couture, "Archival Appraisal: A Status Report," **Archivaria**, Spring 2005, C. 59, s. 84.

Değerlendirmenin, önyargı ve öznellikten arınmış olması düşünülemez ve her zaman dönemin kültürünü ve değerlerini ve kararı veren arşivcinin eğilimlerini yansıtmaktadır. Yazının kullanıldığı malzeme, modern çağ öncesi çok büyük miktarlarda değildi. Bu sebeple var olan malzemenin değeri yüksekti ve arşivciler, bu malzemenin daha büyük bir oranını korumaya yönelik bir eğilim göstermekteydi. 19. yüzyılın sonu ve 20. yüzyıl (Modern Arşivler Çağı), belge evreni için, hem basılı hem de arşiv materyallerinin geniş çaplı çoğalmasıyla dramatik bir şekilde değişti. Modern arşivler, önceki dönem malzemesine uygulanmayan bir seçim ve imha yaklaşımlarının uygulanmasını günümüz için gerekli kılmıştır. Amerikalı arşiv teorisyeni T. R. Schellenberg, geniş kapsamlı değerlendirme tekniklerine ve gereksiz kayıtların imhasına olan ihtiyacı belirleyen ilk arşivci olarak bilinmektedir. Schellenberg, uzun yıllar Ulusal Arşivler ve Kayıtlar İdaresi'nde (NARA) çalışmış ve teorileri kamu kurumlarına ait belgelere dayanıyordu. Kamu belgelerinin oranı, küçük bir yüzdeyi kalıcı bir değerle seçme ve geri kalanını yok etme amaçlı bilimsel bir yöntemin gerekli olduğu kanısını güçlendirmekteydi. Schellenberg'in değerlendirme nitelikleri birincil (belge üreticisinin - idari, yasal ve mali) değeri ve ikincil (tarihsel değer - kanıtsal ve bilgilendirici) olarak sınıflandırılması, devlet arşivlerinde olduğu gibi kişisel arşivler için de geçerlidir.[5]Schellenberg'in arşivsel değerlendirmeye ilişkin ilkeleri ele aldığı çalışmada üç temel prensip belirlenmiştir. Bunlar; kamusal olsun, özel olsun belgelerin kronolojik bir tarih sınırının oluşturulması, özel belgelerin zamana bakılmaksızın arşivsel bir kuruluşa ulaştırılır ulaştırılmaz saklanması gerektiği ve kamusal belgelerin kişiler, nesneler ve fenomenler hakkında içerdikleri bilgilerle orantılı olarak değerlendirilmesidir.[6] Bu ilkelerin elektronik ortamdaki belgeler için de uygun kriterler olduğu düşünülmektedir.

[5] Appraisal and Disposal, s. 32, (Çevrimiçi) http://www.paradigm.ac.uk/workbook/pdfs/04_appraisal_disposal.pdf, 10 Mayıs 2017.

[6] Theodore R. Schellenberg, "Arşivsel Değerlendirme İlkeleri," **Arşivcilik Metinleri** (ss. 55-70), İlhan Bozan (Çev.), İshak Keskin (Haz.), İstanbul, Yeditepe, 2008, s. 58-67.

Arşivlerin oluşturulması, hangi belgelerin tutulacağı, düzenleneceği, tanımlanacağı, erişilebilir olacağı ve korunacağı, değerlendirme aşamasında alınan kararlarla şekillenmektedir.[7] Değerlendirme iki amaçla yapılmaktadır. Bunlar, imha etmek için değerlendirme ve koruma için değerlendirmedir. İmha etmek için değerlendirme, Birleşik Krallık anlayışıyla yapılan değerlendirmedir. Koruma için değerlendirme ise Almanya anlayışıyla yapılan değerlendirmedir. Her iki yaklaşım birbirine tamamen zıttır. Değerlendirmeyi imha için yapanlar, idari, mali ve kısa vadeli amaçlar (yer kazanma) için yaparlar. Koruma için değerlendirme yapanlar ise, arşivlerin kültürel miras ve uzun vadede kanıtlayıcı değeri için yaparlar.[8] Bu yaklaşım ve amaçlar geleneksel belge üretimi sonucunda elde edilen belgelere uygulanan veya benimsenen tavırlardır. Her iki yaklaşımın vardığı sonuçlar arasında ise herhangi bir fark yoktur. Günümüzde geleneksel belge üretimi yanında artık dijital ortam, dijital evren, dijital belge gibi kavramlarla da muhatap kalınmaktadır. Gelişen ve değişen dünya şartları her alana yenilik getirdiği gibi arşiv uygulamaları açısından önemli bir takım yenilikleri de sağlamıştır. Bu yeniliklerin tartışılması, arşivcilik için anlam ve değerinin bilinmesi, geleneksel değerlendirme anlayışının geliştirilmesi noktasında önemlidir.

Dijital evrenin genişliği, geleneksel belge üretimini yok etme eğilimini sergilemektedir. Arşivciler genellikle daha fazla belge tutarlar; çünkü üretim, depolama ve yeni teknolojiler, materyali değerlendirme ve imha konularında hala büyük ölçüde sıkıcı bir faaliyet olarak görülen manuel uygulamalara başvurmaktadırlar. Geniş ve sonsuz gibi görünen dijital evrenin etkin bir şekilde yönetilmesi, arşivci ve araştırmacının değerlendirme konusunda daha fazlasını yapması anlamını taşımaktadır. Değerlendirme, diğer tüm işlevlerin bağımlı olduğu ve bu nedenle dikkatli bir düşünmeyi gerektiren temel bir arşiv işlevidir. Arşivleme konularının yanı sıra, depolama, kataloglama ve uzun vadeli koruma gibi ikincil faktörler de değerlendirmeyle düşünülmesi gereken sonraki adımlardır.[9] Değerlendirmenin tarihsel nedenlerine vurgu yaparken, zamanın gereklerine ne şekilde uyum sağladığını ve ne gibi yaklaşımlarla günümüze

[7] **A.e.**, s. 84.
[8] **A.e.**, s. 85-86.
[9] **a.y.**

ulaştığını görmek tezin ana yapısı için hem anlamlı hem de değerlidir. Değerlendirmeyi değerli kılan bir diğer faktör de günümüzdeki bilgi ve belge üretiminin muazzam büyüklüğüdür. Geçmişteki değerlendirmeyi günümüzün dijital evreninde uygulamak, bunu yaparken bilgi ve belge ortamının şartlarını tartışmak, konuya ilişkin yaklaşımlar sergileyen kuramcıları ve bulundukları ülke şartlarını göz önünde bulundurmak Türkiye için tavsiye edilebilecek bir yaklaşım göstermek açısından yararlı olacaktır.

1992 yılında British Columbia Üniversitesi'nde Luciana Duranti danışmanlığında Jane Turner tarafından hazırlanan yüksek lisans tezinde değerlendirme teorisine ilişkin verilen bilgiler bu çalışma için de değerlidir. Turner, söz konusu çalışmasında, değerlendirmeyi üç teorik ilke kapsamında ele almıştır. Bunlar; tarafsızlık, provenans ve çağdaş değer ilkesidir. Turner, bu üç ilkeyi Avrupa geleneksel değerlendirme anlayışı, Birleşik Krallık geleneksel değerlendirme anlayışı ve Kuzey Amerika değerlendirme anlayışı olmak üzere üç farklı anlayışla ifade etmiştir. Bu üç farklı değerlendirme anlayışını farklı kaynaklarla sentezleyerek geliştirmek ve Avustralya kıtasındaki değerlendirmenin de çalışmaya dâhil edilmesiyle, tezin bundan sonraki bölümlerinde işlenecek olan örgünün de felsefesini oluşturmak araştırmayı daha da önemli hale getirmektedir. Aşağıda sırasıyla Avrupa, Birleşik Krallık, Amerika ve Avustralya arşivsel değerlendirme anlayışları açıklanmıştır.

1. 2. AVRUPA GELENEKSEL ARŞİVSEL DEĞERLENDİRME ANLAYIŞI

Avrupa geleneksel değerlendirme anlayışında, Friedrich Meinecke, Hans Meissner, Marcel Baudot, Johannes Papritz, Elio Lodolini ve Hans Boom gibi arşiv teorisyenlerinin görüşleri, düşünceleri ve teorileri değerlendirilmiştir. Bu teorisyenlerin birçoğunun kapsamlı bir değerlendirme teorisi için arşivcinin tarafsızlık ilkesi ve değer göreceliği ilkelerini benimsedikleri ifade edilmektedir.[10] Avrupa'da değerlendirmenin geçmişi Fransız İhtilali'ne kadar götürülse de, daha öncesinde de idari kontekste belge

[10] Jane Turner, "A Study of the Theory of Appraisal For Selection," **Unpublished Master Thesis**, The University of British Columbia, Department of School of Library Archival and Information Studies, 1992, s. 8.

imha uygulamaları görülmektedir. Örneğin, 12. yüzyılda, papalığa ait kayıtların oluşturulması, söz konusu kayıtlarda tutulan belge birikimini, her organizasyonel faaliyetin tipik örneklerini belgeleyenlerle sınırlandırarak değerlendirme işlevi üstlenilmiştir. Daha sonra, 13. yüzyılda demokratik İtalyan şehir devletlerinin yükselişi, belgelerin imha edilmesi uygulamaları, devletlerin vatandaşlık ilkesine bağlılığı ile sınırlandırılmıştır.[11] Roma hukuku, Avrupa'nın ortak medeni yasası ve onun manevi ve kültürel birliğinin temelini oluşturmaktadır. Bu kavramlar, aynı zamanda Avrupa'daki arşiv teorisyenlerinin dayandığı temel ilkeleri de göstermektedir. Söz konusu kavramlar, 19. yüzyıldaki arşiv kuramcıları -Jenkinson, Cencetti, Brenneke, Bautier- ve zamanımızın Avrupa arşiv literatürünü zenginleştiren diğer pek çok kişi tarafından ele alındığı gibi ayrıca 16. ve 17. yüzyıl hukukçularının yazılarında geliştirdikleri Avrupa arşivleme kuramının da çekirdeği haline gelmiştir.[12]

1.2.1. Almanya Geleneksel Arşivsel Değerlendirme Anlayışı

Daha önce de ifade edildiği gibi, Almanya'da arşivci imhadan önce koruma öncelikli bir davranış benimsemiştir. Prusya Hükümetince değerlendirmeye olan ilgi, 1833 yılından sonra gelişmeye başladı. 1858 yılında idari belgeler arşivcilerin bilgisi dâhilinde olmadan herhangi bir imha işlemine tabi tutulmaması gerekiyordu. Uygulamada başarılı olunmasa da değerlendirme açısından atılan önemli bir adımdı.[13] Arşivcilerin geçmişte ve gelecekte bir sonraki nesiller için neleri koruması gerektiği sorumluluğu 1897 yılında Bavyera'da tanımlanmıştır.[14] 1926 yılında Karl Otto Müller, arşivlerle ilgili en önemli sorunun değerlendirme olduğunu ifade eder ve arşivcinin hangi belgelerin saklanılması ve imha edilmesi kararını vermesi gerektiğini savunmaktadır. Müller, değerlendirme için bazı tavsiyelerde bulunur ve kurumlar için merkezi, orta

[11] **A.e.**, s. 31-32.

[12] Luciana Duranti, "The Concept of Appraisal and Archival Theory," **American Archivist**, Spring 1994, C. 57, S. 2, s. 333-334.

[13] Wilhelm Rohr, "Das Aktenwesen der preussischen Regierung" [The Records System of the Prussian Government], **Archivalische Zeitschrift**, 1939, C. 45, s. 60; Aktaran: Ole Kolsrud, "The Evolution of Basic Appraisal Principles - Some Comparative Observations," **American Archivist**, Winter 1992, C. 55, S. 1, s. 30.

[14] Ottfried Dascher, "Archivar und Historiker. Zum Standort eines Beruf im Wandel von historischen Interessen und Methoden" [Archivist and Historian. The State of a Trade Changed by Historical Interests and Methods], **Der Archivar**, 1983, C. 36, s. 29.; Akt: Kolsrud, **a.e.,** s. 30.

ve yerel olmak üzere üç farklı ayrımda bulunur. Modern arşivlere bakıldığında bu ayrımın kalıcı bir şekilde etkisinin devam ettiği görülmektedir. Nitekim merkezi ve orta yönetim organları daha değerli belgeler üretirken, yerel olanlar daha az ilgi çekici olmaktadır.[15] Alman coğrafyasında değerlendirme ile ilgili önemli gelişmelerden biri de 12 Aralık 1927 kararnamesidir. Bu kararname, Prusya arşiv yetkililerinin Prusya bakanlıklarının tüm kayıtlarının sistematik bir incelemesini yapmaları ve kalıcı değer olarak kabul edilenleri seçmeleri gerektiğini belirtmekteydi.[16] Alman arşivcilere verilen bu yetki ve sorumluluk tecrübeyle birleşerek değerlendirme için yeni ilke ve prensiplerin benimsenmesinin gerekliliğini ortaya koymuştur. Bu sebeple, Heinrich Otto Meisner 1937 yılındaki yıllık Alman arşivciler toplantısında, kendi tabiriyle "bırakın yapsınlar" ve "içgüdü" ile arşivsel değerlendirmenin yapılamayacağını söylemiştir. Meisner, idari belgelerin idarelerce 5 yılda bir gözden geçirilmesini savunmakta ve arşivcilerin rızası olmadan imha yapılmayacağı görüşünü reddetmektedir. Meisner, değerlendirme için üç temel ilkeyi önermektedir:[17]

1. Yıl Sınırı: Ülkeden ülkeye farklılık gösterse de Almanya için bu tarih 1600 civarında başlamaktadır.
2. İçerik: Kalıcı kurumlar hakkında bilgi içeren materyaller korunurken belirli zaman kısıtlı amaçlarla sunulan örneğin istatistiksel araştırmalar (nüfus sayımı materyali, vb.) imha edilebilir.
3. İdari Organın Hiyerarşik Yapısı: Heinrich Otto Meisner, bu ilke için Karl Otto Müller'in kurumların merkezi yönetim makamları veya daireleri, eyalet düzeyinde yer alan yönetim makamları ve yerel düzeydeki (ilçe gibi) yönetim makamları veya daireleri (Almanca: Zentralbehörden, Mittelbehörden, Bezirkbehörden/ İngilizce: Central, Intermediate, Local Authorities) olmak üzere üçe

[15] Karl Otto Müller, "Fragen der Aktenaussscheidung" [Questions on Appraisal], **Archivalische Zeitschrift**, 1926, C. 36, ss. 188-215; Akt: Kolsrud, **a.e.**, s. 30-31.

[16] Kolsrud, "The Evolution of Basic Appraisal Principles - Some Comparative Observations," s. 31.

[17] Heinrich Otto Meisner, "Schutz und Pflege des staatlichen Archivgutes mit besonderer Berucksichtigung der Kassationsproblems" [The Protection and Care of Public Records with a Special View to the Problems of Appraisal], **Archivalische Zeitschrift**, 1939, C. 45, ss. 34-51; Akt: Kolsrud, **a.e.**, s. 31.

ayrımını benimsemektedir. Otorite ne kadar yerel düzeyde ise önemi de o derece düşüktür. Eyalet düzeyinde yer alan otoriteler için de alacakları değer bağımsız yetkili karar vericilerce şekillenecektir.

Alman arşivcilerinin değerlendirme ile ilgili tartışmaları 1957 yılında yapılan Koblenz'deki toplantıda Georg Wilhelm Sante ve Wilhelm Rohr'un, Müller ve Meisner'in düşüncelerini yeniden canlandırmasıyla yeni bir boyut kazanmıştır. Georg Wilhelm Sante ve Wilhelm Rohr, modern arşivlerin büyük bir kısmı, ayrıntılı değerlendirmeyi imkânsız hale getirdiğinden, ilgili birimlerin tüm idari organları kalıcı korumaya az veya çok değersiz olarak tanımlaması gerektiğine karar vermişlerdir. Georg Wilhelm Sante ve Wilhelm Rohr, aynı zamanda birimin idari seviyesini ve birimin bağımsız karar verme yetkisini de dikkate aldılar. Bunu takiben kabine ya da hükümet seviyesinde çok az imhanın olması ya da hiçbir şeyin yok edilmemesi durumu ortaya çıkmış oldu. Ancak imhanın, en düşük idari düzeyde çok ya da her şey olduğu görülmüştür. Bakanlıklar ve bölümler de önem sırasına göre sıralanabilmiştir. Dış politika ticaretten daha önemliydi ve bu yüzden Dışişleri Bakanlığı belgeleri Maliye Bakanlığı'nınkinden daha değerli olacaktı.[18] Bu yaklaşım arşivcinin mümkün olmayan zamanını değerlendirmeye harcamasını bir tarafa bırakarak resmi bir değerlendirme ilkesini ortaya koyması fikrinin genel bir kabul görmemesine neden oldu. Değerlendirmeyle ilgili yapılan tartışmaları körükleyen bu gelişmeler, Fritz W. Zimmermann'ın düşünceleriyle yeni bir tartışma ortamı yaratır. Zimmermann, belgelerin içeriğinin ve kaynaklarının değil, koruma veya imhanın belirleyici neden olması gerektiği iddiasını savunur. Belgelerin pazar değerine (market value) göre değerlendirmesini ileri sürer.[19] Zimmermann'ın pazar değerinin belgelerin uygunluğu için belirleyici kriter olması gerektiği görüşüne yüksek sesle itiraz edilmiş olsa da Alman arşivcileri arasında bu ko-

[18] Hans Booms, "Gesellschaftsformen und Uberlieferangsbildung; Zur Problematik archivalischer Quellenbewertung" [Social Systems and the Selection of Records; On the Problems of Appraisal in Archives], **Archivalische Zeitschrift**, 1972, C. 68, ss. 3-40; Akt: Kolsrud, **a.e.**, s. 32.

[19] Fritz W. Zimmermann, "Wesen und Ermittlung des Archivwertes. Zur Theorie einer archivalischer Wertlehre" [Nature and Appearance of Archival Value. On the Theory of Archival Appraisal], **Archivalische Zeitschrift**, 1958, C. 54. This citation is according to Booms, "Gesellschaftsformen und Uberlieferungsbildung," s. 15; Akt: Kolsrud, **a.e.**, s. 32.

nuda ihtilaf görülmektedir. Belgelerin toplumsal ekonomi açısından değerlendirilmesine karşı en sert eleştiri, 1965'te yayınlanan iki makalede Arthur Zechel'den geldi.[20] Arthur Zechel, Zimmermann'la karşı karşıya gelmenin ötesinde tamamen bağımsız bir arşivcilik bilimi için gerekli teorik temelleri kurmayı amaçlıyordu. Bu nedenle değer teorisi bir anda arşivciliğin temel sorunu haline geldi. Belgelerin değeri (bilimsel) talep dikkate alınmaksızın tanımlanması gerekliyse, o zaman arşivcilikle tarih arasında da açıkça bir hat çizilmeliydi. Bu görüşü savunan Zechel bunu "tarih"i üç aşamaya bölerek yapmaya çalıştı. Bunlardan ilki, -her ne kadar izler bıraksa da- hafıza dışı olup geçmişe karışan tarihi olaylardır. İkincisi, tarihsel bir kaynaktan erişilebilen hatıralardır. Sonuncusu ise kaynakların bilimsel yorumlaması olan tarih yazımıdır. Zechel, arşiv bilimini söz konusu aşamalardan ikincisi olan hatıralar aşamasıyla ilişkilendirir. Özetle, bir arşivci değerlendirdiğinde, sadece arşivsel bakış açısından belgelere bakar. Ancak, kayıtlar halka açık hale getirildiğinde, onlara tarihçi olarak bakmak zorunda kalacak[21] düşüncesi vardır.

Avrupa geleneksel arşivsel değerlendirme anlayışını yansıtan ülkelerden biri de İzlanda'dır. İzlanda Milli Arşivi (National Archives of Iceland, NAI), 1985 yılına kadar tüm belgelerin arşive devredilmesini zorunlu kılarken, 1985 yılında yeni milli arşiv kanununun çıkmasıyla, "Ulusal Arşivlerin iznine sahip olmadıkça veya kayıtların imha edilmesine ilişkin belirli kurallar koyulmadıkça, belgelerini teslim etmekle yükümlü olan tarafların arşivlerinde herhangi bir transfer veya imha işlemi yapmalarına izin verilemez şeklinde yasal zorunluluk getirmiştir.[22] Bu düzenlemeyle, belgelerin değerlendirilmesiyle beraber imha edilmesi hususu da meşru bir çerçeveye oturtulmuş-

[20] Arthur Zechel, "Wertheorie und Kassation" [Value Theory and Disposal], **DerArchivar**, 1965, ss. 1-16 and "Probleme einer Wissenschaftstheorie der Archivistik mit besondere Beriicksichtigung des Archivwesen der Wirtschaft" [Problems of a Science Theory on Archivistique with a Special View to Business Archives], Tradition. **Zeitschrift fur Firmengeschichte und Untemahmenbiographie**, 1965, C. 10, ss. 285-300.

[21] Kolsrud, "The Evolution of Basic Appraisal Principles - Some Comparative Observations," s. 33.

[22] Kristjana Kristinsdottir, "The Turning Point in 1985. The History of Appraisal and Disposal of Records in Iceland," **ArchivaI Science**, June 2003, C. 3, S. 2, s. 201.

tur. Değerlendirme yapılacak belgelerin, içerdikleri bilgiler ve tarihsel kaynaklar olarak değerlerine göre işlemden geçirilmesi, uygulanacak değerlendirme kriterlerinin altını çizmektedir.[23]

1.3. BİRLEŞİK KRALLIK GELENEKSEL ARŞİVSEL DEĞERLENDİRME ANLAYIŞI

Birleşik Krallık geleneksel değerlendirme anlayışında, Hilary Jenkinson ve James Grigg'in teorileri incelenmiştir. Jenkinson'ın arşivlerin doğası teorisi ve Grigg'in arşivlerin doğasıyla ilgili olan tarihsel değer ve idari değer, arşivlerin doğasını arşivsel ve kanıtlayıcı olarak korunmasını sağladığı değerlendirilmektedir.[24] İngiltere'de 19. yüzyılın son çeyreğinde değerli evrakın saklanılması ilkesinden ziyade değersiz evrakların imhasını vurgulayan geleneksel bir meyil söz konusuydu. Yani imha etmek için değerlendirme yapılırdı. 1875 yılında arşiv muavinliği makamı tarafından (Public Record Office, Deputy Keeper) İngiliz Devlet Arşivinde yasal, tarihi, askeri, istatistiki, ekonomik veya resmi amaçlar için tamamen yararsız olan ve herhangi bir menfaat sağlamayan geniş çaplı yasal ve resmi belgelerin var olduğu iddia edilmiştir. Muavinlik, ellerinde bulunan arşivleri imha etme ve değersiz gördüğü yeni kayıtların alınmasını reddetme yetkisine sahip olmasını talep etmiştir. 1877 yılındaki Devlet Arşivi Kanunu (Public Record Office Act of 1877) ile bu yetkiyi almıştır. Bu yetkiyle 1715 yılı öncesine ait belgeler hariç tutulmak suretiyle 1715 yılından 1877 yılına kadar olan evrakların imha edilmesinin yolu açılmış oldu. Daha sonra hariç tutulan 1715 öncesi daha da geriye götürülerek 1660 yılından öncesi evraklar dâhil olmayacak şekilde o tarihten itibaren olan belgeler imha edilebilecekti. Bu yıl sınırı kriteri dışında, belgelerin kalıcı değerini neyin oluşturduğuyla ilgili herhangi bir kriter gözükmemektedir. Ancak, düzenlemede; yasal, tarihi, soy bilimsel ya da antika kullanımı ya da çıkarları bakımından makul olarak düşünülebilecek veya başka bir yerde elde edilemeyen önemli bilgiler

[23] **A.e.**, s. 202.
[24] Turner, "A Study of the Theory of Appraisal For Selection," s. 8.

veren herhangi bir belgenin imha programına dâhil edilmemesine karşı genel bir uyarıda bulunulduğu görülmektedir.[25] 1912 yılında Oxford'daki bir arşivci[26], herhangi bir idari faaliyetin sadece son ürününün, yani bir birimin sadece nihai, yasal olarak bağlayıcı belgelerinin kalıcı korumaya değer olduğu fikrini savunmuştur.[27] Bu gelenek ve Birinci Dünya Savaşı'nın yarattığı durumdan dolayı 1922'de Hilary Jenkinson'un ünlü "Manual of Archive Administration/Arşiv Yönetimi El Kitabı" adlı eseri büyük bir yankı uyandırmıştır. Kitap, "Dünya Savaşının Ekonomik ve Sosyal Tarihi" adlı dizide yer almış ve daha sonra revize edilerek 1937 yılında ve tekrar revize edilmiş haliyle 1966 yılında yayınlanmıştır. Jenkinson'un ana teması gereksiz belgelerden kurtulmanın yolunu bulmaktı. Bunun cevabı ise basit olmakla beraber, arşivcilerin müdahalesi olmadan yapılacak işlerdi. Jenkinson'a göre imha, arşivcinin işinin herhangi bir parçasını teşkil etmiyordu. Tarihçi arşivciden daha iyi değildi. İkisi de çok taraflı ve bilgisiz olacaklardı. Bunun bir sonucu olarak Jenkinson'ın ortaya koyduğu şey, geçmişin bize bıraktığı kayıtların imha edilmesinin kabul edilemez olmasıydı. Çünkü bu işi yapacak yetkin bir kişi olmayacaktı. Modern arşivlerde bu işler nasıl yürüyecekti? Arşivcilerin ve tarihçilerin modern arşivlerle ilgili bilgileri daha kısıtlıydı. Gelecekte, arşivler üzerinde çalışmanın sadece kendi yığınları nedeniyle umutsuzca karmaşık bir iş haline gelebileceği gerçek bir tehlikeydi.[28] Jenkinson, bunlara çözüm önerisi olarak, belgelerin imha edilmesinin idari makamın kendisine bırakılması gerektiği düşüncesindeydi. Bu düşünce, arşiv teorisine özgün ve eşsiz bir İngiliz katkısı olarak görülmektedir. Jenkinson'ın genel olarak arşiv felsefesi, yönetici ile araştırmacı arasında arşivciye izin verdiği oldukça mütevazı bir yerle yakından bağlantılıdır. Arşivcinin birincil görevi, geçmişin tesadüfen ve gelişigüzel olarak tutulan arşivlerinin hizmetçisi

[25] Her Majesty's Stationery Office, **Committee on Departmental Records Report**, London, 1954, s. 16. This 1954 report is otherwise known as The Grigg Report after the name of its chairman, Sir James Grigg. ; Akt: Kolsrud, "The Evolution of Basic Appraisal Principles - Some Comparative Observations," s. 27.

[26] İngiliz tarihçi olan Reginald Lane Poole, Oxford Üniversitesinde diplomatika alanında öğretim görevliliği de yapmıştır. Papers of Reginald Lane Poole (F. 1898–1933), (Çevrimiçi, http://www.magd.ox.ac.uk/libraries-and-archives/archives/online-catalogues/poole-papers-3/, 15 Ağustos 2019). Söz konusu arşivcinin kesin olmasa da, 1909-1927 yılında Oxford Üniversite Arşivinde arşivci olarak çalışan Reginald Lane Poole olması kuvvetle muhtemeldir.

[27] David George Vaisey, "The Image of the Archivist, Harmonization of Training and International Mobility" (Paper delivered at the international symposium entitled "Archives and Europe Without Boundaries," Maastricht, The Netherlands, 2-5 October 1991); Akt: Kolsrud, **a.e.**, s. 27.

[28] Hilary Jenkinson, **A Manual of Archive Administration Including the Problem of War Archives and Archive Making**, Oxford, The Clarendon Press, 1922; Akt: Kolsrud, **a.e.**, s. 27.

olmaktır. İkincil görevi ise öğrencilere arşiv hizmeti vermektir. Jenkinson'ın fikirleri İngiltere'de arşivsel düşünceye güçlü bir etki bırakmıştır. Böylelikle idari organlara ürettikleri belgelere istedikleri gibi işlem yapmaları hakkı verilmiştir. İngilizler, İkinci Dünya Savaşı'nın patlak vermesi üzerine, belgeleri kurtarmaya ve mühimmat üretmeye yönelik bir yol olarak arşiv depolarına başvurduklarında, Jenkinson'ın öğretisine göre oldukça uygun bir tavır sergilemiş oldular. Amerikalılar da 1930'lar ve 1940'larda "belgelerin korunmasından ziyade dikkatlerini belgelerin imhasına verdiler" sözleriyle anlatan Philip C. Brooks, İngiliz pratiğine karşı uyarıda bulunmuş ve kayıtların değeri için üç temel kriter belirlemeye çalışmıştır. Bunlar; belgenin üretildiği orijinal kurum değeri, idari tarih için değer ve tarihsel araştırma için değerdir.[29] T. R. Schellenberg'e göre İngilizler bu bakış açısını 1943 yılında benimsediler.[30] İngilizler, Brooks'un görüşünü kabul ettiler. Çünkü Brooks, belgenin üretildiği birimin bir değer olarak, idari yapının iş amaçlarına yönelik kendi içinde kararlar alması gerektiğini savunuyordu. İngilizler, söz konusu kuruluşların faaliyetleriyle ilgili teknik soruları cevaplamak için gelecek araştırmalara hizmet ettikleri takdirde korunmaları gerektiğini eklemek için Brooks'un listesini değiştirdiler. Böylelikle İngiltere'de Amerika Birleşik Devletleri'nin yardımıyla belgelerin kalıcı olarak korunması için üç kriter geliştirilmiş oldu. Bu üç kriter; idari organın işleyişine ışık tutmak, idari organın tarihine ışık tutmak ve genel olarak akademik bilgi ihtiyaçlarını karşılamaktı. 1952 yılına gelindiğinde Grigg Komitesi (Grigg Committee)'nin kurulması İngiliz değerlendirme anlayışı için önemlidir. Komitenin amacı, İngiltere'de problemleri kapsamlı olarak ele alacak yeni bir değerlendirme sistemini kurmaktı. Komite, idari ve tarihi olmak üzere iki değerlendirme kriteri belirlemiştir. Belgeler iki aşamada değerlendirilmeli, böylelikle idari ölçüt, yürürlükte olan tarihsel ölçüt haline gelecekti. Bunun sonucunda çok fazla çaba sarf etmeden idari organın kendisi tarafından bu ölçütün güvenli bir şekilde yürütülmesi sağlanacaktı. Komiteye göre, bir kurum bir eylemin tamamlanmasının ardından kısa bir süre içerisinde bir belgenin, kuruma ilişkin olarak kendi amaçları için daha fazla gerekli olmayacağına karar verirse, bu belgenin maddi bir tarihsel öneme

[29] Meyer H. Fishbein, "A Viewpoint on the Appraisal of National Records," **American Archivist**, April 1970, C. 33, S. 2, s. 176; Akt: Kolsrud, "The Evolution of Basic Appraisal Principles - Some Comparative Observations," s. 28.

[30] T.R. Schellenberg, **Modern Archives**, Chicago, The University of Chicago Press, 1956, s.137; Akt: Kolsrud, **a.g.e.**, s. 28.

sahip olması muhtemel değildi.[31] Belgelerin %50 ile %90'ı, beş yıl sonra yapılan ilk gözden geçirmede -idari ölçütün bu uygulamasıyla- fazla çaba sarf edilmeksizin imha edilmek zorundaydı. Yirmi beş yıl sonra yapılan ikinci gözden geçirmede, kayıtlar yönetilebilir bir boyuta indirgenmiş olacak ve tarihsel ölçüt daha sonra doğrudan profesyonel bir değerlendirme uzmanı tarafından geri kalan malzemeye uygulanabilecekti.[32] Grigg Raporu ve 1958 tarihli Devlet Arşivi Yasası, İngiltere'deki mücadelede bugüne kadar malzemeyi korumadan önce imhaya neden olan bir noktaya taşıdı. Ancak İngilizler bunun yanı sıra başka bir düşünceye daha sahipti.[33] Bu düşünce, 1981 tarihli Wilson Raporu'ydu[34]. Wilson, Grigg sistemini ağır bir şekilde eleştirdi ve Devlet Arşivi'nin koruma politikasını tam bir başarısızlık olarak değerlendirdi. Wilson Raporu, Grigg sistemiyle uğraşmak için hiçbir girişimde bulunmadı, ancak zamanın imhaya göre daha fazla korumaya yoğunlaştığını öne sürdü. Ayrıca, kalıcı koruma için materyal seçimi sürecinde arşivcilerin daha aktif bir rol oynaması gerektiğini savundu. Bu raporun, yönetim kriterinin geniş çaplı uygulanmasına yönelik bir saldırı olduğu söylenmekle beraber, bir dönüm noktası da sayılabilir. Fakat rapor devlet tarafından dikkate alınmadı.[35]

Günümüzde İngiltere'de farklı uygulamalar da söz konusu olabilmektedir. Örneğin İngiltere Staffordshire ve Stoke On Trent Arşiv Servisi arşivsel değerlendirme ve imha politikasında işlevselliğe dayanan makro değerlendirme yöntemini benimsemektedir. Bunun nedeninin de açıklandığı politikada, "makro değerlendirme, kayıtları tutma, imha etme veya örnekleme kararını gerektirdiği belirtilmektedir. Mevcut kaynaklar göz önünde bulundurulduğunda en uygun yaklaşım budur. İşlevsel analiz, kuruluşların işlevlerini tanımlar ve kalıcı koruma için yüksek bilgi değerine sahip kayıt

[31] Grigg Report, 30; Akt: Kolsrud, "The Evolution of Basic Appraisal Principles - Some Comparative Observations," s. 29.

[32] Kolsrud, **a.g.e.**, s. 29.

[33] Alfred W. Mabbs, "The Public Record Office and the Second Review," **Archives**, 1967-1968, C. 8, s. 180- 184; Akt: Kolsrud, **a.e.**, s. 29.

[34] The Wilson Report, **Modern Public Records. Selection and Access**, London, Her Majesty's Stationery Office, 1981.

[35] Modern Public Records. **The Government Response to the Report of the Wilson Report**, London, Her Majesty's Stationery Office, 1982; Akt: Kolsrud, **a.e.**, s. 29.

dizilerini seçmek için kullanılır"[36] şeklindeki açıklamalar kullanılan değerlendirme yönetiminin kendileri için meşruluğunu ortaya koymaktadır. Makro değerlendirme ve dökümantasyon stratejisi yaklaşımları, arşivcilerin arşiv kurumlarından tüm koleksiyonları tamamen ortadan kaldırmaya ve daha fazla kaynağın korumaya yatırılmadan önce bunları belirlemeye önem vermesine yardımcı olabilecek araçlar için kaynak olarak düşünülmelidir. Her bir değerlendirme teorisi, yüksek düzeyde kayıtların belirli niteliklerine sahiptir. Arşivciler bu niteliklerin ne olduğunu ve farklı değerlendirme teorileri aracılığıyla nasıl uygulandıklarını tam olarak anlamalıdırlar.[37] Bu farklılıklarla beraber yaygın olarak kullanılan Grigg Raporu elektronik ortamdaki belgelerin değerlendirilmesi için için uygun görülmemektedir. İngiliz Ulusal Arşivleri (The National Archives, daha önce Public Record Office) Grigg Raporunu 1954 yılından beri uygulamaktadır. Grigg değerledirme sistemine göre, beş yıl (devam eden işletme değeri ve potansiyel arşiv değeri için) ve 25 yıl (arşivleme değeri için) kuralı geçerliydi. 2013 yılında İngiliz Milli Arşivleri tarafından yayınlanan dokümanda Grigg Raporuna göre değerlendirmenin birçok sebepten dolayı mümkün olmayacağı ifade edilmektedir. Bu sebepler;[38]

- Dijital bilgi savunmasızdır ve format eskimesi veya silinmesi nedeniyle erişilemez hale gelebilir. Kurumlardaki birimlerin, bilgi yaşam döngüsünün başlarında bilginin değeri hakkındaki kararları almaları gerekir. Bu, temel bağlamın korunmasını sağlamak ve bilgilerin etkin ve etkili bir şekilde değerlendirilmesini sağlamak için hayati öneme sahiptir.
- Dijital bilginin artan hacmi, çoğalması ve karmaşıklığı, dosya bazında bir yaklaşımın yasaklayıcı ve kaynak yoğun olduğu anlamına gelir.
- Belge dosya incelemesi zaman alıcıdır ve birim kaynaklarının verimli kullanımı olmayabilir.

[36] Staffordshire and Stoke On Trent Archive Service Appraisal And Disposal Policy, **Method of Appraisal**, 6. Rule, (Çevrimiçi) https://www.staffordshire.gov.uk/Heritage-and-archives/about/Policies/Archive-Service-Appraisal-and-Disposal-Policy.aspx, 10 Mayıs 2018.

[37] Tyler O. Walters, "Contemporary Archival Appraisal Methods and Preservation Decision-Making," **American Archivist**, Summer 1996, C. 59, S. 3, s. 337.

[38] The National Archives, **Best Practice Guide to Appraising and Selecting Records For The National Archives**, y.y., Crown Copyright, 2013, s. 3, (Çevrimiçi) http://www.nationalarchives.gov.uk/documents/information-management/best-practice-guide-appraising-and-selecting.pdf, 16 Ağustos 2019.

- 2013 yılından itibaren 30 yıl kuralı, 10 yıllık bir geçiş zaman çizelgesi içinde kademeli olarak 20 yıla indirilecektir. Mevzuattaki değişikliğe uymak için kısa bir süre içinde daha fazla kaydın gözden geçirilmesi gerekecektir.
- Hükümet değişikliklerinin mekanizmaları (işlevlerin kaldırıldığı veya aktarıldığı yerlerde), kısa sürede büyük miktarda bilginin sık sık değerlendirilmesi gerektiği anlamına gelir.

Görüldüğü üzere dijital ortamın getirdiği zorunlulukla beraber mevzuat ve idari değişiklikler Grigg Raporu'nun yürütülmesinin artık uygun olmayacağını göstermektedir. Bilginin teknolojik dönüşümü 5 yıldan daha az bir sürede gerçekleşir. Onun için Grigg Raporu'nun 5 yıl kuralı burda devre dışı kalabilir. Yine belgelerin arşivsel değeri için konulan 25 yıl sınırı elektronik ortam için çok uzun bir süredir. Ortamın değişkenliği, kırılganlığı ve güvensizliği bu zamanın revize edilmesini gerektirir. Nitekim 2013 yılında 30 yıllık değerlendirme süreci 20 yıla inmiş görünmektedir.

Yine İngiliz Milli Arşivleri tarafından 2013 yılında yayınlanan bir diğer dokümanda arşivsel değerlendirme için etkili ilkeler şu şekilde sıralanmaktadır:[39]

- Zamanlama: Kurumlar rutin belge yönetimi faaliyetlerinin bir parçası olarak belge değerini mümkün olduğunca erken değerlendirmeyi amaçlamalıdır. Grigg sisteminde bu süre 30 yıl iken on yıl öne çekilerek artık 20 yıl olarak öngörülmüştür.
- Metodoloji: Kurumlar değerlendirmeyi daha verimli hale getirmek için belge gruplandırmalarını değerlerine göre yapmalıdır. Bu, mümkün olduğunda, belgelerin oluşturulduğu veya kullanılmakta olduğu bağlamı temel alan belge grupları veya bilgi kategorileri hakkında kararlar alınması anlamına gelir. Kurumların hedeflerini, işlevlerini ve iş süreçlerini anlamak, temel bilgi varlıklarını tanımlamaya ve saklama süreleri hakkındaki kararları desteklemeye yardımcı olacaktır. Ayrıca, söz konusu gruplandırmalar zaman alıcı olabilecek inceleme ihtiyacını bireysel olarak da azaltmalıdır.

[39] The National Archives, **What is Appraisal?**, y.y., Crown Copyright, 2013, s. 5-6, (Çevrimiçi) http://www.nationalarchives.gov.uk/documents/information-management/what-is-appraisal.pdf, 16 Ağustos 2019.

- Sorumluluk: Belgelerin değerinin belirlenmesi, kuruluşun oluşturulmasında ve yönetiminde yer alan iş alanlarına yönelik faaliyetler içermelidir. Bu, belirli belgeleri tutmak için kullanılabilirliği ve yasal gereklilikleri yerine getirecektir. Değerlendirme bu açıdan sorumluluğun paylaşıldığı önemli bir süreç olarak görülmelidir. Örneğin, dijital kayıtların yapısını anlamak ve bulundukları sistemde farklı saklama süreleri uygulamak hem bilgi teknolojilerini yöneten grubun hem de üst yönetimin sorumluluğudur.
- Belgeleme: Belgelerin değeri belirlendikten sonra, kararların alınması ve bilgilerin güncel tutulması önemlidir. "Bilgi Varlık Kayıtları"nın oluşturulması, belirli bilgi risklerini izlemenin yanı sıra, belgelerin değerlerine göre yönetimini desteklemeye yardımcı olacaktır.
- Rehberlik: Belgelerle ilgili koleksiyon politikaları belgelerin potansiyel tarihi değerini anlamak açısından yararlıdır. Hazırlanacak olan koleksiyon politikaları hangi belgelerin ne şekilde değerlendirileceği noktasında yardımcı olacaktır.

1.4. KUZEY AMERİKA GELENEKSEL ARŞİVSEL DEĞERLENDİRME ANLAYIŞI

Kuzey Amerika geleneksel değerlendirme anlayışında ise Philip C. Brooks ve Theodore Schellenberg'in çalışmaları değerlendirme için birincil kaynaklardır. Brooks ve Schellenberg'in, kanıtsal değer ve bilgi değeri kavramları, kullanımı değerle eşitleyen ve teorik problemlerin entelektüel çözümünü saptıran pratik bir stratejiyi yansıtmaktadır.[40] Kanada'da 2003 ve 2005 yılları arasında 450 Kanadalı arşivci ile yapılan anket sonuçları, değerlendirmenin uygulama noktasında ne durumda olduğunu gösteren önemli bir çalışmadır. Elli sekiz soru şeklinde hazırlanan araştırma, özellikle bir iş süreci olarak değerlendirme hakkında bilgi vermektedir. Kanada'daki arşiv depolarında değerlendirmenin arşivciler tarafından nasıl yapıldığı, kullandıkları kaynakların neler olduğu, ne gibi engel ve sorunlarla karşılaştıkları ve deneyim ışığında, bu işi yaparken hangi araçların, becerilerin ve bilginin önemli olduğu ortaya konmuştur.[41]

[40] Turner, "A Study of the Theory of Appraisal For Selection," s. 8.

[41] Barbara L. Craig, "Doing Archival Appraisal in Canada. Results from a Postal Survey of Practitioners' Experiences, Practices, and Opinions," **Archivaria**, Fall 2007, C. 64, ss. 1-45.

Çalışmanın sonuçları arasında "arşivcilerin hangi değerlendirme yöntemlerini yararlı buldukları" sorusu da sorulmuştur. Alınan sonuçlara bakıldığında, Kanadalı arşivcilerin değerlendirme yaparken tek bir yöntemden daha fazlasını kullandıklarını göstermektedir. Kanıtsal ve bilgilendirici olma durumuna göre belgelerin değerlendirilmesi en sık başvurulan yöntemdir ve bu oran %94.73'tür. Tarihsel analiz %90.48'lik oranla başvurulan ikinci yöntem, fonksiyonel analiz ise %82.64 oranla başvurulan üçüncü yöntem olarak görülmüştür. Her zaman ya da zaman zaman kullanılan diğer yöntem çeşitleri arasında kurumda yerleşik öncelikler %84.79, aynı türden önceki elde etme yöntemlerinin özel analizi %74.09, özel kullanım analizi ve edinim planlama ve belgelendirmeye yönelik stratejik yaklaşım %71.37 oranında kullanılmıştır.[42]

1.4.1. Amerika Birleşik Devletleri Geleneksel Arşivsel Değerlendirme Anlayışı

Amerika Birleşik Devletleri'nin İkinci Dünya Savaşı boyunca İngiltere ile arşivcilik açısından bir etkileşim içinde oldukları bilinmektedir. Geleneksel imha anlayışında, Philip Coolidge Brooks, 1940 yılında ABD'de belgelerin artan hacimlerini azaltmanın farklı yöntemlerle mümkün olacağını düşünür. Ona göre bu yöntemler üçe ayrılır. Bunlardan ilki, ilgili tarihsel topluluklara veya kütüphanelere aktarılması için belge üreten kişi veya kuruluş için olanıdır. Bunun için gerekli teşviklerin yapılması, ancak bu birimlerin çoğu zaman sınırlı depolama alanlarına sahip oldukları için hacim sorununu tamamen çözmeyeceği unutulmamalıdır. Bunun yanı sıra diğer iki yöntem de doğru bir beklenti sunmaktadır. Bunlardan birincisi, kayıtların mikrofilm üzerine çoğaltılması ve asılların daha sonra imha edilmesidir. Fotoğraf ekipmanları, indirgeme oranları, okuma cihazları ve diğer teknik faktörler üzerinde çalışmalar yapılmakta ve bazı büyük ölçekli deneyler gerçekleştirilmektedir. Son yöntem ise temsili örneklemedir.[43] Ulusal Arşiv'de bir arşivci olarak çalışan Philip Coolidge Brooks, 1940 yılında yayınlandığı makalesinde, belgelerin üretiminden imhasına kadar bir belgenin tüm yaşam döngüsünü kapsayacak şekilde değerlendirmesini tartışıyordu. Brooks'a göre de-

[42] Craig, **a.e.**, s. 21.

[43] Philip Coolidge Brooks, "The Selection of Records for Preservation," **American Archivist**, October 1940, C. 3, S.4, s. 227.

ğerlendirme fonksiyonunun yerine getirilmesi, belgenin üretildiği birimin iyi bilinmesini gerektiriyordu. Çünkü belgenin üretilme aşamasında diğer belgelerle ilişkisinin bilinmesi önemliydi. Aksi takdirde 20 yıl boyunca bekletilmiş ve unutulmuş belgelerin değerlendirilmesi herhangi bir anlam taşımazdı.[44] Brooks, İngilizlerde olduğu gibi, etkin idare için hangi belgelerin önem taşıdığına karar vermek için değer ölçütlerinin yönetim organının kendi işi olması gerektiğini savunmuştur. Bu görüş, 1950'lerin ortasında Theodore R. Schellenberg tarafından tanımlanan belgelerin birincil değeriyle aynı şeydi. İngiliz görüşüne katılan Schellenberg, bunun kısa ve geçici bir doğası olduğunu ve yöneticinin kararına bırakılması gerektiğini ifade etmiştir. Belgeler, ikincil değerlerini araştırmalara gösterilen önem sayesinde gerçekleştirirler. Schellenberg ile İngilizler arasındaki büyük fark, İngilizlerin birincil değer ile ikincil değer arasında somut ve fiziksel bir bölünmenin varlığını varsaymalarıdır. İdareye kendisi için kullanımına gerek kalmayan belgelerin imha edilmesine müsaade edilmesi, geriye kalan sadece araştırma değeri olan belgeler olacağı anlamını taşıyacaktı. Schellenberg bu görüşü kabul etmez. Ayrıca, İngiltere'de, araştırmaya uygun belgeler için üç değer kriteri belirlenmiştir. Belgelerin kurumun tarihçesi, işlevi hakkında bilgi vermesi ve genel olarak araştırma değerinin olmasıdır. Bu üç öğe de Schellenberg'de yer alır.[45] İlk ikisi, belgelerin "kanıt değeri" kavramının altında bulunur. Sonuncusu, belgelerin "bilgi değeri" kavramına karşılık gelir. Böylece Schellenberg'in sistemi şu şekildedir:

1. Birincil değer – İdari değer (belgenin üretildiği yer)
2. İkincil değer - Araştırma değeri
   a. Kanıt değeri: Kurumun (1) tarihi, (2) organizasyonu ve işlevi hakkında bilgi vermesi
   b. Bilgilendirme değeri: (3) Genel olarak araştırmaya önem veren belgeler

Schellenberg, belgelerin kalıcı değerinin ikincil değer olduğunu söyler. Bu ikincil değer arşivcilerin dikkatini çekmektedir. Bu sebeple Schellenberg, bu tarz belgeler için bir takım değerlendirme standartları koymaya çalışır. Birincil değere baktığımız

[44] **A.g.e.**, s. 226.

[45] Kolsrud, "The Evolution of Basic Appraisal Principles - Some Comparative Observations," s. 35.

zaman, arşivcinin, birimin bağlı olduğu kurumun idari teşkilatlanmasındaki yerini belirlemelidir. İdari kapsam olarak en düşük seviyede olan birimler, detaylı ve genellikle rutin işlemlerin yapıldığı yerlerdir. Bu yerler, muhtemelen kalıcı değere sahip belgelerin olduğu alanlardır. Schellenberg'in bu anlayışı, Alman Heinrich Otto Meisner/ Georg Wilhelm Sante – Wilhelm Rohr anlayışı ile aynıdır.[46] Belgelerin bilgilendirme değeri ise farklı kriterlerle yapılmak zorundadır. Schellenberg, belgenin üretildiği kaynaktan ziyade içinde bulundurdukları bilgiye önem verir. Zimmermann'ın "belgenin ilgi ve provenansı karar verici bir değerlendirme kriteri değildir" görüşüyle de paralellik arz eder. Hiç şüphe yok ki Schellenberg, arşivciye değerlendirme noktasında görev atfetmiş ve arşivcinin değerlendirme sürecinde rol sahibi olmasını savunmuştur. Belgelerin bir kısmının imha edilmesinin bilime hizmet olduğunu vurgulamıştır. Arşivcinin bu görevi, Jenkinson için mesleki ahlak olarak veya Georg Wilhelm Sante ile Wilhelm Rohr için pratik yeterlilik olarak ifade edilse de, Schellenberg bu şekilde düşünmez. Schellenberg, "kanıtsal" ve "bilgisel" değerler arasındaki ayrımı ortaya koyarak, Alman resmi ve hiyerarşik sistemine kendi sistemini dâhil etmeyi başarır. Böylece Schellenberg'in 1956'daki *Modern Archives* kitabı Amerikan, İngiliz ve Alman değerlendirme teorisinin sentezini zarifçe temsil etmektedir.[47] Schellenberg'ten bu yana arşiv teorisi üzerine devam eden tartışmalar, 1981 yılında Frank G. Burke'nin "The Future of Archival Theory in the United States/Amerika Birleşik Devletlerinde Arşiv Teorisinin Geleceği" adlı makalesiyle yeni bir boyut kazanmıştır. Makalede arşivcilerin kendi iş alanlarına yoğunlaşmaları gerektiği ifade edilmektedir. Bu tartışma, birkaç araştırmacı arasında dillendirilmiş olsa da, arşivciler arasında bilinmeyen bir anlaşmazlığa dönüşen teorileşme tartışmasını da başlatmıştır. John W. Roberts, bütün teorileri reddederek, arşivcinin dosyanın içine bakıp tarihsel bir değere sahip olup olmadığını anlayabileceğini savunmuştur. Bu basit düşünce yaklaşımı belgelerin değeri ko-

[46] Kolsrud, **a.y.**, s. 35.
[47] **A.e.**, s. 35-36.

nusunu gündeme taşımaktadır ki Roberts, bu değerin "pazar değeri" olduğunu savunmaktadır.[48] John W. Roberts'ın bu görüşü dogmatik olmakla beraber 1958 yılında Zimmermann'ın görüşüyle de uyuşmaktadır.

Her üç değerlendirme anlayışında da bazı arşivciler, değerlendirme sürecinin üç ölçekli olarak desteklenebileceğini söylemektedirler. İlk ölçüt, "Arşivlemenin Altın Kuralı" olarak Jenkinsoncı görüş olan hayati değeri olan belgelerin tutulmasıdır. Çünkü hayati değeri olan belgeler kurumların faaliyetlerine devam etmesini sağlamaktadır. Bu faaliyetler, bir kurumda belge üreticisinin kurumunun, otoritesinin, fonksiyonunun, politikalarının ve prosedürlerinin temel kanıtlayıcılarıdır. Bu düşünce, Britanya geleneğinde kendini kanıtlayan, ancak açıkça ampirik doğrulama gerektiren idari ve tarihsel değer arasında mantıklı bir bağlantı olduğunu varsayar.[49] Önerilen ikinci ölçüt, değerlendirmenin modern diplomatikanın öngördüğü anlayışlarla zenginleştirilebileceğidir. Diplomatika, arşivcilerin bir belgeyi fonlarıyla ilişkilendirmesinde, bir belgenin niçin üretildiği ile nasıl kullanılacağını ve belgenin hangi fonksiyonları destekleyeceğinin anlaşılmasında yardımcı olur. Son ölçüt ise, Grigg Raporu'nun 5 yıl ve 25 yıl kriterlerine göre değerlendirme yapmasında tavsiyede bulunur. 5 yıl kriteri, ilk değerlendirmenin belge üreticisi tarafından yapılmasını önerir. Dosyanın kapanmasından beş yıl sonra, idari değerin geniş bir şekilde anlaşılmasını tanımlayabilecek olan belge üreticiminin yapıldığı birimdir. Bu ilk değerlendirme (5 yıl kriteri) değerlendirme kavramının bir rehber olarak provenans ilkesini kullanarak uygulanması, dosyaların yarı aktif aşamalarından nihai amaca getirildiklerinde, saklama programları uygulamasının zamanlamasına kolayca uyarlanabilir. İkinci değerlendirme olan 25 yıl kriteri ise arşiv değerlendirmesinin, dosyanın kapanmasından yirmi beş yıl sonra hem idari hem de tarihi değeri belirlemek için belgeyi üreten birimle birlikte arşivci tarafından yapılmasını önerir. Belge üretimi, orijinal kullanım ve arşiv değerlendirmesi arasındaki zaman aralığı, ilk seri seçimin yeniden değerlendirilmesinde arşivciye yar-

[48] John W. Roberts, "Archival Theory: Much Ado About Shelving," **American Archivist**, Winter 1987, C. 50, S. 1, ss. 66-74; Akt: Kolsrud, "The Evolution of Basic Appraisal Principles - Some Comparative Observations," s. 36.

[49] Turner, "A Study of the Theory of Appraisal For Selection," s. 124-125.

dımcı olabilecek sürece tarihsel bir bakış açısı sağlar. Bu 25 yıl kriterine göre değerlendirmede, provenans ilkesi, koruma için seri seçimini daha da geliştirmek için çağdaş kroniklerin kullanımı ile birleştirilerek uygulanması tavsiye edilir.[50]

Özellikle dijital ortamda etkili değerlendirme, kayıt oluşturma ve kayıtların iş sınıflandırmasına dayanan iyi sistemlere bağlıdır. Değerlendirme, hangi kayıtların kalıcı olarak arşivde tutulacağına karar vermekle birlikte, kuruluşun iş ve hesap verebilirlik gereklilikleri karşılandıktan sonra imha olanları da kapsar.[51] Terry Eastwood'a göre elektronik belgelerin arşivsel değerlendirmesi dört farklı aktiviteden oluşmaktadır. Bu dört faaliyet (1) belgeler ve bağlamları hakkında bilgi toplamak ve analiz etmek, (2) üreticilerinin ve toplumunun ihtiyaçlarını karşılayacak kapasitelerini değerlendirmek, (3) bunların korunmasının fizibilitesini belirlemek ve yukarıdakilere dayanarak, (4) değerlendirme kararını vermektir.[52]

1.5. AVUSTRALYA KITASI GELENEKSEL ARŞİVSEL DEĞERLENDİRME ANLAYIŞI

Avustralya kıtası değerlendirme anlayışında, Yeni Zelanda'da makro değerlendirme ve Avustralya Belge süreci model tabanlı DIRKS (Designing and Implementing Recordkeeping Systems)[53] metodolojisi değerlendirmede etkin olarak kullanılan iki modeldir. Terry Cook ve Chris Hurley, Nazi savaş suçluları hakkındaki belgelerin imha edilmesi ile ilgili vaka çalışmalarında, değerlendirme amacının ve arşivlerin sorumluluğunun oldukça farklı olan "Heiner Meselesi" adını verdikleri anlayışlarını ortaya koymuşlardır. Bu görüşler, sırasıyla, makro değerlendirmeyi Terry Cook, belgelerin süreklilik modelini de Chris Hurley temsil etmektedir.[54] Yeni Zelanda'da değerlendirme uygulaması zor bir geçmişe sahiptir. 1985 yılından 2005/2006 yıllarına kadar Yeni Zelanda devlet sektörünün gelişimini şekillendiren birçok kamu yönetimi reformunun etkisi hissedilmektedir. 1980'li ve 1990'lı yıllar boyunca bu reformlar kamu

[50] **A.g.e.**, s. 125-126.
[51] O'Brien, **Appraisal and Disposal Policy**, s. 2.
[52] Terry Eastwood, "Appraising Digital Records for Long-Term Preservation," **Data Science Journal**, December 2004, C. 3, s. 204.
[53] The National Archives of Australia: "Designing and Implementing Recordkeeping Systems," (Çevrimiçi) http://www.naa.gov.au/recordkeeping/dirks/summary.html, 10 Haziran 2018.
[54] John Roberts, "Macroappraisal Kiwi Style: Reflections on the Impact and Future of Macroappraisal in New Zealand," **Archival Science**, December 2005, C. 5, S. 2-4, s. 197.

sektörünü küçültme, toplumsal sözleşme (kontraktualizm) ve kurum teorisi üzerine şekillenmiştir. Zamanın gereklerine uyumlu olarak, 1990'lı yıllar boyunca Yeni Zelanda Arşivleri, ticari amaçlarla yapılan, tartışılabilir bir değerlendirme hizmeti yürütmüştür. Böyle bir ortamda makro değerlendirme temelli bir yaklaşımı kullanmanın zorlukları başka yerlerde araştırılmıştır. Pek çok bakımdan, bu ticari amaçlarla yapılan bir yaklaşımın vurguladığı değerlendirme görüşü, planlı ve entegre bir çabadan ziyade, farklı bir piyasa tarafından verimli bir şekilde tutulan duyarlı bir hizmet olarak bilinmektedir. Bu, makro değerlendirme alanında da vurgulanan değerlendirme uygulamasına bir düzeyde titizlik ve proje yönetimi disiplini getirmiştir. Ancak, değerlendirmenin operasyonel faaliyetinin etkinliği açısından herhangi bir fayda, faaliyetin bir bütün olarak etkili, koordine ve iyi hedeflenmiş olmasını sağlamakla ilgili sorunlardan daha ağır basmıştır. 2004 yılının Haziran ayında dış kaynak kullanımından vazgeçilmiş ve Yeni Zelanda arşivleri, değerlendirme için yeni bir strateji geliştirme konusunda pozisyon almıştır. Yeni Zelanda Arşivleri, 2003-2004 yıllık raporu, değerlendirme alanında daha stratejik bir şekilde faaliyet gösterme niyetine dikkat çekmiş, 2003-2004 hükümet kayıtları için daha etkili bir imha reformuna doğru önemli adımlar atmıştır. Belgelerin imhası, bu noktaya kadar, büyük ölçüde reaktifti ve kurumların kendilerini fazla evraktan kurtarma motivasyonuna dayalıydı. Bu yaklaşım, değerlendirme için sunulan belgeler için yüksek düzeyde imha kararları vermiştir. Fakat uygulayıcılar tarafından baştan savma yapıldığı için kötü sonuçlanmıştır. En değerli devlet evrakının Yeni Zelanda Arşivine aktarılmak üzere değerlendirilip değerlendirilmediği sorusu cevapsız kalmıştır. Bu sorunu çözmek için günümüzde iki strateji benimsenmektedir:[55]

1. Proaktif değerlendirme projeleri için kurumların önceliklendirilmesi: Bu stratejide kurumun idari pozisyonu ve hâlihazırda sahip olduğu imha kapsamı dâhil olmak üzere bir dizi kritere dayanmaktadır.
2. Önceliklendirme sonrası: Kurumların yetkili kişileriyle görüşmeler yapılmış ve bu görüşmeler 2004-2005 yılında başlamış olan temel değerlendirme projelerinin altyapısını hazırlamıştır. Bu projeler, daha önce bugüne kadar değerlendirmelere konu olan fazla belgelerin ayrı bloklar yerine tüm kurumlara ait

[55] **A.e.**, s. 187-188.

> belgelerin bir bütün halinde imha ihtiyaçlarını karşılaması planlanmıştır. Bu yaklaşım, 1991'den beri sağlanan fırsat maliyeti (dış kaynak kullanımı) değerlendirme hizmetinin durdurulmasını gerekli kılmış ve Hükümet, 2004 bütçesinde, bu değerlendirmeyi ücretlendiren değerlendirmelerden uzak tutmak için finansman sağlamıştır.[56]

Yukarıda belirtilen iki yaklaşım, hükümet genelinde nesnel ölçütlere dayanan önceliklendirme ve kurum üst yönetimiyle kararlaştırılan kapsamlı, planlı değerlendirme projeleri, Kanada Kütüphane ve Arşivleri'nde -Devlet Arşivleri- (Library and Archives Canada, LAC) uygulandığı gibi, makro-denetlemenin bilindik özellikleridir. Bununla birlikte, bu stratejilerin her ikisi de "uygulama" boyutunun makro değerlendirme boyutlarıdır. Uygulanacakları ölçütler belirlediklerinden ve sahip oldukları değerin (belgelerin, belge üreticilerinin veya belge yönetimi ortamının diğer özelliklerinin) nasıl anlaşıldığını belirlediklerinden, uygulamalarını destekleyen teorik sorular daha temeldir. Bu bağlamda, Avustralya belge sürekliliği yaklaşımı, Yeni Zelanda'daki değerlendirme uygulamasına makro değerlendirmeye göre daha büyük bir etki yaratmıştır.[57]

[56] Archives New Zealand, **Annual Report 2004**, Wellington, Archives New Zealand, 2004, ss. 14-15; Akt: Roberts, "Macroappraisal Kiwi Style…..," s. 188.

[57] Roberts, **a.g.e.**, s. 188.

İKİNCİ BÖLÜM

ELEKTRONİK BELGE YÖNETİM SİSTEMİ MODELLERİ

2.1. ELEKTRONİK BELGE YÖNETİM MODELLERİ

Modern belgelerin arşivsel niteliği bakımından günümüz arşivsel uygulama eğilimleri arasında yaklaşım farklılıkları vardır. Bu farklılıklar özellikle Amerika, daha düşük düzeyde olmak üzere Avustralya temelinde yoğunluk kazanmış durumdadır. Bu farklılıklar temelde; arşivler ve belgeler (günümüz Osmanlı Türkçesi ile yazılmış belgeler gibi), kamu belgeleri ve kamu haricindeki belgeler, güncel belgeler ve tarihsel belgeler bağlamında görülmektedir.[1] Bu yaklaşım farklılıkları çeşitli belge yönetim modellerini de beraberinde getirmiştir. Dünyada yaygın olan üç temel belge yönetimi modelinden söz edilebilir. Bunlar;

- Avrupa İdari Modeli – Arşivsel Model (European Administrative Model – Archival Model)
- Anglo-Sakson Modeli – Yaşam Döngüsü Modeli (Anglo-Saxon Model – Lifecycle Model)
- Avustralya Modeli – Belge Sürekliliği Modeli (Australian Model – Records Continuum)'dir.

Bu modellerin incelenmesi, arşivsel değerlendirme ve arşiv imha teorileri açısından anlamlıdır. Dünyadaki arşiv uygulamalarına bağlı olarak ortaya çıkan bu farklılıklar, birden fazla arşiv imha teorisinin ortaya çıkmasının önünü açmıştır. Farklı modellere bağlı olarak farklı imha teorileri kurgulamak yerine, yaygın olan ve yukarıda da ifade edilen üç modeldeki kurguları incelemek ve buna göre elektronik ortamdaki belgeler için arşiv imha teorisinden söz etmek yerinde olacaktır. Sistem özellikleri bakımından bu modellerin değerlendirilmesi elektronik ortamdaki imha konusunu daha kapsamlı bir biçimde tanımlama olanağı verecektir. Bu modeller alt başlıklar halinde aşağıda verilmiştir.

[1] Frank Upward, "Structuring the Records Continuum - Part One: Postcustodial Principles and Properties," **Archives & Manuscripts**, 1996, C. 24, S. 2, s. 3.

2.2. AVRUPA İDARİ MODELİ – ARŞİVSEL MODEL

Avrupa arşivsel yaklaşımında belge ile doküman arasında bir ayrım söz konusu değildir. Avrupa dillerinin birçoğunda belge kelimesinin kullanımı sınırlıdır. Dokümanın kullanımı ise yaygındır. Bu sebeple doküman, Avrupa idari modelde olduğu gibi araştırmanın bu kısmında aynı şekilde kullanılacak ve belgeyle aynı anlamı taşıyacaktır. İdari modelde, doküman yönetimi kuralları, yönetimsel ihtiyaçlarla belirlenmiştir ve idari personel tarafından yönetilmektedir. Avrupa anlayışında ayrıca belge yönetim fonksiyonu da yoktur. Sadece arşivsel fonksiyon vardır.

Verilen bilgiler çerçevesinde, Avrupa idari modelinde dokümanın yaşam döngüsü iki aşamadan meydana gelmektedir. Bunlar; güncel dokümanlar ve arşivlenmiş dokümanlardır. Güncel (aktif) dokümanlar kullanıcılar (ilgili idari personel) tarafından üretilip yönetilir. Zaman tanımı belirgin değildir ve saklama planları yoktur. Arşivlenmiş (aktif olmayan) dokümanlar arşivsel değerlendirmeye kadar tutulur. Değerlendirme işlemi arşivciler tarafından yapılır. Değerlendirme sonucunda süresiz saklanılması gereken dokümanlar arşivlere gönderilir.[2]

İnternet ve teknolojinin gelişimine paralel olarak Avrupa arşiv modeli de yeniliklere göre yeniden şekillenmiştir. Avrupa Komisyonu tarafından 1996 yılında üzerinde çalışılmaya başlanan MoReq (model requirements for the management of electronic records) elektronik ortamdaki belgelerin yönetimi için kapsamlı ve gerekli teknik özelliklerin uygulandığı bir model olarak geliştirilmiştir. Çalışma sonucunda 2001 yılında MoReq'in ilk sürümü diyebileceğimiz model yayınlanmıştır. Bu ilk sürüm, Avrupa'nın birçok yerinde kabul edilebilir kullanıma sahip olmasının yanı sıra Avrupa dışında da kabul görmüştür. Ancak gelişen teknoloji MoReq'in artık ihtiyaçları yeterince karşılamadığını göstermiştir. Koruma modülünün olmaması, teknik özelliklere uygunluğun değerlendirilebileceği testlerin yapılamaması gibi bazı eksikler MoReq'in

[2] Lucia Stefan, "The Three Records Management Models," (Çevrimiçi) https://www.slideshare.net/Stelucia/records-management-models-4849738, 9 Nisan 2018.

ilk sürümünün güncellenmesini gerektirmiştir. Bunun için 2005 yılında başlayan çalışmalar 2008 yılında sonuç vermiş ve böylelikle MoReq2 yayınlanmıştır.[3] Günümüzde Avrupa arşivsel modeli olarak kullanılan ve MoReq2'nin devamı olan MoReq2010 Avrupa Birliği ülkeleri için ortak bir model olarak 2010 yılında kullanıma elverişli hale getirilmiştir. Bu yıldan itibaren Avrupa Birliği ülkelerinin küçük ve büyük çaptaki tüm kurum ve kuruluşlarında kullanılmaya başlanmıştır.

MoReq,[4] MoReq2 ve MoReq2010'un anlaşılması günümüz Avrupa arşivsel modelini yansıtması açısından değerlidir. Daha önce de ifade edildiği gibi Avrupa arşivsel modelde belge kavramı yerine doküman kavramı tercih edilmektedir. Fakat MoReq ve revizyonu devamındaki dokümanlarda, elektronik doküman yönetim sistemleri (EDYS) yerine elektronik belge yönetim sistemleri (EBYS) kullanılmaktadır. EDYS'lerin EBYS'lerle büyük oranda örtüştüğünün görülmesi, EDYS'lerin bazı eksiklerinin EBYS ile çözülebilmesi, Avrupa'nın EDYS yerine EBYS kullanmasını anlamlı kılmıştır.[5]

İlk sürüm MoReq,[6] Avrupa için bilgisayar sistemlerindeki elektronik belgelerin yönetilmesini sağlamada yardımcı olmuştur.* Söz konusu özellikler şu şekilde sıralanabilir:[7]

- Evrensel kapsam ve uygulama özelliği,
- Farklı birçok dile uyumluluk özelliği ve
- Genel geçer standardizasyon özelliği.

---

[3] European Communities, **Model Requirements for the Management of Electronic Records (MoReq2),** Update and Extension, France, 2008, s. 9, (Çevrimiçi) https://www.project-consult.de/Files/MoReq2_body_v1_0.pdf, 29 Ekim 2018.

[4] MoReq bu çalışma kapsamında her üç sürümü tanımlayan bir kavram olarak görülmektedir. Kavramın ilk sürümle karıştırılmaması için MoReq kavramı yerine "ilk sürüm" olarak adlandırılmıştır.

[5] European Communities, **MoReq2**, s. 109.

[6] European Communities, **MoReq Specification-Model Requirements for the Management of Electronic Records**, Bruxelles- Luxembourg, CECA-CEE-CEEA, 2001, (Çevrimiçi) https://ec.europa.eu/idabc/servlets/Doc1faf.pdf?id=16847, 31 Ekim 2018.

* MoReq'ten önce Avrupa'daki ülkelerden bir kısmı kendi belge yönetim standardına sahipti. Bu ülkeler MoReq'in geliştirilmesiyle birlikte sahip olduğu karakteristik özellikleri sebebiyle MoReq'i benimsemişlerdir.

[7] DLM Forum Foundation, **MoReq2010®: Modular Requirements for Records Systems — Volume 1: Core Services & Plug-in Modules**, 2011, s. 16, (Çevrimiçi) http://moreq2010.eu/ , 31 Ocak 2019.

MoReq'in ilk sürümü, bölümlerin ve gereksinimlerin nasıl eklenmesi, düzenlenmesi ve silinmesi ve bunu yaparken gereklilikler dâhilinde karşılıklı referanslama gibi konuların yönetilmesi hakkında kılavuz niteliğindeki bilgileri içeriyordu.[8]

2005 yılında DLM Forum'un MoReq güncellenmesi ve genişletilmesi amacını taşıyan çalışması sonucunda MoReq2, 2008 yılında yayınlanmış oldu. MoReq2'nin önemli bir özelliği belge yönetim sistemlerini test edebilmesi ve test sonucunda sertifika vermesidir. Sistem tedarikçileri, hizmetlerini bir MoReq2 test merkezinde test etme ve ürünlerinin spesifikasyona uygun olduğu konusunda bağımsız bir sertifika alabilme olanağı buldular. MoReq2, test etmeyi ve sertifikalandırmayı desteklemek için, gereklilikler dâhilinde bir üstveri modelini sunduğu gibi XML şemasını hatta farklı ürün ve uygulamalar arasında yaygın olan bir alma/gönderme formatı tanımlamayı da başlatmıştır. MoReq2'nin test ve sertifikasyon programının tanıtımı, MoReq gerekliliklerinin benimsenmesi için gerekli olan titizlik ve kalite güvencesini ortaya koyan son derece önemli ve aşamalı bir adım olması açısından anlam kazandı. Bunun sonucunda, yüksek kaliteli ürünlere sahip sistem tedarikçileri bağımsız doğrulama ve uygunluk kanıtı elde edebilirken, tüketiciler de tanınmış kalite standartlarını karşılayan bir dizi ürün arasından seçim yapabilir hale geldiler.[9] Bunların yanında MoReq2'nin getirdiği olumsuz sonuçlar da görülmüş oldu. Eğer ürünler MoReq2'ye göre test edilip sertifikalandırılmışsa, bu ürünlerin yerel düzeyde getirdiği zorluklar nasıl aşılabilirdi? Daha önce test edilmiş ve uygun şekilde onaylanmış bir ortak yazılım ürününün tedarikçisi, uygulamada daha sonraki eklemeler, kurumsal düzeyde bireysel gereksinimlere göre değişiklikler veya silme işlemlerini nasıl öngörebilir? Karmaşık olduğu değerlendirilen diğer nokta da sisteme ekleme, değiştirme ve silme gibi durumlardan nasıl emin olunabileceği idi? Sistemdeki bu tereddütler, üç yılda bir yapılan DLM Forum'un 2008 yılında yapılan Fransa Toulouse'daki konferansta DLM Forum'un bir alt komisyonu olarak MoReq Governance Board'un (MoReq Denetleme Kurulu) oluşturulmasını sağladı. Kurulun görevi MoReq'in tüm açılardan ele alınmasını sağlamaktı.

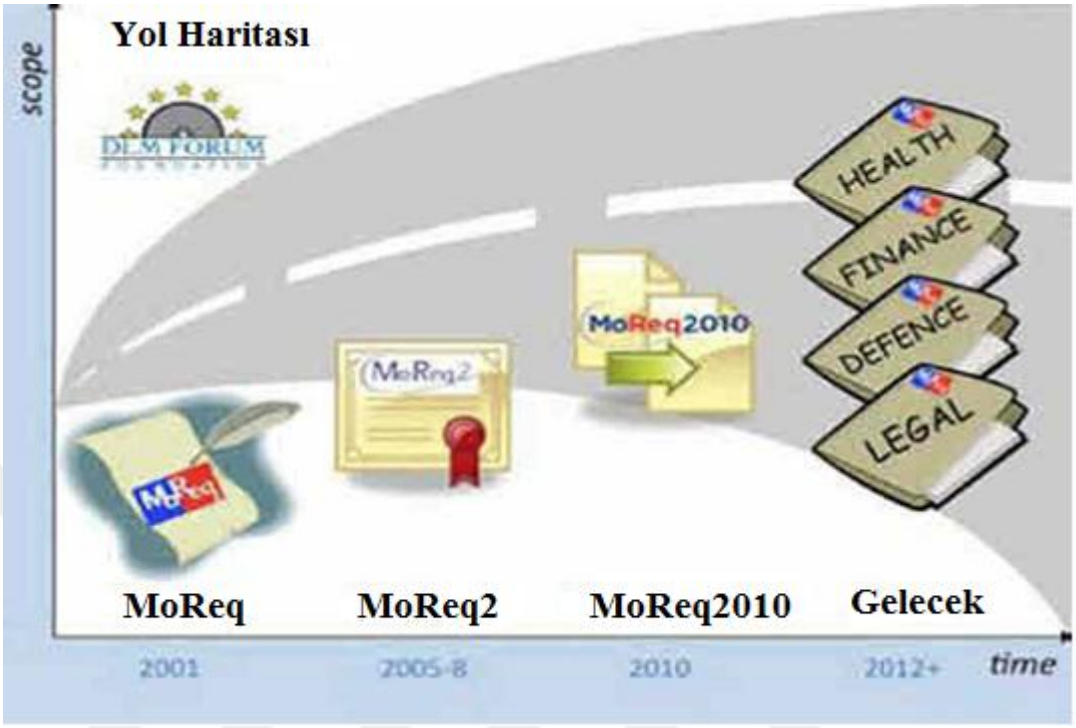
[8] **A.y.**
[9] DLM Forum Foundation, **MoReq2010**, s. 16-17.

Kurul, bunun yanı sıra özellikle aşağıda sıralanan maddeler üzerinde de çalışmalara başladı:[10]

- Sistem için sürekli bir koruma sağlamak, MoReq için bir yol haritası belirlemek ve sistemin sonraki sürümlerini planlamak,
- Sistemin çeşitli dillere çevrilmesini yönetmek, uygun çevirileri doğrulamak ve çeviri için MoReq rehberi hazırlamak,
- Belirlenen test merkezlerinde MoReq ile karşılaştırmalı yazılım testleri için hibe programları düzenlemek,
- Belirlenen test merkezlerinde yazılım ürünlerinin test edilmesini ve sertifikalandırılmasını denetlemek,
- Destekleyici kılavuzlar ve eğitimsel materyallerle eğitim ve çalıştaylar düzenleyerek sistemi anlamlı hale getirmek ve
- Aktif olarak MoReq'i pazarlamak, vaka çalışmalarını derlemek ve MoReq adaptasyonunu teşvik etmek, böylelikle MoReq markasını korumak.

[10] **A.y.**

Şekil 2.1: MoReq Denetleme Kurulu'nun Yol Haritası



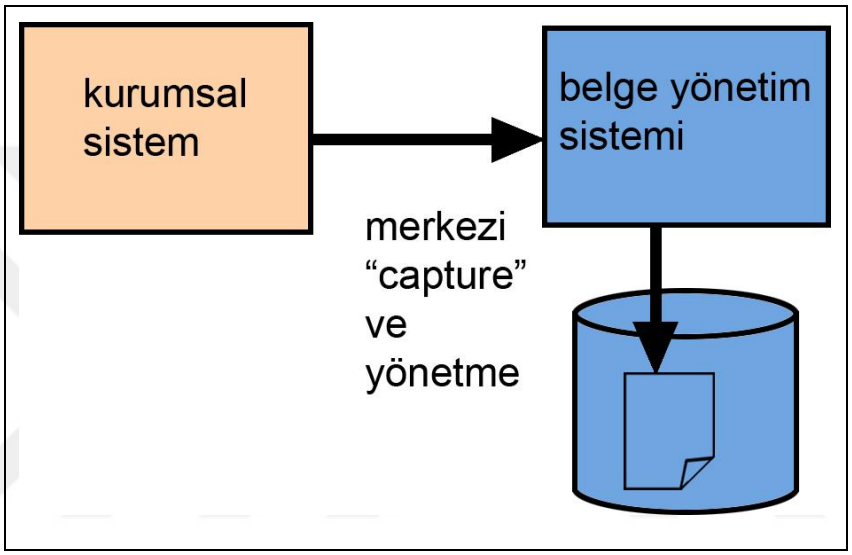
(**Kaynak:** DLM Forum Foundation: MoReq2010®: Modular Requirements for Records Systems — Volume 1: Core Services & Plug-in Modules, 2011, s.17, (Çevrimiçi) http://moreq2010.eu/ , 31 Ocak 2019.)

MoReq'in yol haritası (Şekil 2.1) geleneksel belge yönetimi için kriterler sunmuş olduğunu göstermektedir. Bu da sistemin daha çok ofis veya büro tabanlı olarak işlev gördüğünü doğrulamaktadır. Yol haritasında, elektronik belge yönetim sistemi ve kurumsal içerik yönetimi önemlidir. Fakat tıp, eczacılık, hukuk ve finans hizmetleri gibi alanlarda söz konusu sistemin uygulanabilirliği kısıtlıdır. Bu alanlar tipik olarak kendi sektörleri içindeki özelliklerine veya mevzuata göre yönetilmektedir. Bu sebeple kendi değerlerini yansıtacak belge yönetim kriterlerini benimsemişlerdir/benimseyeceklerdir. MoReq'in bu alanlara yönelik çözümler sunması sistemin varlığı için değerli olacaktı.[11] Kurulu'nun tanımladığı eğilimlerden bir diğeri de belge yönetim sistemi

[11] DLM Forum Foundation, **MoReq2010**, s. 17.

tasarımında artan farklılıklardı. Kavramsal olarak, MoReq® orijinal olarak, bir kuruluşun bağımsız belge yönetim sisteminin, kullanıcılar ve diğer iş sistemleri de dâhil olmak üzere çeşitli harici kaynaklardan kendi veri deposuna kayıtları çekeceği tek bir merkezi depo modeline dayanıyordu. Bu geleneksel mimari Şekil 2.2'de gösterilmiştir.[12]

Şekil 2.2: Merkezi Belge Sağlama ve Yönetme Sistemi

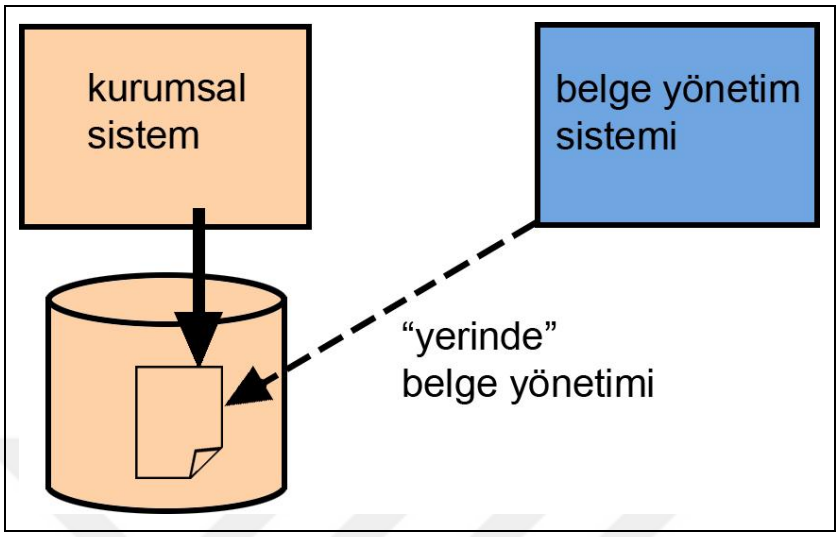


(**Kaynak:** DLM Forum Foundation: MoReq2010®: Modular Requirements for Records Systems — Volume 1: Core Services & Plug-in Modules, 2011, s.18)

Şekil 2.2'de geleneksel bir belge yönetim sisteminde kurumsal sistemlerden alınmış belgelerin yanı sıra belge yönetim sistemi tarafından kontrol edilen bir arşiv yönetim merkezi bulunmaktadır. MoReq Denetim Kurulu'nun bunun için geliştirmiş olduğu uyumlu, genişleyebilen ve tercih edilebilir mimari yapılar çözüm üretebilir niteliktedir. Ortaya çıkan modellerden biri (Şekil 2.3), kendi merkezileştirilmiş havuzuna kopyalamaktan ziyade, belgeleri kendi üretildikleri iş sistemlerinde yöneten belge yönetimi depolama sistemidir.

[12] **A.g.e.**, s. 18.

Şekil 2.3: Yerinde Belge Yönetimi Sistemi

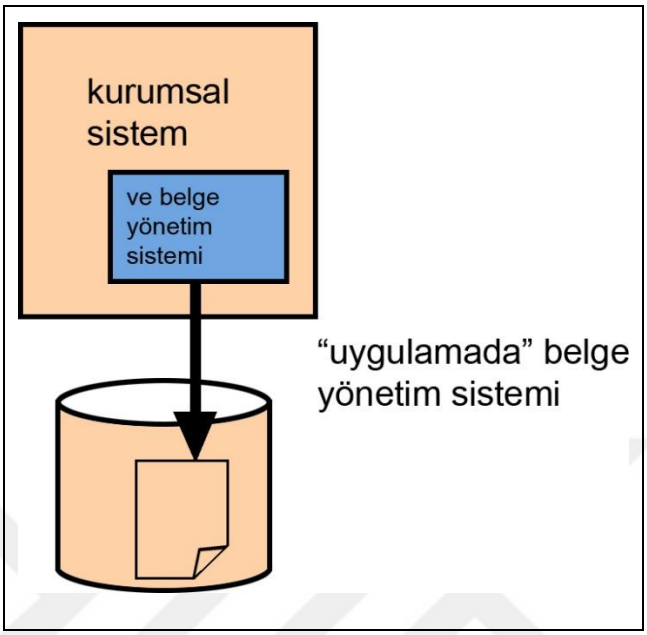


(**Kaynak:** DLM Forum Foundation: MoReq2010®: Modular Requirements for Records Systems — Volume 1: Core Services & Plug-in Modules, 2011, s.18)

Şekil 2.3'te alternatif bir mimari olarak, kurumsal sistemlerin sahip olduğu bilgi ve belgeyi, (bu bilgi ve belgeyi yerinde tutmak şartıyla) belge yönetim sisteminin kurumsal kontrol ve süreç uygulamalarına izin vermesidir. Bir başka olası mimari ise, kayıt kontrollerinin, kurumsal sistemin kendisi tarafından benimsenmesidir. Böyle bir kurumsal sistem, aynı zamanda, belirli bir kurumsal sistem tarafından tutulan veya üretilen belirli bir kayıt kümesini yöneten bir kayıt sistemi olarak işlev görür.

Uygulamanın kendisinin bizzat belge yönetim sistemi olduğu bu yaklaşım, "uygulamada" belge yönetimi olarak da tanımlanabilir. Belge yönetimi modeli olarak kurumsal sistem Şekil 2.4'te gösterilmiştir.

Şekil 2.4: Uygulamada Belge Yönetim Sistemi



(**Kaynak:** DLM Forum Foundation: MoReq2010®: Modular Requirements for Records Systems — Volume 1: Core Services & Plug-in Modules, 2011, s. 19)

Şekil 2.4'te belge yönetimi kontrolleri ve süreçleri basit, esnek ve daha iyi anlaşıldıkça, kurumsal sistemlerin en azından kendi ürettikleri kurumsal kayıtları için belge yönetim sistemleri haline gelmeleri giderek daha fazla mümkün olacaktır. MoReq yol haritasında, ayrıca küçük ve büyük bütün bilgi yönetim sistemlerine uygun ve ölçeklendirilebilir ihtiyaçları tanımlama amacıyla hedefler belirlenmiştir. MoReq2 ilk sürüm'e göre fonksiyonel özelliklerini iki katına çıkarmıştır. Fakat MoReq'in artarda basımları aynı gelişim randımanı sağlamadı. Özellikle daha küçük ölçekli kurum ve kuruluşlarda ciddi engellerin olması MoReq'in 2009 yılında geliştirilmesi gereken iki aşamasının daha olduğunu ve bu aşamaların modelin gelecek aşamaları olarak hedeflenmesi gereğini ortaya koydu. Bunlar;[13]

- Kısa vadeli olan birinci aşama için, 2010 yılında başlanmak üzere MoReq gerekliliklerini, modüler çizgiler boyunca yeniden düzenleyecek, mümkün olduğunda basitleştirecek ve alternatif belge yönetim sistemleri mimarileri için destek sunacak bir sistem içyapısı projesinin başlatılması ve

[13] **A.g.e.**, s. 19.

- Uzun vadeli olan bu aşamanın 2012 yılında başlamak üzere, alanında yetkin uzmanlarla daha modüler bir yaklaşımın sağladığı esnekliğe dayanarak insan çabasının görüldüğü bütün alanlara uygulanabilir bir MoReq yapısı sunulması.

Bu hedeflerin ilki 2010 yılında DLM Forum Foundation AGM tarafından gerçekleşmiş oldu. Bu da MoReq2010'un resmi olarak başlatılması açısından önemli bir adım sayılmaktadır.

MoReq2010 ile "model gereksinimleri kavramı" "modüler gereksinimler kavramı" ile yer değiştirmiş oldu. MoReq2010 belge yönetimi öncelikle Avrupa'da ve daha sonrası için dünyada daha iyi tanınması, anlaşılması ve benimsenmesi için gelecek teknolojilerle bağ kurması açısından önemlidir.[14]

MoReq2010'un hazırlanması sistem ve süreçlerdeki varlıkların tanımlanmasını gerektirmektedir. Dolayısıyla her kurum ve birey belgelere sahip oldukları kadar bu belgelerin kullanıcıları olarak da varlık sahibidirler. Kurumlar ve bireyler var olduklarının bir kanıtı olarak belgeleri yeterince korumak ve güvenliğini sağlamak zorundadırlar. Bu belgelerin taşıdıkları bilgiler ölçeğinde korunup korunmayacağına karar verilmektedir. Bireysel olarak pasaport, kimlik kartları, sürücü belgeleri gibi belgeler korunması gereken belgeler olarak düşünüldüğünde, alışveriş listeleri, müsvedde gibi bilgi taşıyan belgeler korunması ve güvenliğinin sağlanması gerekmeyen belgelerdir. Bu noktada bireylere ilişkin bilgiler her zaman belge niteliğinde değildir. Bu ayrım bireyler için olduğu gibi kurumsal anlamda da aynı niteliktedir. Bu sebeple, kurumsal belgeler, kurumsal bilginin bir alt kümesi olan başka bir fonksiyonu yerine getirmektedir. Çünkü belgeler, kurumsal bilgi içinde öneme haiz görülen bilgilerin çekilmesi ve belgelere yansıtılması gerekli görülen bilgilerdir.[15] Kurumsal bilgi ve belge ayrımında gereksiz bilgi, yani belgelemeye ihtiyaç duyulmayan bilginin kurumsal bilgi alanlarında yer tutması problem olarak görülmektedir. Personelin kurumsal bilgiler içinde hangi bilginin önemli olduğunu anlamlandırması veya hukuki bir fiil olarak çağrılması veya bilgi edinme hakkı çerçevesinde sunulması noktasında istendiğinde

[14] **A.g.e.**, s. 20.
[15] DLM Forum Foundation, **MoReq2010**, s. 20-21.

bütün bunların kurumlara ve dolayısıyla personele ağır yük getirmesi bu problemi göstermektedir. Kurumlardaki istenmeyen bilginin azaltılması, dolayısıyla belge süreç ve sistemlerinin uygulanabilirliğini tartışmak ve buna bağlı olarak süreç ve sistemlerin anlamlandırılması gerekmektedir. Bu anlayışla hazırlanan MoReq2010'un belge yönetim süreç ve sistemlerini bilmek önemlidir.

MoReq2010, belge yönetim süreçlerini ISO 15489 (ISO 15489-1: 2001: Information and documentation – Records management – Part 1: General)'da belirtilen listeye göre uyarlamaktadır. Buna göre belge yönetim sürecinde belirlenmesi gereken en temel unsur, hangi bilgilerin belge gibi tanımlanmasının bilinmesidir.[16] Bunun bilinmesi her ne kadar elektronik ortamda olmuş olsa da bir yapıya sahip olmasını gerektirir. Bu yapı, belgelerin dokümanter yapısı (üretilme koşullarının bilinmesi, taşıyıcı ortamın sürekli kullanımı ve otantikliklerinin korunması) olarak bilinmektedir.[17] Tanımlanan diğer unsurlar şu şekildedir:[18]

- Belgelerin ne kadar saklanacağının belirlenmesi;
- Belgelerin üretilmesi ve kaydedilmesi;
- Belgelerin sınıflandırılması;
- Belgelerin depolanması ve kullanılması;
- Belgelere erişim kontrolünün sağlanması;
- Belgelerin takip edilmesi/izlenmesi;
- Belgelerin imhası ve
- Belge yönetim süreçlerinin belgelenmesidir.

ISO 15489, belge yönetim sistemi kullanan bir kurumun bu süreçleri uygulamasını önermektedir. Söz konusu standart ayrıca, standart bir belge yönetim sistemini, belgeleri saklayan, yöneten ve belgelere erişim sağlayan bir bilgi sistemi olarak tanımlar.

[16] **A.g.e.**, s. 22.

[17] Niyazi Çiçek, "Belgelerin Dokümanter Yapısı," **Arşiv Dünyası,** S. 13, 2012, s. 37.
[18] DLM Forum Foundation, **MoReq2010,** s. 22.

MoReq2010, bir belge yönetim sistemi için özellikle aşamalı olarak gerekliliklerin tanımlandığı teknik bir şartname niteliği taşır. ISO 15489'un sunduğu belge yönetim süreç tanımlamalarının ötesinde daha geniş çerçevede bu süreçlerin ayrıntılı uygulanmasını olanaklı kılar. MoReq2010 uyumlu olduğu belge sistemleri (MoReq2010 compliant records system [MCRS]) ile birlikte çalışabilirlik potansiyeline sahiptir. Bir MCRS sadece kendi varlıklarını ve kendi süreçlerini anlamakla kalmaz, bunları başka bir MCRS tarafından anlaşılabilen standart bir formata da aktarabilir. Birlikte çalışabilirlik belge yönetiminde, bir belge yönetim sisteminin kullanması anlamında önemlidir. Kurumlar günümüzde sahip oldukları teknolojileri 3-5 yılda bir yenilemektedir. Ancak, belgeler genellikle 3-5 yıldan daha uzun tutulmaktadır. Örneğin bir kurum 75 yıl tutması gereken belgelere sahipse, 75 yılın sonunda belge yönetim sistemleri arasında muhtemelen 15-25 kere belgeleri yeni teknolojilerle çalıştırabilecek dönüşümü sağlamak gerekliliği ile karşı karşıya kalacaktır. Eğer dönüşüm sürecinde belgeyle ilgili bilgi bağlamında bazı kayıplar yaşanırsa, 15-25 kez gerçekleşecek dönüşüm sürecinden sonra yaşanacak kayıplar belgenin bütünlüğü üzerinde ağır tahribatlara sebebiyet verebilir. Belgelerin dönüştürülmesi, MCRS'in ana fonksiyon hizmetlerinin bir parçası değildir. Ancak her MCRS sahip olduğu bilgiyi MoReq2010'un ortak XML dışa aktarma formatına uygun hale getirmek zorundadır.[19]

MoReq2010'a göre belgelerin doğası, elektronik ortamdaki bilgi varlıklarının, bir belge olarak yönetilebilir olmasıyla açıklanmaktadır. Süreç ve sistemler bağlamında bir belgede ortak bir anlayışın sergilenebilmesi için tam bir tanımının yapılması gerekir. ISO 15489 bir belgeyi, hukuki zorunluluklar gereği ya da işin yürütülmesi sırasında bir kurum veya kişi tarafından kanıt ve bilgi olarak oluşturulan, alınan ve muhafaza edilen bilgiler[20] olarak tanımlamaktadır. Geçmişte her ne kadar bilgi, sadece kâğıt ortamda olmuş olsa da, kâğıt ortamdaki bilginin yerini büyük oranda artık elektronik bilgiler almıştır. Elektronik ortamdaki bilgi her ne kadar kâğıdın yerini alsa da mevcut belge ve fiziksel kayıtlar varlığını sürdürecek ve buna yönelik sistemlere de ihtiyaç olacaktır.

[19] **A.g.e.**, s. 22-23.

[20] International Organization for Standardization (ISO), **15489-1: Information and Documentation – Records Management – Part 1: General,** 2001, 3.15.

Fiziksel olsun elektronik olsun belgenin sahip olduğu bazı karakteristik özellikleri vardır. Bu özellikler hem fiziksel hem de elektronik ortam için önemlidir. Bunlar;[21]

- Gerçeklik: Belgenin içerdiği bilginin ne olduğu ve belgeyi üreten kişinin belgeyi ne amaçla ürettiğidir.
- Güvenilirlik: Belgenin içerdiği bilginin tam olması ve sahip olduğu konuyu yansıtmasıdır.
- Bütünlük: Belgenin tamam olması ve değiştirilmemesidir. Bir diğer ifadeyle elektronik belgenin tanımsal ve fiziksel bütünlüğünün korunmasıdır.[22]
- Kullanılabilirlik: Belgenin bir yerinin olması, erişilebilir olması, sunulabilir olması ve yorumlanabilir olmasıdır.

ISO 15489'da belirtildiği gibi belgeler, işlemler veya olayın ilgili olduğu zaman ya da bir süre sonra, işlemin gerçekleştirilmesi için iş içinde rutin olarak kullanılan araçlar veya gerçekler hakkında doğrudan bilgiye sahip olan kişiler tarafından oluşturulmalıdır.[23] Bu durum belgelerin iki yolla üretildiğini göstermektedir. Birincisi, belgeler bireylerce üretilmektedir. İkinci ise, belgelerin araçlarla üretilmesidir. MoReq2010'da insanlar ve iş sistemleri, bir belge yönetim sisteminin kullanıcıları olarak görülmektedir ve bunlar belge üretmeye yetkilidirler. Bu nedenle MCRS çeşitli arayüzler geliştirmiştir. Bunlar; insanlar için arayüz, iş sistemleri için arayüzler veya her ikisi için hazırlanan arayüzlerdir.[24]

MoReq2010'da varlıklar ve bu varlıkların ilişkili olduğu hizmetler vardır. MoReq2010 ile uyumlu bir belge yönetim sistemi, belgeleri varlıklar olarak yönetir. MoReq'te, belgeler sadece bir varlık türü olarak tanımlanmaktadır. Varlık türü olarak belgeler haricinde sistem içinde tanımlanmış birçok varlık grubu söz konusudur. Bu da belgeler haricinde belge gibi bir varlık türü olarak ifade edilebilecek çok sayıda bilgi kaynağı olduğunu göstermektedir. Bu varlık türleri ise şu şekildedir: Kümelenme (aggregation), sınıf, bileşenler, içeriksel üstveri öğesi tanımı, tasviye, tasviye (saklama)

[21] **A.y.**, 3.15.

[22] Hamza Kandur, **Elektronik Belge Yönetimi Sistem Kriterleri Referans Modeli (v.2.0),** 2. bs., Ankara, Devlet Arşivleri Genel Müdürlüğü Cumhuriyet Arşivi Daire Başkanlığı, 2006, s. 55.

[23] **A.g.e.**, 7.2.3.

[24] DLM Forum Foundation, **MoReq2010**, s. 24.

planı, varlık türü, işlem, fonksiyon tanımı, grup, üstveri öğesi tanımı, belge, rol, hizmet, şablon ve kullanıcı olmak üzere 16 tür bulunmaktadır.[25] Bu varlık türleri arasında kümelenme (aggregation) kavramı yeni bir kavram olarak karşımıza çıkmaktadır. Sistemde hem sınıf hem de aggregation kavramlarının bulunması söz konusu iki kavram arasındaki farklılığın ne olduğu sorusunun cevabının verilmesini gerektirmektedir. Öncelikle, fiil olarak tanımı yapılan ve kümelenme olarak ifade edilen bu kavram (aggregation), "parçaların aynı veya farklı veri yapısına sahip olabileceği ve veri yapısının ilgili bileşik türün temel parçası olabileceği yapılanmış bileşenler topluluğu"[26] olarak açıklanmaktadır. Uluslararası Arşiv Konseyi (International Council on Archives-ICA) ise aggregation kavramını "elektronik belgelerin kümelenmeleri, birleştirildiğinde, örneğin bir dosya gibi tekil bir elektronik belge nesnesinin üstünde bir seviyede bulunabilecek ilgili elektronik belge varlıklarının birikimidir. Kümelenmeler, ilgili elektronik belgeler ile oluşturuldukları sistem veya ortam arasında var olan ve üstveri bağlantılarında ve / veya diğer ilişkilerinde kaydedilmiş olan ilişkileri temsil eder".[27] şeklinde tanımlanmıştır.

ICA, elektronik belgelerin kümelenmelerinin, paylaşılan özellikler veya nitelikler gibi ilişkileri veya ilgili elektronik belgeler arasında sıralı ilişkilerin varlığını yansıtabileceğini de ifade etmektedir. Ayrıca belirli bir kümelenmenin elektronik belgeleri arasındaki ilişkinin niteliği, amacı ve yapısı gibi faktörlere, belgelerin içeriği ve formatına bağlı olarak değiştiğini açıklamıştır.[28] ICA kümelenmeyi (aggregation" aşağıda verilen şekildeki yerine göre belirtmektedir.[29]

[25] **A.g.e.**, s. 249-264.

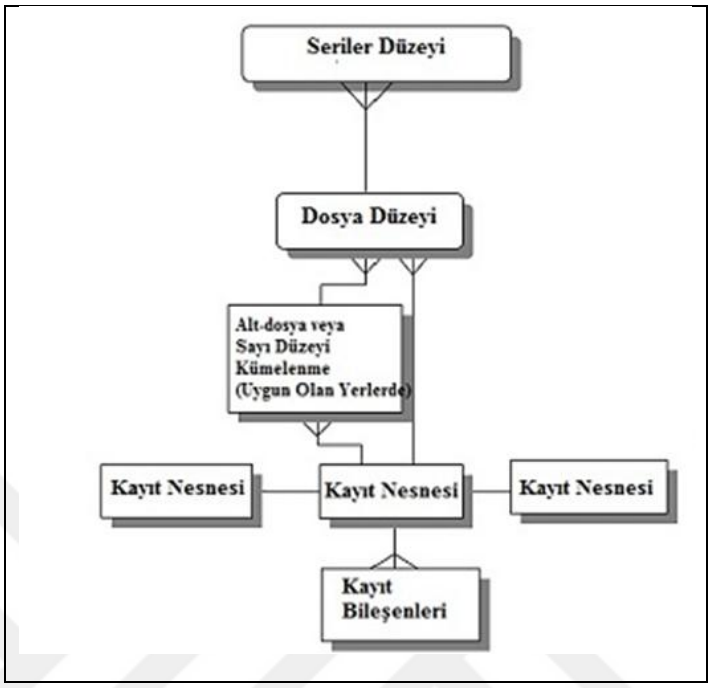
[26] Türk Standartları Enstitüsü, **Bilişim Terimleri Sözlüğü**, Ankara, Onur Matbaacılık, 2006, s. 6.

[27] International Council on Archives, **Principles and Functional Requirements for Records in Electronic Office Environments – Module 2: Guidelines and Functional Requirements for Electronic Records Management Systems**, 2008, s. 18.

[28] **A.y.**

[29] ICA, **a.g.e.**, s. 19

Şekil 2.5: Aggregation (Belgelerin Kümelenmesi)



(**Kaynak:** International Council on Archives, Principles and Functional Requirements for Records in Electronic Office Environments – Module 2: Guidelines and Functional Requirements for Electronic Records Management Systems, 2008, s. 19.)

Yukarıda sıralanan karakteristik özellikler ve belge üretim sorumluluğuna ek olarak bir belge yönetim sisteminde bütün belgelerin ilişkili olduğu bir üstveriye sahip olması gerekir. Üstveri, ISO 15489'a göre belgelerin bağlam, içerik ve yapısını veya bunların zaman içinde yönetilmesini tanımlayan bilgi olarak ifade edilmektedir.[30] Üstveri kendi arasında üç temel yapıya bölünür. Bunlar; tanımlayıcı üstveri, yapısal üstveri ve idari üstveridir. Tanımlayıcı üstverinin amacı sistemdeki varlıkların kimliklendirilmesi ve bulunmasıdır. Yapısal üstveri, bileşik nesnelerin nasıl biraraya getirildiğini gösteren elektronik dosya gibi verilerdir. İdari üstveri ise, elektronik belgenin yönetilmesi için bilgi sağlamaktır. Bu bir belgenin ne zaman ve ne şekilde üretildiği bilgisinin yanı sıra belgeyle ilgili dosya türü, diğer teknik bilgiler ve belgeye kimin erişecebileceği bilgisidir.[31] Üstveri, "belgelerin yeni sistemlere taşınmaları veya koruma politikaları geliştirilmesi durumunda hayati derece öneme sahip belgeleri standardize

[30] ISO, **15489-1: 2001,** 3.12.

[31] eDocuments, "Descriptive Metadata," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/index55e8.html?page_id=403, 11 Temmuz 2019.

etme ve erişilebilir kılma"[32] olmalarından dolayı MoReq yapısı için anlamlı olduğu gibi tüm EBYS'ler için önemlidir.

2.3. ANGLO-SAKSON MODELİ – YAŞAM DÖNGÜSÜ MODELİ

Yaşam döngüsü modeli, 1930'ların sonlarında Amerika Ulusal Arşivinden (US National Archives) Phillip Coolidge Brooks and Emmett J. Leahy tarafından tasarlanmıştır. Daha sonraları Ira A. Penn'in[33] tasarımı geliştirmesiyle model yaygınlık kazanmıştır. Modele göre, bir belgenin diğer biyolojik organizmalar gibi bir yaşamı vardır. Belge doğar (üretim aşaması), yaşar (devralma, düzenleme, koruma ve kullanım aşaması) ve ölür (değerlendirme ve imha aşaması).[34] Amerika Birleşik Devleti'nde gelişen bu model belge yönetimi kavramının da burada gelişmeye başladığını göstermektedir.[35]

Bir yaşam döngüsü, özellikle doğal bilimlerde, bir organizmanın yaşam tarihini oluşturan süreçler dizisinin tamamı olarak tanımlanabilir. Bireyler, nesiller boyu gözlemlenebilir bir tekrarlama kalıbı içinde tür veya cinsler gibi kendilerine ait aynı yaşam tarihini paylaşır.[36]

Bu model sosyal bilimlerde, insanın yaşam döngüsünde devam eden ritüellerin açıklanması için kullanılmaktadır. Örneğin, doğumla başlayıp yetişkin olarak topluma karışıp evlenme ve ölüm olarak devam eden yaşam döngüsü gibi. Yaşam döngüsündeki aşamalar genellikle, bir toplumdaki hak ve sorumlulukların güçlü bir şekilde ri-

---

[32] Bahattin Yalçınkaya, "e-Devlet Üstveri Standardının Oluşturulması ve Türkiye İçin Modellenmesi," **Yayımlanmamış Doktora Tezi**, Marmara Üniversitesi, Türkiyat Araştırmaları Enstitüsü, 2014, s. 24.

[33] Ira A. Penn, Amerika Birleşik Devletleri'nde Federal Hükümette belge yönetim analisti olarak görev yapmıştır. Ayrıca, ARMA (Association of Records Managers and Administrators) tarafından yayınlanan Records Management Quarterly adlı derginin editörlüğünü de yapmıştır (Ira A. Penn v.d., **Records Management Handbook,** Second Edition, New York, Routledge, 2016).

[34] Louise Spiteri, "Records Continuum Model,", **CNSA 2012 Conference,** 2012, (Çevrimiçi) https://www.slideshare.net/cleese6/records-continuum-model, 2 Mayıs 2018.

[35] Mehmet Fahri Furat, "Arşivcilik Hizmetlerinde Profesyonelleşme Süreci ve Türkiye," **Yayımlanmamış Doktora Tezi,** İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, 2009, s. 23.

[36] Sue Mckemmish, "Yesterday, Today and Tomorrow: A Continuum of Responsibility," **Proceedings of the Records Management Association of Australia 14th National Convention**, 15-17 Sept 1997, s. 2, (Çevrimiçi) https://monash.figshare.com/articles/Yesterday_today_and_tomorrow_a_continuum_of_responsibility/4037433, 4 Mayıs 2018.

tüellerle kurulduğunu ifade eden bir ilişki içinde ortaya çıkar. Doğal bilimlerdeki uyarlama gibi, sosyolojideki uyarlamalar yaşam sürecinin son evresi olan ölümle biten ve kuşak olarak da ifade edilen bir model sağlar.[37]

Yaşam döngüsünün belge yönetimi için anlamına bakıldığında, belgelerin üretilmeleri üzerinde ayrıntılı aşamalarda tanımlanabilen ve tekrar eden özellikleri ifade eder. Söz konusu aşamalar, zaman dilimi boyunca bireysel belgeler için uzun müddet gözlemlenebilir olmaları açısından önemlidir. Döngü, bireysel belgeler için tekrar eden ve uygulanabilen bir özelliğe sahiptir.[38]

Modelde belgeler için organizasyonel ihtiyaçların yerine getirilmesi, belgelerin "birincil" kullanımı olarak adlandırılmaktadır. Belgelerin örgütsel amaçlar için kanıt olarak birincil kullanımı sona erdiğinde, kurumların geleneksel olarak, kurumun kendisinin -kolektif hafızanın kanıtı olarak- aynı belgelere ilgi duydukları görülmüştür. Bu ilgi, eskiden belgelerin "ikincil" değer olarak kullanıldığı anlamına gelmektedir. Kurumsal ve kolektif hafıza ile ilgili konulara bakmanın bu yolu, yaşam döngüsü kavramına bağlıdır.[39]

Yaşam döngüsü kavramı, kayıtlı bir bilginin genel yönetiminde, bir düzen duygusu ve sistematik bir yaklaşımın desteklenmesinde faydalı olmuştur. Bununla birlikte prensiplerine sıkı sıkıya bağlı kalmak, arşivcilerin ve belge yöneticilerinin daha fazla işbirliği ve koordinasyonuna yönelik eğilimlere zarar vermektedir. Model, belge yönetimi ve arşiv işlemlerinin birbiriyle ilişkili, hatta iç içe geçtiği birçok yolu göz ardı eder. Büyük bir bürokraside, belge yönetimini ve arşiv işlevlerini dikkatlice belirleyerek, rolleri ve sorumlulukları netleştirmeye çalışmak uygun olabildiği gibi tam tersi bir durumu da yansıtabilir. Çünkü arşivcinin belgelerin üretilmesinden, imha sürelerinin belirlenmesine veya tasnif sistemlerinin geliştirilmesine hizmet etmede herhangi bir rolünün olmadığı vurgusu yapılmaktadır. Böyle bir durumda da belge yöneticisinin sürekli olarak değerli belgeleri tespit etmede veya araştırmacılara hizmet etmede gerçekten bir sorumluluğu yok mudur sorusu sorulmalıdır. Bu tartışmalar modelce cevap bulması gereken konulardır. Günümüz şartlarında yaşam döngüsü modelinde belge

[37] **A.g.e.**, s. 1.
[38] **A.y.**
[39] **A.y.**, s. 1.

yönetimi ve arşiv aşamaları arasındaki farklılığın artık kabul edilemez olduğu inancı da yaygındır.[40] Ancak yaşam döngüsü modeli belge yönetiminde açık bir şekilde tanımlanabilen aşamalar olduğunu tartışmakta ve güncel ile tarihsel belge yönetimi arasında belirgin bir fark ortaya koymaktadır.[41]

Yaşam döngüsüne ilişkin bilgi verirken, tartışılması gerekli ve önemli olan bir konu daha vardır. Bu konu değişen kayıt ortamı ve buna bağlı olarak gelişen elektronik belge yönetimidir. Geleneksel olarak, belgeler kâğıt olarak üretilip saklanır. Belge olarak saklanan kâğıdın üzerindeki bilgi var olduğu müddetçe ve o belgenin kendisinin var olması, o bilgi ve belgeye erişim için yeterlidir. Eğer belge yanlış dosyalanıp yerleştirilmişse yerinin belirlenmesi için çok çaba gerekebilir ve bunun maliyeti de yüksektir. Ancak, yeterli zaman verilip ve yeterli çaba harcandığında belgeye erişmek imkânsız değildir. Bu durum geleneksel belge yönetimi için geçerli olmakla beraber elektronik belge yönetimi için böyle bir durum söz konusu değildir. Elektronik formdaki bilgi güncellendiği zaman, daha önce var olan bilgi kaybolabilir.[42] Elektronik veri tabanı işlemleri, orijinal bilgi için referans olan kopyaya ve kronolojik dosyaya erişimi sağlamayabilir. Elektronik ortamdaki depolanan bilgi, toz, ısı, duman, aşınma ve hatta sıradan telefonlardan yayılan manyetik etkilerden dahi olumsuz olarak etkilenebilir. Elektronik depolama alanına dâhil edilen bilgi, güç (elektrik) dalgalanmasında veya kesintisinde tamamen yok olabilir. Dosyalanan bilginin sistem türünü ve kullanılan dosyalamayı bilemeyen kişi, bilgiye erişemeyebilir veya sistemi ve yapıyı iyi bilenlerce dosyaların tamamına ancak erişilebilir. Bu problemler sadece otomatik veri süreçlerine veya bilgi yönetim sistemlerine ilişkin değildir. Belge yönetim problemlerine ilişkin olarak da düşünülmelidir. Çünkü bunlar kayıtlı bilginin nasıl üretildiği, korunduğu, kullanıldığı ve düzenlendiğiyle doğrudan ilişkilidir. Bu nedenle, yukarıda ifade edilen problemlerin çözümü kayıtlı bilginin iyi yönetilmesidir.[43]

[40] Jay Atherton, "From Life Cycle to Continuum: Some Thoughts on the Records Management - Archives Relationship," **Archivaria**, Winter 1985-1986, C. 21, s. 47.

[41] McKemmish, "Yesterday, Today and Tomorrow: A Continuum of Responsibility, " s. 2.

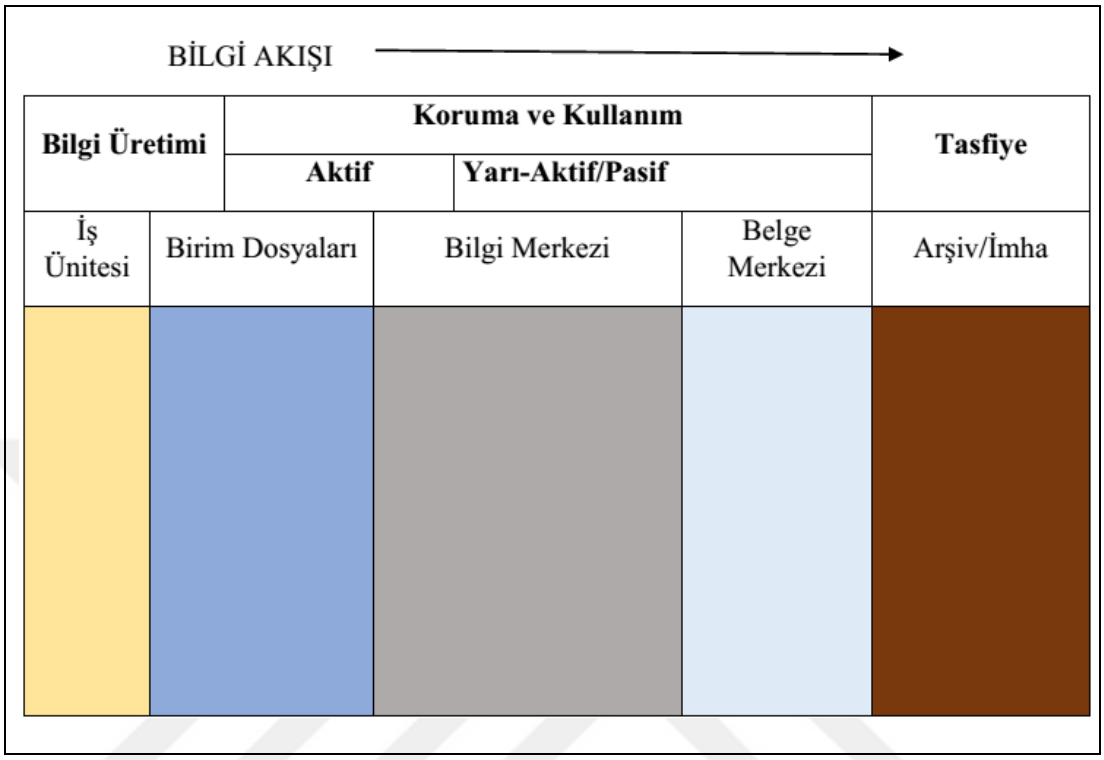
[42] Ira A. Penn v.d., **Records Management Handbook**, Second Edition, New York, Routledge, 2016, s. 9.

[43] **A.g.e.**, s. 9-10.

İfade edilen sorunlar haricinde ele alınması gereken önemli bir diğer konu da bilginin ispatı meselesidir. Kâğıt belgeler, iş hayatında uzun süre bilginin doğrulanması noktasında yardımcı oldu. Kâğıdın yerini alabilecek manyetik, optik, holografik ve daha tanımlanmayan yeni ortamlar ortaya çıksa/çıkacaksa da, iş hayatında temel olan belgelerin ispatı gerçeğini değiştirmeyecektir. Bu gerçek tek başına kâğıt değildi. Kâğıtla beraber uygun belge yönetimi de bu gerçeğin içinde yer aldı. Yüzyılı aşkın sürede, kâğıt belgelerin iş hayatında bilginin ispatı için kullanılması iki unsurla gerçekleşti. Bunlar; kâğıt ortam ve belge yönetimiydi. Bu ikili ayrılmaz bir şekilde birbirine bağlıydı. Elektronik belge yönetiminde bu bağlılık da söz konusu değildir. Bilginin ispatı için gereklilik, bilgi ortamına bakılmaksızın devam etmektedir. Yeni tekniklerin, politikaların, yöntemlerin ve standartların bütün ortamlar için uygun hale getirilmesi zaman alacak ve kurum çapında bir beyin (hafıza) güveninin eski kâğıt yöntemleriyle olduğu kadar rahat olmasına odaklanmasını gerektirecektir. Bununla birlikte, kurum ve kuruluşların, bilginin doğrulanmasına duydukları ihtiyaç artacak, elektronik bilgi veri tabanlarının kaynaklarını tanımlamak ve doğrulamak zorlaşacak ve bu zorluğun artarak devam edecektir. Artan bu ihtiyacı karşılamak için, belge yönetimi bir değişim geçirmektedir. Birçok kurum ve kuruluşun varlığı, onların bu değişimi kolaylaştıracak yatırımlar yapmasına bağlıdır. Çünkü bilgi teknolojileri, kurum ve kuruluşların idaresinde yaklaşan yenilikleri sunmaktadır.[44]

[44] Penn v.d., **a.g.e.**, s. 10-11.

Şekil 2.6: Yaşam Döngüsü Modelinde Bilgi Akışı Aşamaları



(**Kaynak:** Ira A. Penn v.d., Records Management Handbook, Second Edition, New York, Routledge, 2016, s. 13.)

2.4. AVUSTRALYA MODELİ – BELGE SÜREKLİLİĞİ MODELİ

Belge sürekliliği yaklaşımı, Frank Upward[45] tarafından 1990'lı yıllarda geliştirilmiştir. Upward, Jay Atherton[46]'ın görüşlerinden yoğun bir şekilde etkilenmiştir. Atherton'ın belge yönetimi ile arşivcilik arasındaki ilişkiyi ortaya koyan teorileri Upward için önemli birer kaynak olmuştur.[47]

Belge sürekliliği (records contiuum), belge yönetimi, kanıt, işlem ve belge üreticisinin kimliğinin örtüşen özelliklerini vurgulayan bir arşiv bilimi yaklaşımıdır.[48] Diğer bir tanıma göre ise, belgelerin üretilmesinden (ve belge yönetimi sistemlerinin tasarımında üretilmeden önce) belgelerin arşiv olarak saklanması ve kullanılmasına kadar tutarlı bir yönetim süreci sergileyen bir yaklaşımdır.[49]

Avustralya yaklaşımında belgenin kavram olarak karşılığı süreklilik değerinin kayıtları ifade etmesidir ve bu arşivlere işaret ediyor olduğunu göstermektedir. İşlemsel, kanıtsal ve bellek amaçlarına yönelik kullanımlarını vurgulayan ve belgelerin kısa bir süreliğine veya bir yüzyıl gibi uzun bir süre için saklanıp saklanmayacağı arşivleme / belge yönetimi yaklaşımlarını birleştirmektedir.[50] Geleneksel belge yönetimi teorisinde, belgeler farklı değere sahiptir. Bu değerler;[51]

- Birincil değer, iş aktivitelerini destekleyen ve kanıt değeri olan belgeleri kapsayan,

---

[45] Frank Upward, Avustralya'da Centre for Organisational and Social Informatics adlı kurumda baş araştırmacı olarak çalışmıştır. Daha önce Monash Üniversitesi'nde öğretim görevlisi olarak, özellikle belge yönetimi sistemleri tasarımında arşivler, kayıtlar, bilgi yönetimi ve bilgi sistemleri faaliyetlerinin yürütüldüğü birimlerde çalıştı. Söz konusu alanlarda danışman ve uygulayıcı olarak çalışan Upward, daha iyi belge yönetim uygulamalarını teşvik eden kar amacı gütmeyen bir kuruluş olan Recordkeeping Institute'ün direktörlüğünü yaptı ((Çevrimiçi) https://recordscontinuum.info/wiki/UpwardFrank, 3 Ocak 2019).

[46] Jay Atherton, Kanada Devlet Arşivleri Kayıt Yönetimi Biriminin yöneticiliğini yaptı. Daha önce Federal Arşiv Bölümü (Federal Archives Division, PAC) yönetici olarak görev yaptı. Kanadalı Arşivciler Derneği (Association of Canadian Archivists), L'Association des archivistes du QuCbec, Belge Yöneticileri ve İdarecileri Derneği (The Association of Records Managers and Administrators-ARMA) ve Amerikan Arşivciler Derneği (Society of American Archivist- SAA) üyesidir (Çevrimiçi) https://archivaria.ca/archivar/index.php/archivaria/article/view/11233/12172, 3 Ocak 2019.

[47] Spiteri, "Records Continuum Model,".

[48] Pearce-Moses, **A Glossary of Archival and Records Terminology**, s. 333.

[49] Spiteri, "Records Continuum Model,".

[50] Upward, "Structuring the Records Continuum - Part One: Postcustodial Principles and Properties," s. 5.

[51] Spiteri, "Records Continuum Model,"

- İkincil değer, araştırmayı destekleyici geçmiş için kanıt niteliği taşıyan belgelerdir.

ISO 15489'da da geleneksel belge yönetimi teorisine uygun olarak belgenin tarifi şu şekilde yapılmaktadır. "Yasal yükümlülükler ya da işin yürütülmesi sırasında bir kurum veya kişi tarafından kanıt ve bilgi olarak oluşturulan, alınan ve korunan bilgiler" şeklindedir.[52] Louise Spiteri'nin[53] yorumuyla "bir kaydın kanıt değeri sadece içerik, yapı ve bağlam korunursa mevcut olabilir. Bağlam, birbirine ait olan farklı belgeler ile belgenin oluşturulduğu süreç arasındaki bağlantıdır."

Süreklilik yaklaşımında üzerinde odaklanılan temel unsurlardan biri, belgelerin kâğıt veya elektronik formda olup olmadıklarına bakılmaksızın, fiziksel varlıklar yerine mantıksal çerçevededir. Belge yönetimi mesleğinin kurumsallaşması, belge yönetimi sürecinin iş ve toplumsal süreçlere ve amaçlara entegre edilmesi ihtiyacına önemli bir vurgu yapılmasını gerektirir. Bu nedenle belge yönetimi kavramı da bu yaklaşım içinde ele alınmaktadır.[54] Süreklilik modelinde üzerinde odaklanılan temel unsurlardan biri de belge yönetimi ve arşivsel görevlerin yeni "belge yöneticileri (recordkeepers)" mesleği ile birleştirilmesinin teşvik edilmesidir. Bu noktada post-custodialism teorisinin açıklanması yerinde olur. Amerikan Arşivciler Derneği, Postcustodial teoriyi, arşivcilerin, merkezi bir depodaki etkin olmayan belgelerin koruyucularından, belgelerin üretildiği ve kullanıldığı ofislerde dağıtılan bir belge yöneticisinin rolüne kaydırmak[55] olarak açıklamaktadır.[56] Post-custodialism[57] arşivlerin dijital belgelerin

[52] ISO, **15489-1.**

[53] Louise Spiteri, Kanada Dalhousie Üniversitesi Bilgi Yönetimi alanında, bilgi yönetimi, meta veriler, kataloglama, belge yönetimi ve indeksleme gibi konulara ilişkin ders vermektedir. Thesaurus ve taksonomiler gibi indeksleme dillerinin oluşturulma noktasındaki araştırmalara yoğunlaşmaktadır (Çevrimiçi) https://dal.academia.edu/LouiseSpiteri, 3 Ocak 2019.

[54] Upward, "Structuring the Records Continuum - Part One: Postcustodial Principles and Properties," s. 5.

[55] Society of American Archivists, "Postcustodial Theory of Archives," (Çevrimiçi) https://www2.archivists.org/glossary/terms/p/postcustodial-theory-of-archives, 18 Ağustos 2019.

[56] Alistair G. Tough, "The Post-Custodial/Pro-Custodial Argument From A Records Management Perspective," **Journal of the Society of Archivists**, 2004, C. 25, S. 1, s. (Çevrimiçi) https://doi.org/10.1080/0037981042000199115 , 4 ağustos 2019.

[57] Custodial ve post-custodial kavramları 1870'li yıllarda Hollandalı Theodoor Van Riemsdijk'in görüşlerine dayanmaktadır. Çünkü Riemsdijk, belgelerin gelecekteki kullanımları yerine, belgenin niçin ve nasıl üretildiğine odaklanmıştır. Bu düşünce, Riemsdijk'i modern post-custodialism yaklaşımının öncüsü olarak bilinmesini sağlamaktadır. (Eric Ketelaar, "Archival Theory and the Dutch Manual," **Archivaria**, Spring 1996, C. 41, s. 33.) Daha sonraları custody kavramı Shellenberg ve Jenkinson tarafından da kullanılmıştır. 1980 yılında F. Gerald Ham, arşiv bilimi literatürüne ve teorilerine

nihai depoları olması gerekmediğini ve dijital belgelerin, oluşturuldukları belge saklama sistemlerinde dağıtılmış bir belge yöneticisi olarak önceki rolünün yeniden şekillenmiş pozisyonunda bulunabileceğini öngörmektedir. Arşivcinin rolü de bu post-custodialism ortamında yeniden düşünülebilir. Belge yönetim sistemlerinin de arşiv olması gerektiğinden, arşiv değerlerinin sistem tasarımına dâhil edilmesi için arşivcilere danışılmalıdır.[58]

Arşiv bilimi, prensipler kadar alt özellikleri de kapsamına dâhil eder. Belge sürekliliği, dört aşama etrafında inşa edilen bir yaklaşımdır. Bunlar; belge yönetimi, kanıt değeri, işlem ve üretim sorumluğunun tanımlanması aşamalarıdır. Bu aşamalar, arşiv bilimindeki ana temaları ve alt özelliklerini açıklamakta ve her bir aşama, boyutsal olarak bağlanabilecek dört katmanda sunulmaktadır.[59]

1. Belge yönetimi aşaması: Bu aşamada kişi aktivitelerine ilişkin kayıtlı bilgiyi depolayacak araçlarla ilgili bilgi verilmektedir. Belge yönetimi aşaması, belgenin içeriği, yapısı ve üretim bağlamına sahiptir.
2. Kanıt değeri aşaması: Bu aşama, eylemlerin izinden, belgelerin sağlayabileceği kanıtlardan ve bunların kurumsal ve kolektif hafızadaki rollerinden oluşur.
3. İşlem aşaması: Bu aşama, eylemleri, etkinlikleri, işlevleri ve amaçları koordinat olarak sunar. Yaklaşımda terimler basit bir şekilde tasarlanmış etiket-

"postcustodialism" kavramını tanıtmıştır. (Corie Zylstra, "Custodial and Post-custodial Approaches to Archives," **Sunum**, (Çevrimiçi) http://coriezylstraeportfolio.weebly.com/uploads/1/4/4/2/14421694/zylstrafinalpresentation.pptx, 17 Ağustos 2019). F. Gerald Ham, custodial ve post-custodial kavramaları arasındaki ilişikiyi şu şekilde açıklamaktadır: İki önemli gelişme ki bunlar teknolojinin arşiv belgesine etkisi ve arşiv programlarının yayılması, post-custodial döneminde arşiv dünyasını giderek daha fazla şekillendirecektir. Yani teknoloji ve teknolojinin arşivcilikte uygulanmasını sağlayan programların custodial dönemde olmayan değişimler olduğunu ve bu değişimlerle beraber post-custodialism döneminin yaşanacağı ifade edilmektedir. (F. Gerald Ham, "Archival Strategies for the Post-Custodial Era," **The American Archivist**, Summer 1981, C. 44, S. 3, s. 211). Ham'e göre arşivciler bu dönemin sağladığı gelişmelerle daha entegre arşivleme sistemleri geliştirmek için arşivleme programlarının ve varlıklarının yayılması ve yerelleştirilmesinin rasyonelleştirilip koordine edilmesine yardımcı olabilirler. (**A.g.e.**, s. 213).

[58] Mark Koerber, "A Critique of the Records Continuum Model," **Unpublished Minor Thesis** for the Masters of Information Management (Archives and Records Management), University of South Australia, School of Information Technology & Mathematical Science, Adelaide, 2017, s. 8.

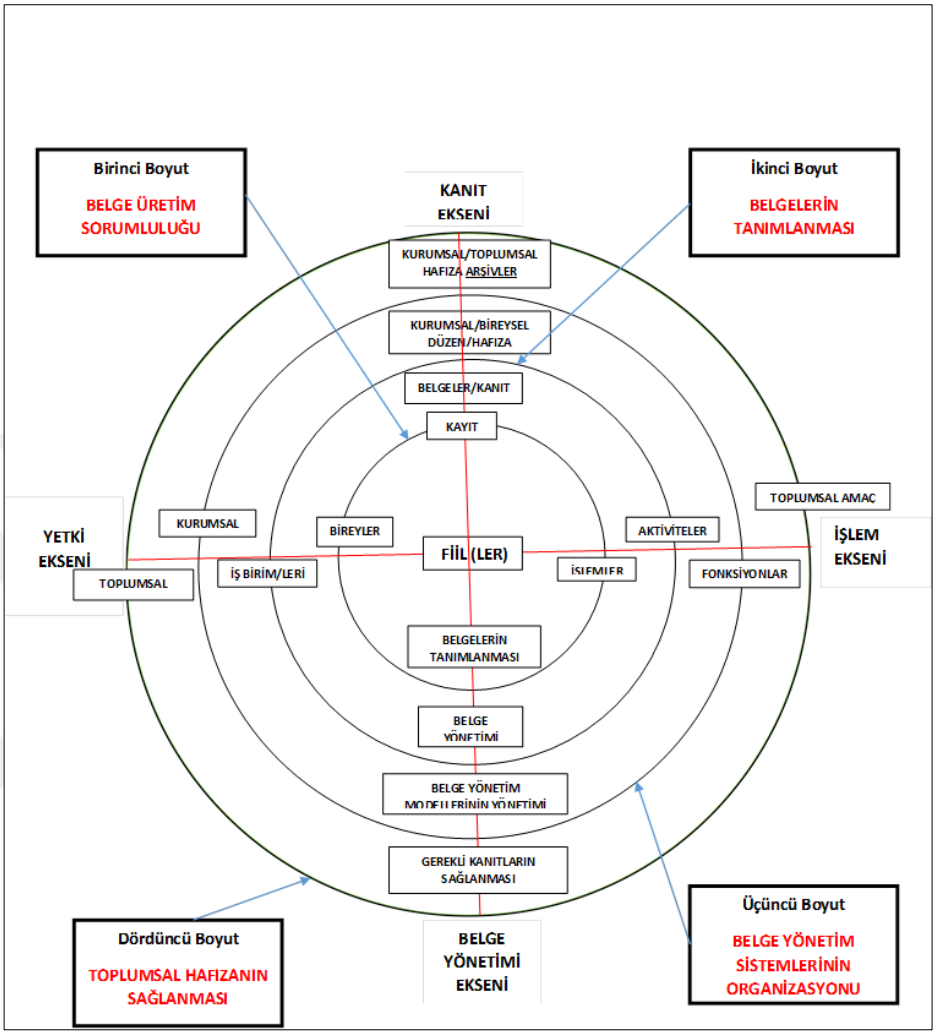
[59] Upward, "Structuring the Records Continuum - Part One: Postcustodial Principles and Properties," s. 6-7.

lerden ibarettir. Bu aşama, olayların gerçekleştirilmesinde üstlenilen faaliyetlerin kayıtları olarak belgelere ve bu faaliyetlerin belgeler arasında bağlantı oluşturmasına vurgu yapmaktadır. Temel olarak, kurumların işlevleri ve bunların faaliyet alt kategorilerine göre nasıl parçalandığını ya da eylemlerin kendilerinden nasıl oluştuğunu yansıtmaktadır. Bu aşamanın amacı, arşivleri içine alan daha geniş bir toplumsal perspektiften bakılan işlevi yansıtmaktır.

4. Üretim sorumluluğu tanımlama aşaması: Bu aşama failin, failin ilişkili olduğu iş ünitesinin (tek başına fail olabilir), ünitenin ilişkili olduğu kurumun (aynı zamanda fail veya ünite de olabilir) ve kimliğinin nasıl işlediğini temsil eder. Bu temsil, unsurların daha geniş sosyal tanımlamayla kurumsallaştırılmasıdır.

Aşamaların ayrıntılı olarak gösterildiği Frank Upward'ın kullandığı şekil, bu tez için Türkçe olarak tarafımızdan hazırlanarak aşağıda sunulmuştur.

Şekil 2.7: Avustralya Belge Sürekliliği Modeli



(**Kaynak:** Frank Upward, "Structuring the Records Continuum - Part One: Postcustodial Principles and Properties," s. 6; Yazar tarafından Türkçe olarak yeniden hazırlanmıştır.)

Yukarıda açıklanan aşamalar şekil üzerinde eksenler olarak ifade edilmektedir. Bu aşamaların veya eksenlerin örtüşen özellikleri şekildeki boyutlarla açıklanmaktadır. Model esas alınarak aşamalı bir analiz yapmak ve bir belge yönetimi sistemi okuması gerçekleştirmek mümkün olabilir. Süreklilik modelinin koordinatlarına bakıldığında, belge yönetimi sisteminin farklı aşamaları ortaya çıkmış olur. Bu aşamalar sı-

nırlar olarak düşünülmemelidir. Koordinatlar değişebilir ve değişimler aşamalar arasında eş zamanlı olarak gerçekleşebilir. Ancak belge yönetimi sistemi nasıl kurulursa kurulsun aşağıda belirtilen şekilde analiz edilir.[60]

Aşamaların sırasıyla değerlendirilmesi yapıldığında sahip oldukları değerler daha iyi anlaşılabilir. Buna istinaden birinci aşama üzerinde düşünüldüğünde, işlemler, bağlantılar ve kararlar kayıt altına alınmaktadır. Belge üretimi ve kontrol süreçleri uygulanmaktadır: Bunlar;[61]

- Belgenin içeriğinin tutulması,
- Belgenin yapısının belirlenmesi (belgesel formu),
- Belgeleri anında eylem bağlamında düzenlenmesi ve yerleştirilmesi ve bunların geri çağrılması ve
- Belgelerin depolanması ve güvenliğinin sağlanmasıdır.

İkinci aşama, bir iletişim sistemi sonrası (örneğin kaydetmeyi de içeren geleneksel kayıt fonksiyonelliği), veri için ilgili dokümanları ve dokümanların paylaşılması için veriye değer atfetme ve verinin imhasını içeren kayıt bilgisinin korunmasıdır. Kanıt tabanlı belge yönetimi yaklaşımını destekleyen bir belge sürekliliği modeli açısından dört aşamadan ikincisi çok önemlidir. Bu, belgenin, ilk aşamadan anlık bağlamlarından ayrıldığı yerdir. Bu ayrıştırma süreci, belgeye 'sembolik bir simge' olarak değer verir. Bir doküman bir eylemin içine gömülür, ancak doküman, bir belge olarak belgenin dış referans noktaları kullanılarak geçerli olmasına ihtiyaç duyar. Bu noktalar, alındığı belge yönetimi sisteminin işleyişini ve belgenin parçası olduğu teknik, sosyal (iş dâhil) ve iletişim süreçlerine ilişkin bilgileri içermektedir.[62]

İkinci aşamada, belge yönetim süreçleri ve sistemlerinin uygulanması ifade edilmektedir. Bu süreç ve sistemler, üçüncü ve dördüncü aşamalarda oluşturulan tasarım

[60] Upward, **a.g.e.**, s. 7.
[61] Mckemmish, "Yesterday, Today and Tomorrow: A Continuum of Responsibility".
[62] Upward, "Structuring the Records Continuum - Part One: Postcustodial Principles and Properties," s. 8.

gereksinimleri, standartlar ve en iyi uygulama modelleriyle uyumlu olarak yapılmaktadır. Uygulanan süreçler ve sistemler şu şekildedir:[63]

- İş süreçleri içinde belirlenen noktalarda belgenin tutulması (önceden belirlenen sınırlar kapsamında),
- Yapılan işlemlerle ilgili belgeler ve sosyal aktiviteler olarak bunların kalitesinden emin olmak için gerekli üstverinin tutulması ve korunması (örneğin tutulan üstveri, belgelerinin yerlerini, diğer belgelerle olan ilişkilerini ve belgelerin faaliyet bağlamına göre bağlayan verileri sunması) ve belgelerin kullanılabilmesi (bütünlük, kesinlik - doğruluk ve güvenirlik) ve zaman içinde erişilebilirliğinin sağlanması,
- Belgelerin erişim izinlerine ve kullanıcı görüşlerine göre zaman içinde kullanım için gönderilmesi ve
- Belgelerin zaman içinde depolanması ve güvenliğinin sağlanmasıdır.

Üçüncü ve dördüncü aşamalar da kontrol, regülasyon, standardizasyon ve düzenleme açılarından bilgi yönetim uzmanlarının yönetsel rollerindeki aşamalar olarak düşünülebilir. Üçüncü aşama, formlama, yönetme ve ortak hafızaya erişim sağlama gibi içsel konularla ilişkilidir. Dördüncü aşama, dışarıdan bakıldığında hukuksal ve kurumsal sınırlar çerçevesinde kolektif hafızanın temelleri ile ilgilidir.[64] Üçüncü aşamayı düşündüğümüzde,

- bireysel/kurumsal hafızanın bir parçası olan kanıt değeri belirtmek üzere kurum ve çalışanlar açısından gereklilikleri tanımlamak,
- bireysel veya kurumsal alanda bilgi yönetim sistemlerini kurmak,
- bireysel ve kurumsal bağlamdaki bilgi yönetim sistemlerini gösteren kurumsal bilgi tabanları ve sınıflandırma şemaları geliştirmek,
- bir kişinin veya bir kurumun yaşamı boyunca belgeleri hayatta tutacak depolama ve taşınma stratejilerini belirlemek ve

[63] Mckemmish, "Yesterday, Today and Tomorrow: A Continuum of Responsibility".
[64] **A.g.e.**, s. 8.

- bireysel veya kurumsal alanda belirli rollere göre erişimi yönetecek erişim stratejileri geliştirmek üzerine şekillenmektedir.

Dördüncü aşama, kolektif (toplumsal) hafızayı inşa etmek, geri çağırmak ve yaymak (sosyal, kültürel veya tarihsel) için arşivsel bilgi sistemi bakımından gerekli olan bilgi çeşitlerini içeren bir sistemdir. Dördüncü aşamayı düşündüğümüzde;

- Toplumsal ve kültürel görevlerin kolektif hafıza işlevi görmesi için gerekli kanıtların tanımlanması veya belirlenmesi,
- Bir birey veya bir kurumun yaşamı ötesinde belgelerin sürdürülebileceği belge yönetim sistemlerinin kurulması,
- Bilgi yönetim sistemleri bağlamında en geniş yapının ve fonksiyonun gösterildiği bilgi havuzlarının ve sınıflandırma şemalarının geliştirilmesi,
- Bir kişinin veya bir kurumun yaşamı sonrası belgeleri sürdürebilecek depolama ve taşınma stratejilerinin belirlenmesi ve
- Yetki alanları arasında erişimi yöneten erişim stratejilerinin geliştirilmesi hususları anlaşılmalıdır.

Süreklilik modelinin kavramsal bir araç olarak genişliği ve zenginliği, belge yönetimi içinde tanımlanacak üç uzmanlık alanı içerisinde fiil-yapı konularını kapsayabildiği ölçüde genişler:[65]

- Modern belge yönetimi - mevcut belge yönetimi eylemleri ve gerçekleştirildikleri yapılar,
- Düzenleyici belge yönetimi - düzenleme süreçleri ve politikalar, standartlar, kanunlar, mevzuat ve en iyi uygulamaların duyurulması gibi eylemler için yapıları etkinleştirme ve kontrol etme ve son olarak
- Tarihsel belge yönetimi - depolama, geri çağırma ve paylaşma için belgeyle ilgili aranan verilerin bir parçası olarak fiil ve yapının adli olarak incelendiği provenans araştırmaları.

[65] Upward, "Structuring the Records Continuum - Part One: Postcustodial Principles and Properties," s. 4. (Frank Upward, arşivleme sürecine bir vurgu yapabilmek için olayı sunarken, kendi deyimiyle Jean-François Lyotard ve Antony Giddens'in kalın ciltleri arasında ince bir arşiv fasikülü olarak belgelerin süreklilik modelini sunduğunu ifade eder.)

Belge yönetimi teorisi, herhangi bir ülke ya da kültürün geleneklerinden daha fazlasıdır ve evrensel düzeyde kavramsallaştırılabilmelidir. Ancak gelecekte varlığın devamı için daha fazla süreç odaklı olmak zorunluluğu unutulmamalıdır.[66]

Belgelerin süreklilik modeli perspektifinde belgeler, bu süreçte sürekliliği olan nesnelerden ziyade bir süreç olarak görülmektedir. Elektronik belgeler, aynı noktada farklı yerlere aktarılır ve kullanılır, böylece asıl konumun doğruluğunu garanti etmek önemsiz hale gelir. Bunların özgünlüğü, kaydın varlığı boyunca ilgili bilgileri meta verilerle görselleştirerek garanti eder.[67] Özetle Upward'ın vurguladığı ilkeler şu şekilde ifade edilebilir:[68]

- Belgeler işlemsel, kanıtsal ve bellek amaçları için kullanılır ve saklama sürelerine bakılmaksızın arşivleme / belge yönetimi ile ilgili birleştirilmiş yaklaşımlarla ele alınmalıdır.
- Belgeler, kâğıt veya elektronik formda olup olmadıklarına bakılmaksızın, fiziksel varlıklar yerine mantıksal olarak ele alınır.
- Belge yönetimi mesleğinin belge yönetimini, iş ve toplumsal süreçlere ve amaçlara entegre etmesi gerekmektedir.
- Arşiv bilimi, belge yönetimi hakkındaki bilgileri organize etmenin temelidir.

Bütün bunlardan çıkarılacak sonuç; belge yönetiminin süreklilik modelindeki rolü nedir? Sorusunun cevabı ise şu şekilde verilebilir:[69]

- Yönetişimi kolaylaştırmak.
- Kurumsal, sosyal, kültürel ve tarihsel hesap verebilirliği kolaylaştırmak.
- Ortak ve kurumsal hafızayı tutmak, özellikle deneysel bilgiyi belge olarak tutmak.
- Hem kişisel hem de ortak kimliğin kanıtlarını sağlamak.

---

[66] Frank Upward, "Structuring the Records Continuum, Part Two: Structuration Theory and Recordkeeping," **Archives & Manuscripts**, 1997, C. 25, S.1, s. 9.

[67] Terry Eastwood, v.d., **Currents of Archival Thinking**, Santa Barbara, California, Libraries Unlimited, 2010, s. 152-153; Akt: Erica Hellmer, "Authenticity in Electronic Archives: Securing Digital Records," **Unpublished Master Thesis**, Mid Sweden University, Institution for Archives and Information Science, 2015, s. 18.

[68] Louise Spiteri, "Records Continuum Model,", **CNSA 2012 Conference,** 2012, (Çevrimiçi) https://www.slideshare.net/cleese6/records-continuum-model, 2 Mayıs 2018.

[69] **A.g.s.**

- Varlık olarak yararlanılabilecek bilgiler ile süreç içinde yeni üretilmiş belgelerden katma değerli bilgiler sağlamak.

Bu bilgiler çerçevesinde süreklilik modelinin sunduğu katkıları da şu şekilde ifade edebiliriz:[70]

- Bu model belge yöneticileri ile arşivcileri ortak bir amaçla (belgenin güvenirliğini, gerçekliğini ve bütünlüğünü garanti etmek için) entegre edilmiş belge yönetimi çerçevesinde bir araya getirmektedir.
- Model, belge yönetimi ve arşivleme süreçleri için ortak anlayış, uygun standartlar, en iyi birleşik uygulama kriterleri ve disiplinler arası yaklaşımlar sağlamaktadır.
- Model, geçmişi günümüzle ve günümüzü de gelecekle bağlantı kuran sürdürülebilir belge yönetimi yaklaşımı sunmaktadır.

Süreklilik modeli, Avustralya'da elektronik belge yönetimi politikaları ve stratejilerinin geliştirilmesi ve son zamanlarda süreklilik tabanlı profesyonel uygulamaların özelliklerini en iyi şekilde yansıtan standart ortamda uygulanabilen bir yapıdır.[71]

Süreklilik temelli bir yaklaşım, birleşik zaman-mekân boyutlarını önerir. Belgeler, üretilmelerinden itibaren zaman ve mekânda sabit olmakla birlikte, belge yönetim sistemleriyle ileriye taşınır ve farklı zamanlarda ve alanlarda yaşayan insanlara sunularak çok amaçlı kullanımlar sağlar.[72]

[70] **A.g.e.**
[71] McKemmish, "Yesterday, Today and Tomorrow: A Continuum of Responsibility", s. 3.
[72] **A.y.**

ÜÇÜNCÜ BÖLÜM

ELEKTRONİK BELGENİN VARLIĞININ YAZILIM VE DONANIM YÖNÜ VE BU YÖNLERE AİT İZLER

3.1. ELEKTRONİK BELGE YÖNETİM SİSTEMLERİ

Elektronik belgelerin varlığının yazılım ve donanım yönleri elektronik belge yönetim sistemi (EBYS) veya elektronik doküman yönetim sistemi (EDYS) bağlamında düşünülmektedir. EBYS, iş faaliyetlerinin kanıtlarını sağlamak amacıyla elektronik ortamdaki belgelerin üretimini, kullanılmasını, korumasını ve tasviyesini yönetmek için kullanılan otomatik bir sistemdir. Bu sistemler uygun bağlamsal bilgileri (üstveri) korur ve değerlerini kanıt olarak desteklemek için belgeler arasında bağlantı kurar.[1] EBYS'ler, sınıflandırma programları dâhilinde belgelerin oluşturulmasını ve korunmasını yönetmek, saklama ve tasfiye programlarını uygulamak, erişimi ve kullanımı kontrol etmek için kullanılabilir. EBYS, bir kurumun iş sistemleri ve uygulamaları tarafından oluşturulan belgeleri sistemde tutmasının yanı sıra ilgili üstverilerle birlikte bir kayıt tutmalı ve bir sınıflandırma şeması içinde sınıflara ayırmalıdır. Elektronik belgeler fiziksel belgelerle aynı örtülü üstveriye sahip olmadığından, bunlara atfedilen üstverinin kapsamı daha büyüktür. Bir elektronik belge, birçok farklı parçadan veya dijital nesneden oluşabilir ve bunları yönetmek için kullanılan sistem, tüm bu nesneleri koruyabilmeli ve orijinal belgenin gerçek ve güvenilir bir kopyası olarak yeniden oluşturabilmelidir.[2]

---

[1] National Archives of Australia (NAI), **Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records**, Exposure Draft, 2004, s. 78, (Çevrimiçi) https://mayaar-binaginting.weebly.com/uploads/1/0/6/1/10612501/digital_recordkeeping.pdf, 7 Temmuz 2019.
Bu sistemler genel olarak EDYS olarak da isimlendirilebilir (ICA, **Principles and Functional Requirements for Records in Electronic Office Environments – Module 2**, s. 60.). İskoçya Milli Arşivi (National Records of Scotland) de EBYS'lerin, belgeleri izlemek ve depolamak için tasarlanmış bir bilgisayar programı veya program grubu olarak tanımlar.

[2] National Records of Scotland, **Electronic Records Management Systems**, (Çevrimiçi) https://www.nrscotland.gov.uk/record-keeping/electronic-records-management/electronic-records-management-systems, 29 Haziran 2019.

EBYS'ler dünyada farklı yazılımlar ve yaklaşımlar olarak karşımıza çıkmaktadır. Bu yazılımlar, üç farklı EBYS yaklaşımı bağlamında ele alınmış ve yukarıda açıklanmıştı. Bunlar; Avrupa idari modelini temsilen MoReq (2001, 2008 ve 2010) örneği, Anglo-Sakson modelini temsilen yaşam döngüsü ve Avustralya modelidir. Bu çerçevede sistem içinde belgelerin nasıl izler bıraktığı belgelerin sistem içindeki evrelerine bağlı olarak aşağıda açıklanmıştır. Bu evreler üç ayrı süreç olarak karşımıza çıkmaktadır. Bunlar;[3]

Belge üretim süreci	Belgelerin, üretimi/sağlanması/düzenlenmesi/tanımlanması/indekslenmesi
	Üretilen ve sağlanan belgelerin yönetimi
Belge kullanım süreci	Belgelerin erişimi, görüntülenmesi
	Belgelerin paylaşımı, dolaşımı ve kullandırılması
İmha ve koruma süreci	Belgelerin saklanılması, tasviyesi, imhası ve korunmasıdır

EBYS öncesi süreçlerin belgelerin sistemdeki varlığı ve bu varlığa ilişkin izlerin bilinmesi açısından önemlidir. Belgeye ilişkin izlerin daha iyi anlaşılması hangi sistem ve yazılım olursa olsun belgenin yaşam evrelerinin bilinmesini gerektirir. Aşağıda belgenin yaşam evrelerine bağlı olarak belge varlığı ve izleri tartışılmaktadır.

3.1.1. Elektronik Ortamda Belge Üretim Süreci

Elektronik ortamdaki belgelerin üretilmesi diğer ortamlara göre içerik, kurumsal ve yasal nitelikleri bakımından aynı özellikleri taşır. Bulunduğu ortam gereği farklılık arz eder.[4] Belge bulunduğu ortama bakılmaksızın idari faaliyetler sonucunda oluşan, yazışmalar, formlar, talimatlar, raporlar vb. nedenlerle üretilirler.[5] Bu faaliyetler, bir politikanın, alınan kararların, eylem ve işlemlerin, kurumsal içeriğe uygunluğun, düzenlemelere ve mevzuata uygunluğunun kanıtıdır. Faaliyetler söz konusu amaçların

[3] Dartmouth College, **The Document Life Cycle: Definitions, Supporting Technologies, and Applications**, (Çevrimiçi) https://www.dartmouth.edu/~library/recmgmt/forms/DocLifeCycle.pdf, 6 Ocak 2019.

[4] Niyazi Çiçek, **Kurumsal Bilgi ve Belge Yönetimi**, 2. bs., İstanbul, Marmara Belediyeler Birliği Kültür Yayınları, 2018, s. 110.

[5] Fahrettin Özdemirci, **Kurum ve Kuruluşlarda Belge Üretiminin Denetlenmesi ve Belge Yönetimi**, İstanbul, Türk Kütüphaneciler Derneği, 1996, s. 28.

yanı sıra çalışma ortamındaki meslektaşların ne yaptığı (tecrübesinden faydalanmak adına) ve ne karar alındığının, bunların sonradan hatırlanarak benzer konularda hangi kararların alınması noktasında yardım alma, proje ve süreçlerin ilerlemesini izleme adına birer kanıt gibi birçok amaçla yapılır. Özetle, süreç analizinde ihtiyaç duyulan güncellemelerin bilgisi böylelikle edinilmiş olur.[6] EBYS'lerde belge yönetimi,

"*belge üretim işlemleri, belge şablonları, belge hiyerarşisi, dosyalama, belge işlem süreçlerinin (kurum içi ve kurum dışı güvenli belge gönderimi ve alımı, belge arama belge niteleme ve dizinleme, barkod kullanımı, belge/dosya transfer işlemleri, belge/dosya değerlendirme-ayıklama-imha işlemleri vb.) diğer bileşenlerle entegre olarak yürütüldüğü ana bileşendir.*"[7] Şeklinde açıklanmaktadır.

Kamu kurum ve kuruluşlarında belgeler üç süreç sonunda üretilir. Bu süreçler;[8]

- Kâğıt ortamın dijitalleştirilmesi sürecinde üretilen belgeler: Bu süreç çoğunlukla belgelerin tarayıcılar marifetiyle dijital ortama aktarımı şeklinde kurum içinde veya kurum dışında (dış kaynaklı hizmet alımı*) gerçekleşir.
- Yapılandırılmamış elektronik belgeler: Ofis uygulama formatları (Open Document Format-ODF, PDF ve Office Open XML Format-OOXML gibi) ile birey veya kurumların e-posta yoluyla veya diğer özel elektronik sistemler aracılığıyla gönderilen belgelerdir.
- Yapılandırılmış elektronik belgelerle üretilen belgeler: Bu belgeler bir birey veya kurum tarafından web ortamından veya özel amaçlı yazılım uygulamaları aracılığıyla veya bir kamu yönetimi içinde dâhili olarak oluşturulmuş olan belgelerdir.

Yukarıda belirtilen süreçlere bağlı olarak yapılması gerekli bazı kurumsal işlemler aşağıda açıklanmıştır. Bunları açıklamadan önce süreçlerde kullanılan ve tanımlanması konunun daha iyi anlaşılmasını sağlayacak olan bazı kavramların açıklanmsı gerekmektedir. Bunlar; yapılandırılmamış ve yapılandırılmış verinin tam olarak neyi ifade ettiği ve belgelerin güvenirliği ile ilgili neyin kastedildiğidir. Yapılandırılmamış

[6] The National Archives of United Kingdom, **Records Management Guides-4:Active Records Management: Records Creation**, 2006.

[7] Fahrettin Özdemirci v.d., **Elektronik Belge Yönetimi ve Arşivleme Sistemi: Geçiş Süreci ve Uygulama Yönetimi**, Ankara, 2013, s. 81.

[8] eDocuments, "Creation of e-Documents,"

* Bu süreç riskli olabilir. Bu sebeple kurum içi yapılması tercih edilmelidir.

veri, kurumsal veri tabanında bulunmayan, elektronik posta mesajları, kelime işlem belgeler, videolar, fotoğraflar, ses dosyaları, sunumlar, web sayfaları ve diğer birçok kurumsal belgeyi ifade eder.[9] Yapılandırılmış veri, bir kayıt veya dosya içindeki sabit bir alanda bulunan verileri ifade eder. Bu ilişkisel veritabanlarında ve elektronik tablolarda bulunan verileri içerir. Verinin hangi ortamda ve nasıl bulunacağını tanımlar.[10] Yapılandırılmamış ve yapılandırılmış verinin kullanılarak kurumsal belge üretiminin elektronik imza, elektronik mühür, elektronik zaman damgası ve bunların doğrulanması - onaylanması işlemleri, belgelerin güvenirliği olarak tanımlanır.[11]

3.1.1.1. Kâğıt Belgelerin Elektronik Ortama Aktarılma Sürecinde (Dijitalleştirme) Üretilen Belgeler

Kâğıt belgelerin elektronik ortama aktarılma süreci, kâğıt ve dijital ortam arasında köprü görevi görür. Elektronik ortama aktarılma işlemi sırasında/sürecinde dokümanların içeriklerinin eklenti programlar kullanılması (OCR, ICR gibi) yöntemiyle otomatik olarak sistem tarafından işlenmesi sağlanır ve bu süreç idari işlemlerde kâğıt belgenin ortadan kalkmasının ilk adımını temsil eder. Mümkün olduğunda, yapılandırılmış veriyi sayısallaştırılmış belgelere, örneğin, üstveri düzeyinde, belgenin kullanıldığı içeriğe göre gerekli alanların doldurulmasıyla ilişkilendirilmesi önerilmektedir. Dijitalleştirme süreci, kâğıt ortamdaki belgelerin birey veya tüzel kişi tarafından ilgili birime teslimi ile başlar. Bazı hallerde/durumlarda kâğıt belgelerin elle imzalanması da gerekebilir. Bundan sonra, genellikle aşağıdaki adımlar takip edilir:

- Tarama Süreci: Bu işlemin kurum içerisinde tarama işleminden ve tarama çıktı kalitesinden sorumlu bir kurum çalışanı tarafından gerçekleştirilirmesi tercih edilir. Barındırma maliyet ortamı kaynaklı sebeplerden dolayı kurum dışı yapılması da tercih edilebilir. JPEG (Birleşik Fotoğraf Uzmanları Grubu-Joint Photographic Experts Group), TIFF (Etiketli Görüntü Dosyası Formatı-Tagged Image File Format) veya PNG (Taşınabilir Ağ Grafiği-Portable

[9] Vangie Beal, "Unstructured Data," (Çevrimiçi) https://www.webopedia.com/TERM/U/unstructured_data.html, 13 Ekim 2019.

[10] Vangie Beal, "Structure Data," (Çevrimiçi) https://www.webopedia.com/TERM/S/structured_data.html, 13 Ekim 2019.

[11] eDocuments, "Trust Management Service," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/index6e40.html?page_id=759, 13 Ekim 2019.

Network Graphic) gibi dijital görüntüler için desteklenen birkaç formatta tanımlanır. Ayrıca, taranmış dijital görüntülerin minimum kabul edilebilir bir çözünürlüğünün tanımlanması önemlidir. Örneğin 300, 400, 600 veya 1200 DPI (Dots Per Inch-İnç Başına Nokta Sayısı) gibi. Taranmış görüntülerin aktarılacağı programların ve kullanılacağı yerlerin minimum ve maksimum çözünürlük ihtiyacı belirleyici olmalıdır. (örneğin OCR, ICR programlar…)

- Tarama sürecinden sonra elektronik ortamdaki belgeler kurumlarca aşağıdaki adımlar çerçevesinde işlenir:
  - ✓ Üstveri ekleme süreci: Bu aşamada elektronik belge ile ilişkilendirilen üstveriler, yeni oluşturulan belge hakkında amaç, köken, oluşturma zamanı vb. gibi gerekli bilgilerin sağlanmasına yardımcı olur. Dijital belgeler için "tanımlayıcı üstveri" kullanılır. Tanımlayıcıların temel amaçları, elektronik belgenin keşif ve tanımlamasını sağlamaktır.
  - ✓ Doğrulama süreci: Taranan elektronik belgelerin orijinale uygunluğunu (kanıt olarak değeri) ve geçerliliğini doğrulamak için (duruma özel), söz konusu belgeler elektronik olarak mühürlenir veya bir çalışan tarafından kurum adına imzalanır. Ayrıca, işleyişe göre kurum prosedürüne bağlı olarak, belgenin kurumsal EBYS'ye dâhil olduğunu gösteren resmi niteliği ve zorunluluğu olan ve elektronik belge üzerinde gösterilen bir zaman damgası uygulanır.
  - ✓ Belge tanımlayıcı ile kodlama: Daha sonra elektronik belgelere özgü bir güvence türü olarak, özgün bir belge tanımlayıcıyla (Unique Document Identifier-Doğrulama Kodu) kodlanır. Doğrulama kodu, hem kâğıt (elektronik ortama aktarılmış) hem de elektronik olarak üretilmiş belgeler dâhil, tüm yaşam döngüleri boyunca elektronik belgelerin özgün bir şekilde tanımlanmasına olanak tanır. Çoğunlukla elektronik olarak verilen tüm belgelerde görünen, bu nedenle basılı kopyaların doğruluğunu onaylayan alfasayısal bir koddur. Gösterge mekanizması, elektronik olarak imzalı belgeye dayanan (bir karma tekniği ile) ve birçok iletişim kanalı (e-posta, basılı damga) yoluyla çeşitli paydaşlara (bireyler, kurum çalışanları) iletilen bir doğrulama kodunun kullanılmasına dayanır. Çevrimiçi bir doğrulama servisi aracılığı ile herhangi

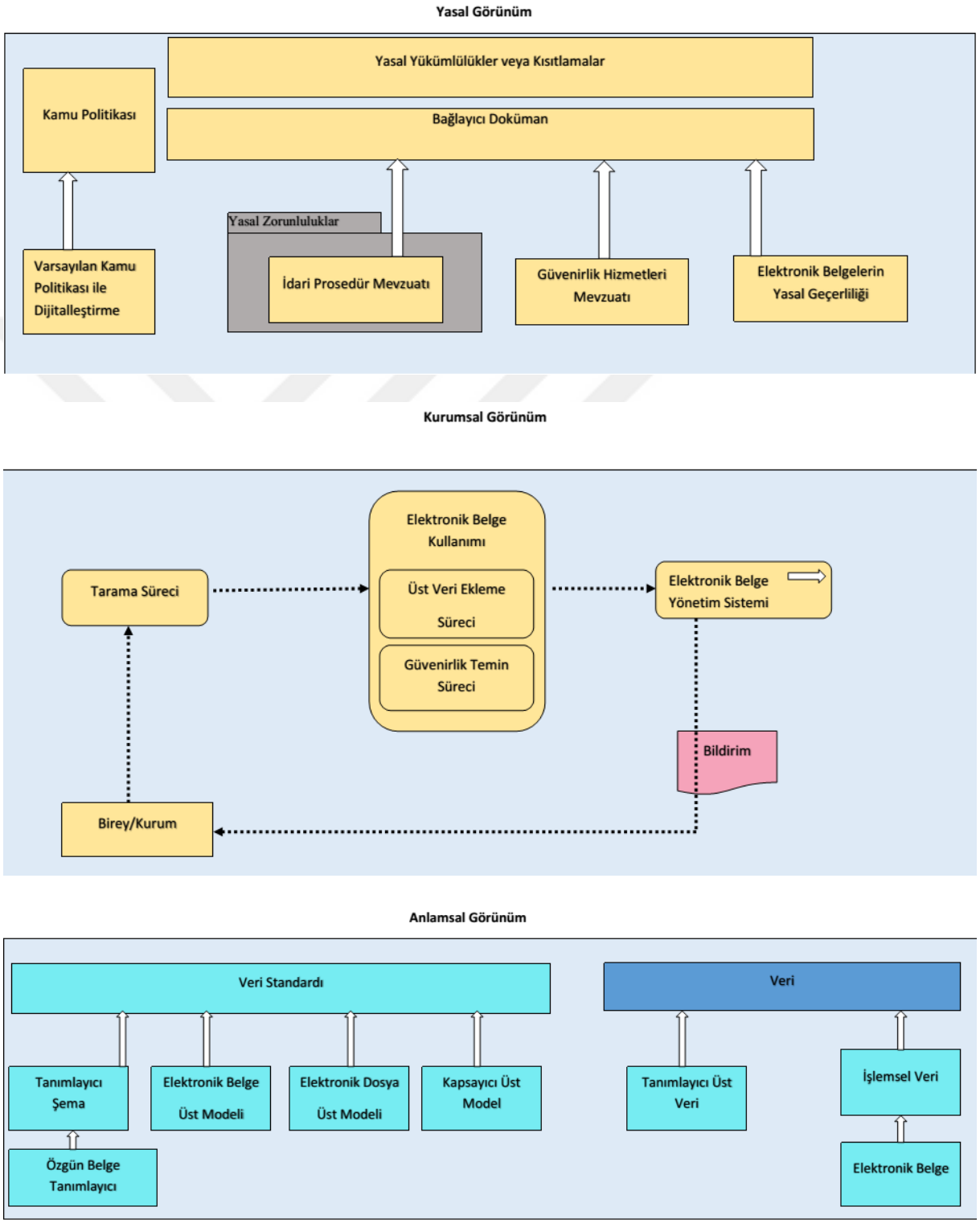
bir paydaş imzalı bir belgenin gerçekliğini doğrulayabilir veya hatta belgeyi alabilir. Çoğu zaman, bu kodun hatırlanması ya da ilgili doğrulama portalı formuna manuel olarak kopyalanması zordur; dolayısıyla otomasyon seviyesini arttırmayı amaçlayan bazı tamamlayıcı teknikler kullanılır. Böyle bir teknik, kendi başına doğrulama kodunun ve doğrulama URL (Uniform Resource Locator, Standart Kaynak Bulucu)'sinin QR[12] (Quick Response Code, Hızlı Yanıt Kodu) biçiminde kodlandığı QR gömme tekniğidir. Bu şekilde, kodu almak için herhangi bir QR okuyucu (pratik olarak herhangi bir akıllı telefon) kullanılabilir. İspanya'da böyle bir mekanizmaya örnek olarak, genellikle İspanyol yönetiminde kullanılan bir elektronik belgenin elektronik parmak izi olarak ifade edilen Güvenli Doğrulama Kodu (Computerized System Validation, CSV) verilebilir. Elektronik belgeler ve elektronik dosyalar için bir güven yönetimi bileşeni olarak düşünülebilir.

Son olarak, yukarıda açıklanan elektronik belgenin ilk kullanımından sonra belge, ilgili kurumun EBYS'sine girer. Bu noktada, bir birey / kurum tipik olarak, oluşturulan elektronik belgeye daha fazla erişim için kullanılan özgün belge tanımlayıcıyı da içeren bir kabul bildirimi alır. Böylece kâğıt ortamdaki belgelerin kurumsal EBYS'ye geçişi sağlanmış olur. Kâğıt belgelerin elektronik ortama aktarılma sürecinde dijitalleştirme süreci geçirmiş kâğıt belgelerin durumuna ilişkin bilgilere kurum politikalarında yer verilmesi de bu sürecin bir parçasıdır ve üzerinde düşünülmesi gereken önemli bir konudur. Bu süreç ile ilgili şekil aşağıda verilmiştir.[13]

[12] QR Kodu, temel işlem, web sitesi adresleri, metin bilgileri, kartvizit türü verileri için iletişim bilgileri ve diğer birçok kullanım gibi büyük miktarda karakter kodlayabilen iki boyutlu bir barkoddan oluşur (State of Indiana, "What Is a QR Code and How Is It Used on IN.GOV?", (Çevrimiçi) https://www.in.gov/core/qr_code.html, 13 Ekim 2019).

[13] eDocuments, "Digitisation of Paper," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/index5534.html?page_id=6, 13 Ekim 2019.

Şekil 3.1: Dijitalleştirmeyle Üretilen Belgelerin Yasal, Kurumsal, Anlamsal ve Teknik Görünümü



(**Kaynak:** eDocuments, "Digitisation of Paper," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/index5534.html?page_id=6, 13 Ekim 2019; Yazar tarafından Türkçe olarak yeniden hazırlanmıştır.)

3.1.1.2. Yapılandırılmamış Elektronik Belgelerle Üretilen Belgeler

Kâğıt ortamdaki belgelerin dijitalleştirilerek kurumsal belge yönetim sistemine katılmasından sonra yapılandırılmamış elektronik belgelerle ilgili işlemler şu şekilde modellenebilir:[14]

- Birey / Kurum Kimlik Doğrulama Süreci; bu süreç, bir belgenin üreticisinin gerçekten talep oluşturup oluşturmadığının kanıtı için hizmet eder.
  - ✓ Güvenirlik Sertifika Süreci; belgenin elektronik olarak imzalanması sürecinin kişiler açısından güvenirliğini ifade eder. Elektronik imzalamayı gerçekleştirmek için gerekli referanslar olan özel veya açık anahtarlar bu kapsamda düşünülebilir. Bunlar genellikle devlet tarafından verilen kimlik belgesinin bir parçası olarak sağlanır, ancak belirli bir amaç için oluşturulmuş bir kimlik bilgisi de olabilir.
  - ✓ Ek Güvenlik Süreci; kapsamlı kurumsal işlemlere, şifreleme gibi ek güvenlik kontrolleri eklenmesini sağlayan süreçtir. Örneğin şifreli bir iletişim protokolü kullanarak aktarım düzeyinin sağlanmasıdır. Bu düzey genellikle belge veya taşıyıcı depolama aracını kapsar. Örneğin XML şifreleme gibi.

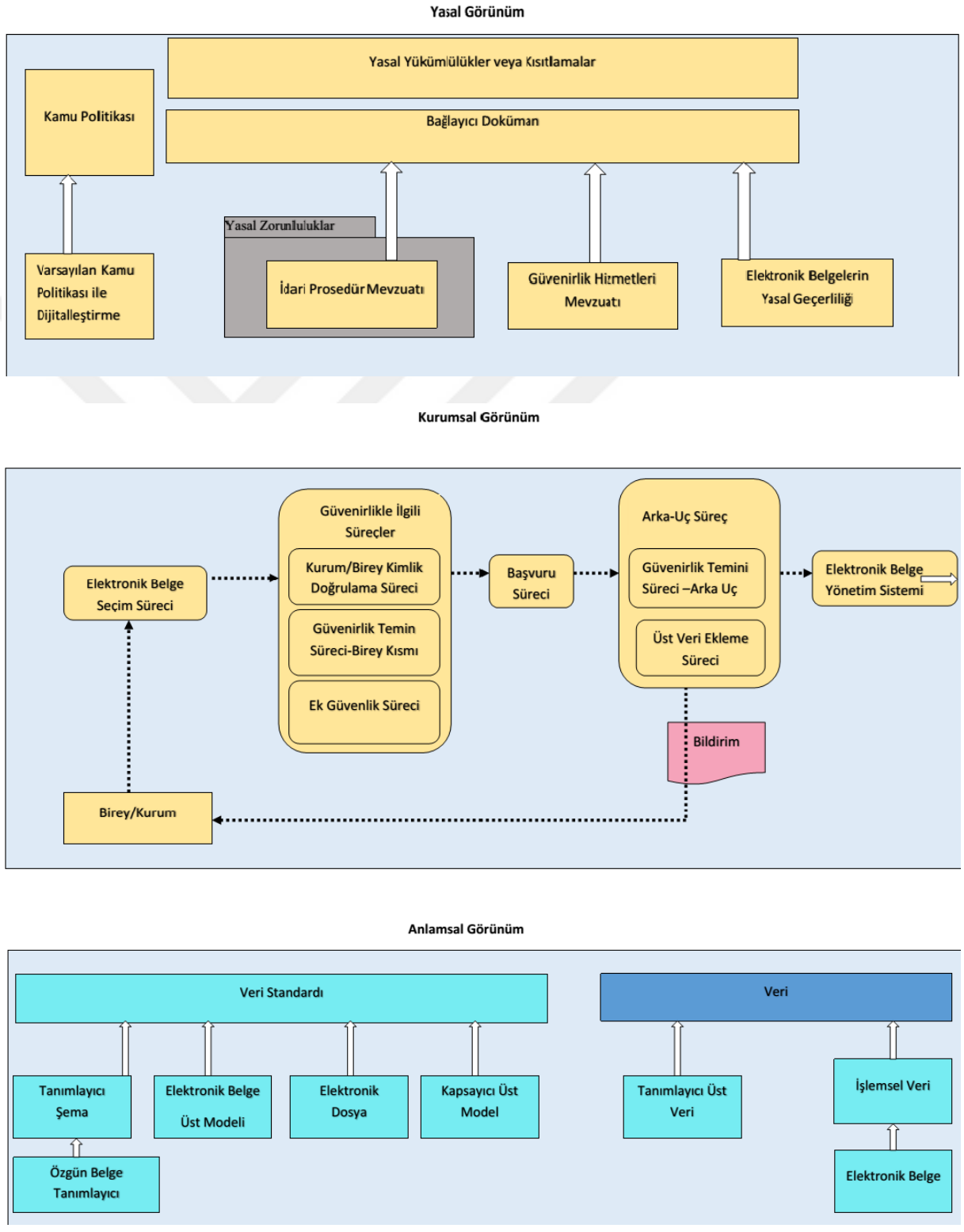
[14] eDocuments, "Creation of Unstructured e-Documents," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/index9902.html?page_id=46, 13 Ekim 2019.

- Güvenirlikle ilgili süreçlerin yerine getirilmesinden sonra, ilgili birime bir elektronik belge sunulur. Belge alındığında, birim tarafından gerçekleştirilen bazı arka uç (back-end) işlemleri vardır. Bu işlemleri aşağıdaki gibi sıralayabiliriz:
    - ✓ Bir birey/kurum tarafından oluşturulan güvenirlik bileşenlerinin onaylanması dâhil olmak üzere güvenirlik sağlayan arka uç süreci. Örneğin elektronik imza doğrulama/onaylama, elektronik imzalar, mühürler ve zaman damgalarını kapsar.
    - ✓ Üstveri ekleme süreci. Örneğin MoReq2010'da önceden tanımlanmış bir bağlamsal üstveri öğeleri grubunun aynı anda bir varlığa eklenmesine izin verilir. Bunun için de bir üstveri öğe tanımları listesini içeren üstveri şablonları sisteme tanımlıdır. Üstveri şablonları, belirli bir hizmet veya sınıflandırma altında oluşturulmalarının bir sonucu olarak üretilen varlıklara uygulanabilmektedir.[15] Özetle belge üretiminde zorunlu alanların sistem tarafından tanımlanmış olması gerekir.
- Son olarak, elektronik belge kurumsal belge yönetim sistemine dâhil olmuş olur.

Yapılandırılmamış veriyle belge üretim sürecinin yasal, kurumsal, anlamsal ve teknik görünümü aşağıdaki şekilde gösterilmiştir.

[15] DLM Forum Foundation, **MoReq2010®: Modular Requirements for Records Systems — Volume 1: Core Services & Plug-in Modules**, 2011, s. 100. (Çevrimiçi) http://moreq2010.eu/, 31 Ocak 2019.

Şekil 3.2: Yapılandırılmamış Veriyle Üretilen Belgelerin Yasal, Kurumsal, Anlamsal ve Teknik Görünümü



(**Kaynak:** eDocuments, "Creation of Unstructured e-Documents," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/idex9902.html?page_id=46, 13 Ekim 2019; Yazar tarafından Türkçe olarak yeniden hazırlanmıştır.)

3.1.1.3. Yapılandırılmış Elektronik Belgelerle Üretilen Belgeler

Yapılandırılmış elektronik belgeler, ilgili birimde çoğunlukla aşağıdaki yöntemlerden biriyle yapılır:[16]

- Bir birey veya kurum tarafından gönderilen belgeler için: Bu süreç, bir web portalı veya bu amaç için geliştirilmiş bir yazılım uygulaması aracılığıyla önceden tanımlanmış ve yapılandırılmış bir formun doldurulması ile başlar. Ardından, yapılması gereken bazı güvenirlik ile ilgili süreçlerle devam eder. Bu işlemlerden bazıları isteğe bağlı olabilir ve gerçek sıraları belirli bir duruma bağlı olarak değişebilir. Güvenirlik ile ilgili süreçler genellikle şunları içerir:
  - Birey / Kurum Kimlik Doğrulama Süreci; bir belgenin üreticisinin gerçekten talep oluşturup oluşturmadığının kanıtı için gerekli bilgileri sağlar.
  - Güvenirlik Sertifika Süreci; kapsamlı bir idari prosedür gerektiriyorsa, belgenin elektronik olarak imzalanması sürecini ifade eden kişiyi ilgilendiren süreçtir. Elektronik imzayı gerçekleştirmek için gerekli referanslar olan

[16] eDocuments, "Creation of Structured e-Document," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/indexe527.html?page_id=71, 13 Ekim 2019.

açık anahtar sertifikası, genellikle devlet tarafından verilen kimlik belgesinin bir parçası olarak sağlanır, ancak belirli bir amaç için belirlenmiş bir kimlik bilgisi de olabilir.

- Ek Güvenlik Süreci; kapsamlı idari işlem gerektiriyorsa, şifreleme gibi ek güvenlik kontrolleri eklenmesini sağlar. Örneğin şifreli bir iletişim protokolü kullanarak aktarım düzeyinin sağlanmasıdır. Bu düzey genellikle belge veya taşıyıcı depolama aracını kapsar. Örneğin XML şifreleme gibi.

- Kurum içinde hazırlanan belgeler için: Birim içindeki yapılandırılmış elektronik belgeler, kurumda kullanılan elektronik belge sistem yazılımları kullanılarak oluşturulabilir. Daha da özelleştirilirse, temel veri girişi EBYS yazılımı içinde metin editörü ile üretilir. Bu durumda, belge üretimini tetikleyenlerin en önemlisi olan form işleme süreçlerinin anlaşılması önemlidir. Form işleme süreçleri, belge üretim sorumluğunun başlayıp paraf ve onay makamlarınca gözden geçirildikten sonra formların belge olarak şekil bulmasıdır. Hangi yolla olursa olsun belge üretim sorumluluğu kurumlarda belge üretiminin başladığı aşamadır. Bu aşamada kişilerin işlemleri dokümana dönüşür. Paraf ve onay mercilerinden onay ve imzalar tamamlanmışsa söz konusu doküman belge olarak tanımlanır. Belgeler işlemlerin birer kanıtı olarak tutulur. Saklama planlarıyla beraber birimlerde ve kurumlarda saklama sürelerinin tamamlanması beklenir. Kurumlar form işleme süreçleriyle elektronik formların oluşturulması ve kullanılması, kurumların standart bir formatta veri toplamalarını ve verileri otomatik olarak bir EBYS çözümüne girmelerini veya yüklemelerini sağlar. Elektronik formlar genellikle bir form tasarım paketi kullanılarak veya standart HTML editörleri kullanılarak oluşturulur. Form tasarım paketleri tipik olarak yalnızca form tasarım bileşenlerini değil, aynı zamanda kuruluşların formdaki her alanı "etiketlemesini" veya tanımlamasını ve bu verileri bilgileri alacak ve daha sonra işleyecek bir veri tabanı veya

uygulama ile ilişkilendirmesini sağlar. Bu form yönetimi araçları ayrıca kurumların veri girişini kolaylaştırmak için tamamlandıkları gibi formlar üzerinde düzenleme kontrolleri yapmasını ve / veya düzenlemelerini sağlar."[17]

Yapılandırılmış elektronik belgeler HTML, XHTML, XML, LaTeX ve Microsoft Word'ün .doc formatı gibi formatlarla temsil edilir. Ofis, web tarayıcıları, sunum paketleri, çevrimiçi form işleme sistemleri ve diğer birçok yazılım paketi tarafından kullanılırlar. Yapılandırılmış elektronik belgeler çoğunlukla tek tek karakterleri veya karakterleri temsil etmek için basit kodlar kullanarak okuma sırasında bir metin kodlaması içerir. Metin kodlamasında başlık, sayfa numaraları, konu başlığı, yazarlar, metnin bölümleri gibi farklı bölümlerin mantıksal işlevleri açıklamalarda veya "işaretleme" kısımlarında bulunur. Yapılandırılmış elektronik belgeler ayrıca metnin görünümü ile ilgili olan yazı tipleri, yazı tipi stilleri, yazı tipi boyutu, renkler ve çizimler içerebilirler.[18] Bu bilgiler EBYS'ler içinde belge üretimine yardımcı bileşenler olarak karşımıza çıkmaktadır. Bunun haricinde taranarak sisteme aktarılan belgelerde sistem içinde belge varlığına katkıda bulunmaktadır. Yine elektronik mail, ses dosyaları, video klipleri, dijital şema ve haritalar, yapılandırılmış veri, veritabanları, çoklu medya dokümanlarının hepsi sistem içinde belge türleri arasında sayılır. Sayılan bu tüm belge üretim veya sağlama yolları kurumdan kuruma değişiklik göstermekle beraber EBYS sistem kriterlerine göre şekillenir.[19] Burada ifade edilen kanallar tam bir listeyi yansıtmamaktadır. Çünkü yazılım ve donanımın gelişen teknolojiyle belge varlığına daha fazla çeşitlilik katacağı kaçınılmazdır.

Yapılandırılmış elektronik belge kurumsal belge yönetim sistemine dâhil olduğunda, kurum tarafından gerçekleştirilen ek işlemler de vardır. Bu işlemler aşağıdaki gibi sıralanabilir:

---

[17] Association for Information and Image Management International (AIIM), **Recommended Practice: Analysis, Selection, and Implementation of Electronic Document Management Systems (EDMS)**, AIIM International, USA, 2009, s. 18.

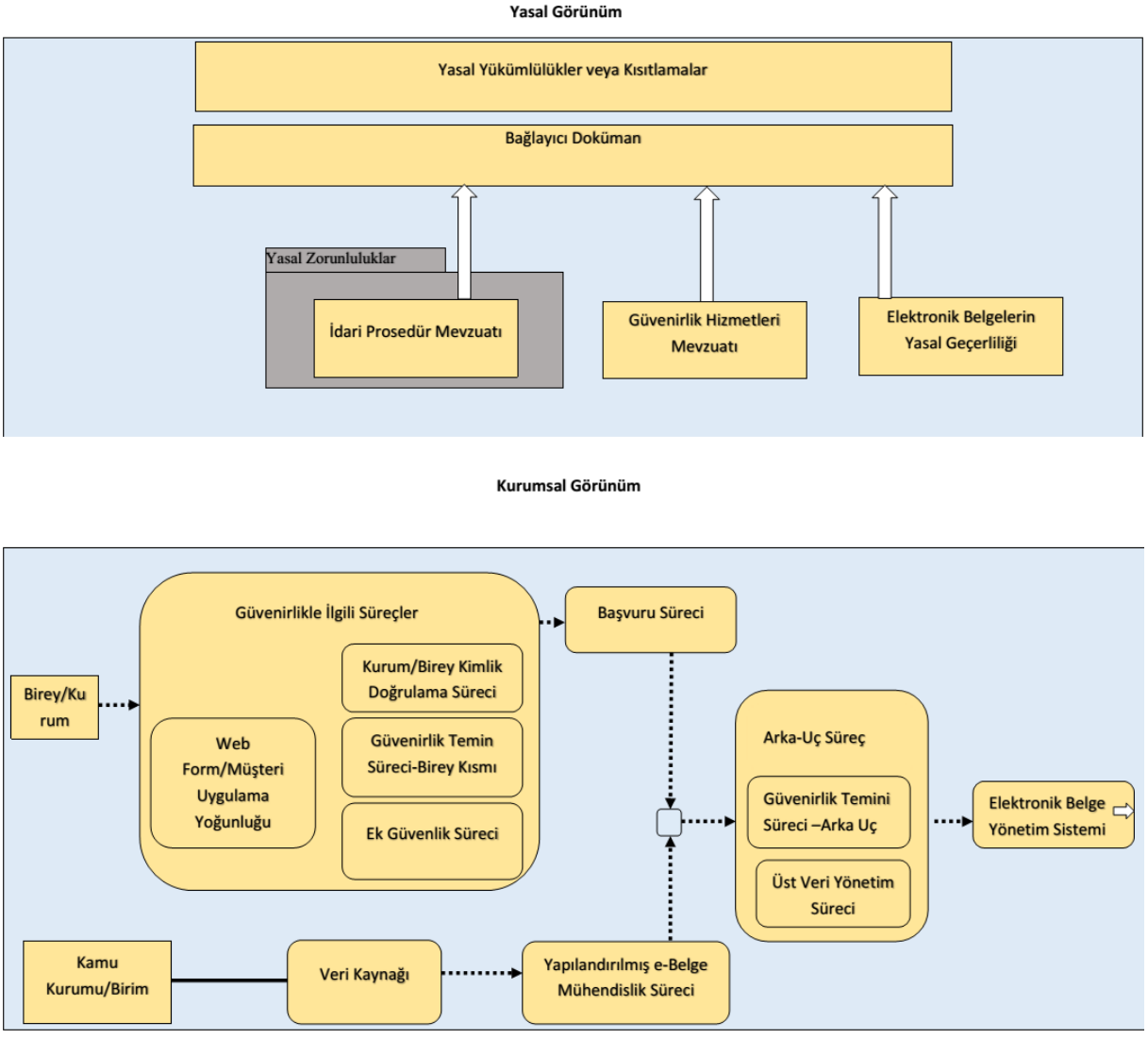
[18] Thomas M. Breuel, "The Future of Document Imaging in the Era of Electronic Documents," s. 4, (Çevrimiçi) https://pdfs.semanticscholar.org/8867/20e7c6fae33799e9768af3e365dde4f8d6ac.pdf, 19 Şubat 2019.

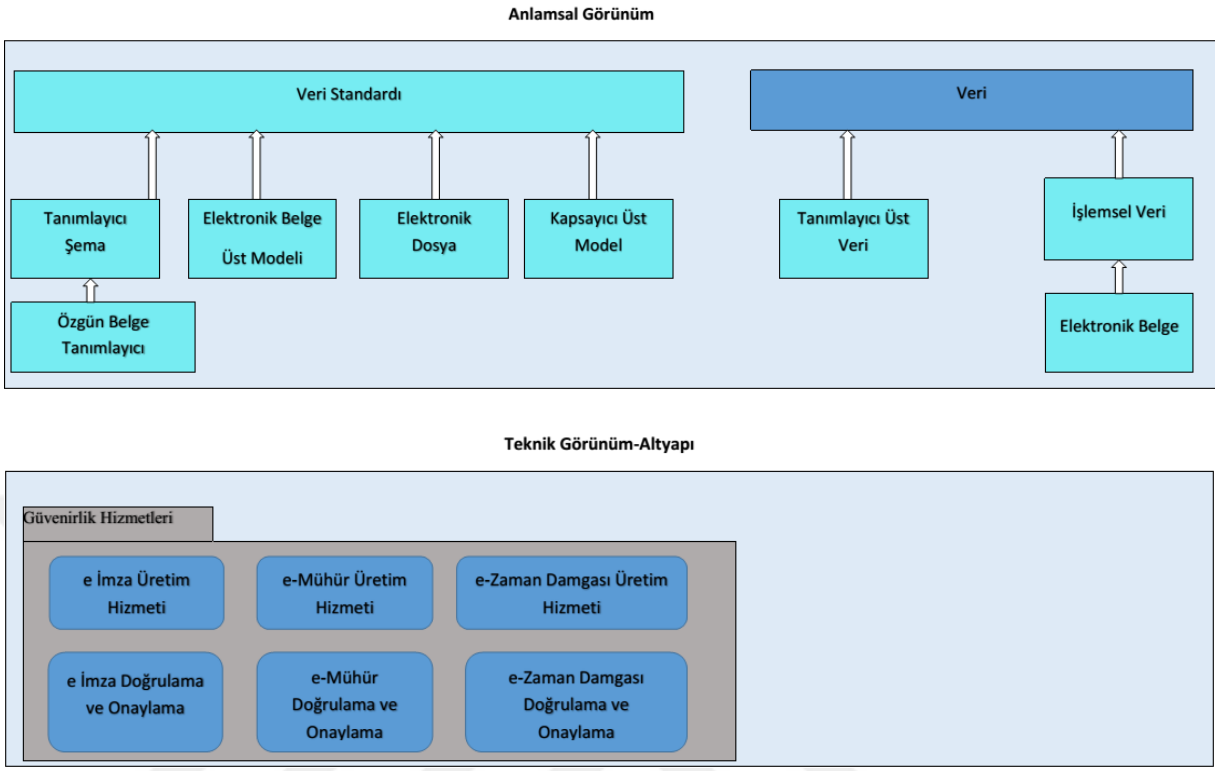
[19] European Communities, **MOReq: 2001**, s. 44-46.

- Bir birey/birim tarafından oluşturulan güvenirlik bileşenlerinin onaylanması dâhil olmak üzere güvenirlik sağlayan arka uç süreci. Örneğin elektronik imza doğrulama/onaylama, elektronik imzalar, mühürler ve zaman damgalarını kapsar.
- Üstveri ekleme süreci

Son olarak, elektronik belge kurumsal EBYS'nin bir parçası haline gelir. Yapılandırılmış veri süreçleri aşağıdaki şekilde gösterilmektedir.

Şekil 3.3: Yapılandırılmış Veriyle Üretilen Belgelerin Yasal, Kurumsal, Anlamsal ve Teknik Görünümü

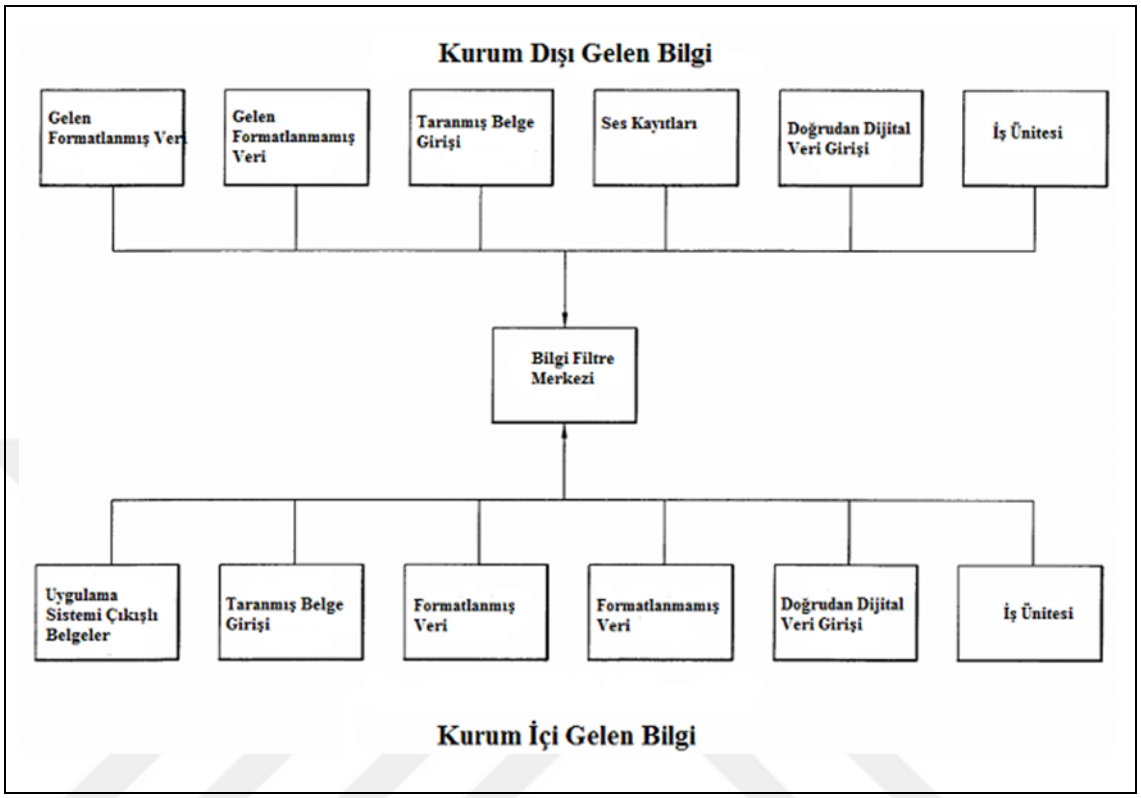




(**Kaynak:** eDocuments, "Creation of Structured e-Document," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/indexe527.html?page_id=71, 13 Ekim 2019; Yazar tarafından Türkçe olarak yeniden hazırlanmıştır.)

Yukarıda ifade edilen üç farklı belge üretim süreci farklı şekilde de düşünülebilir. Bir kurumda EBYS sistemine eklenen veya üretilen belgeler, kurum içi ve kurum dışı faaliyetlere dayalı olmak üzere ikiye ayrılabilir. Kurum içi olsun veya kurum dışı her iki şekilde de belge üretim süreçlerine yardımcı olan veri akış göstergeleri bulunur. Bunlar, kurumun belge elde etmesini tetikleyen unsurlar olarak da ifade edilebilir. Söz konusu unsurlar aşağıdaki tablodaki gibi belirtilebilir.

Şekil 3.4: Kurum İçi ve Kurum Dışı Gelen Bilgi



(**Kaynak:** Judy J. Johnson ve James R. McElroy, Computer Based Records Management System Method, United States of America, Patent Number: 5.813.009, Sep. 22, 1998.)

Şekle göre kurumlarda belgeye dönüşen bilginin çeşitli yollarla olduğu görülmektedir. Bu yollar temel iki kategori olan kurum içi ve kurum dışı olmak üzere ikiye ayrılmaktadır. Kurum içi gelen bilgiler kendi arasında farklılık taşımaktadır. Bunlar, kurumsal diğer uygulamalardan gelen veri, kâğıt ortamdaki belgelerin taranarak sisteme dâhil edilmesi, formatlanmış veri, formatlanmamış veri, dijital aygıtlarla direk sisteme dâhil edilen veri ve son olarak metin editörü ile üretilip belgeye dönüşen bilgi (iş ünitesi) olmak üzere altı kısıma ayrılmaktadır. Kurum dışı gelen veri de aynı şekilde altı kısıma ayrılmaktadır. Kurum içi gelen bilgilerden farklı olarak ses kayıtları şeklinde gelen veri belirtilmiştir. Diğer veri çeşitleri aynıdır. Bu çeşitlere ek olarak gelişen teknoloji ürünlerine bağlı olarak günümüzde yaygın olarak kullanılan mobil cihazlardan gelen veriler ve bulut bilişimden gelen veriler de kurum içi ve kurum dışı gelen bilgiler içinde yer alabilir.

Türkiye'de EBYS yazılımları için uygunluk alınan temel doküman olan TS 13298 (2015) nolu standarda göre belge üretimi yukarıda yapılan açıklamalara uygun olarak yapıldığı söylenebilir. Nitekim standartta;[20]

"*elektronik belgeler kurumsal fonksiyonların yerine getirilmesi sırasında üretilir veya alınırlar. Kurum içinde üretilenler yanında kurum dışı kaynaklardan da belge akışı söz konusudur. Bu belgeler farklı kişi ve kurumlar tarafından üretilmiş farklı formatlarda olabilirler. Belgeler tek ünite şeklinde olabileceği gibi belge grupları şeklinde de olabilirler. Yerel veya geniş alan ağları, elektronik posta veya faks gibi elektronik araçlarla iletilebildikleri gibi sayısallaştırma yöntemiyle de elektronik ortama aktarılmış olabilirler.*" İfadesi yer almaktadır.

Bunlar haricinde kurumsal faaliyetler, kurum dışı gerçek ve tüzel kişilerden alınan belgelerin işleme alınmasıyla da yerine getirilebilir.[21] TS 13298'e göre açıklanan belge üretimi yukarıda ifade edilen aşamalarla örtüşmektedir.

3.1.1.4. Belgenin Sahip Olması Gereken Özellikleri

Üretim süreçleri tanımlandıktan sonra EBYS'lerde üretilen belgelerin sahip olması gereken bazı özellikleri vardır. Bu özellikler uluslararası olması yanında ulusal olarak kabul edilen TS ISO 15489 nolu enformasyon ve dokümantasyon – belge yönetimi standardında orijinallik, güvenirlilik, bütünlük ve kullanılabilirlik olarak ifade edilmektedir.[22] TS 13298'de ise bu özellikler; tanımlanabilirlik, bütünlük, onay ve kayıt bilgisi, yapısal özellikler, üretim sorumluluğu ve mülkiyet hakları ve son olarak da teknolojik özellikler şeklindedir.[23] EBYS'ler, kâğıt ortamdaki bir belgeyle aynı hukuki değeri taşıyabilmesi için elektronik belgelerin de kâğıda atılan imza gibi kimlik doğrulama aracına ihtiyaç duyar. Bunun için de Türkiye'de 2004 yılında yayınlanan elektronik imzaya ilişkin elektronik imza kanunu, el ile atılan imza değerine mukabil elektronik ortamda kullanılabilecek hukuki araçları zorunlu kılmıştır. Elektronik imza, kanun metninde[24] "*başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi*" ifade eder şeklinde açıklanmıştır. Bu kanunla beraber elektronik ortamda kamu evrakının üretimi yasal bir çerçeveye oturtulmuştur.

---

[20] TSE, **TS 13298: 2015**, İster No: 6.1.2.
[21] **A.g.e.**, İster No: 6.2.1.
[22] TSE, **TS ISO 15489-1: Enformasyon ve Dokümantasyon – Belge Yönetimi**, s. 12.
[23] TSE, **TS 13298:2015**, s. 26-31.
[24] "5070 sayılı Elektronik İmza Kanunu," **Resmi Gazete**, 23 Ocak 2004, S. 25355.

Elektronik ortamda belge üretimi hem karmaşık hem de sistemli bir yapıdadır. Karmaşık olması kullanıcılar olarak bizlerin haberi olmadan gerçekleşen bit ve byte iletişimidir. Yani kaynak kodların buluşmasıdır. Sistemli oluşu ise tamamen mantıksal ve işlemler dizgesi olmasıdır. Bu mantık ve işlemler dizgesi görevleri gereği emir komuta zinciri bağlamında istenilenleri yerine getirmektedirler. Uygulamalar açısından farklılık gösterse de temel çalışma mantığı aynıdır.

Birçok kurum ve kuruluş belge yönetim süreçlerini tamamen kâğıt ortamda veya hem kâğıt ortam hem de elektronik ortamın bir kombinasyonu olarak hibrid sistemlerde yürütmektedirler. Hem kâğıt ortamda hem de elektronik ortamda süreçlerin yönetilmesi kurumların bilgiyi kendi faaliyetlerine ilişkin olarak tutma isteğinden kaynaklanmaktadır. Elektronik iletişimin geniş çaplı kabulü ve internetin yaygın kullanımıyla kurumların kendi faaliyetlerine ilişkin belge üretimi iyice artmıştır. Elektronik belge yönetim sistemlerinin bu artışla beraber kullanılması kurumlar için önemlidir. Bu sistemleri uygulamak isteyen kurum ve kuruluşların söz konusu sistemlerle ilgili gerekli temel bileşenleri uygulamak ve ardından iş birimlerinin gerektirdiği işlevleri sisteme dâhil etmek elektronik ortamın getirdiği zorunluluklardandır. Böylelikle yeni teknolojilerin tam olarak benimsenmesi ve günlük faaliyetlerin sekteye uğratılmadan sürdürülmesi sağlanabilmektedir.[25] Elektronik belge yönetim sektöründe iyi uygulama örneklerinin ortak kavramlarla tartışılması alandaki temel teknolojilerin anlaşılması açısından yararlıdır. Ayrıca temel teknolojilerin anlaşılması bu teknolojilerdeki belge varlığına işaret eden veya bu varlığa dair izler bulundurmasının nasıl mümkün olduğunun göstergesidir.

3.1.1.5. Web Uygulamaları

Kamu kurumlarında ve özel sektörde elektronik belge yönetim sistemleri farklı yazılım uygulamalarıyla sunulabilir. Bunlar; web uygulamaları, masaüstü uygulamaları ve mobil uygulamaları olmak üzere üçe ayrılır. Masaüstü ve mobil uygulamaları web uygulamalarına bağlı olarak şekillendirilir. Bu sebeple web uygulamalarının anlaşılması her üç uygulama için de önemlidir.

[25] AIIM, **Recommended Practice Report**, s. 11.

Web tabanlı yazılımlar, yazılım kurulumu, internet uygulama sunucusu, yazılım kodu ve veritabanı kurulumuyla yapılır. Bu kurulumlardan sonra uygulama elektronik ortamda belli bir alan adıyla veya bir IP adresiyle erişime açılır. Bu sistem kurulduktan sonra istemci sunucu mantığı ile web tabanlı yazılım çalışır duruma gelmiş olur. İstemci ve sunucu arasındaki iletişimi hızlı bir şekilde sağlayacak iş çatıları kullanılır. Bu çatılar iş çatısı kütüphanelerinin desteğiyle yapılır. Sunucu tarafından yapılmakta olan işlemler sürekli olarak veri tabanından bilgiler alıp kaydeder. İşlemlerle veri tabanı arasındaki bu aksiyonlar veri tabanı için bağlantı oluşturmaktadır. Bağlantıların yoğun olması sisteme aşırı yük getirdiğinden havuz bağlantı yöntemi de kullanılmaktadır. Web tabanlı elektronik belge yönetim sistemleri, bu kurulum ve yardımcı yöntemlerden sonra genel çözüm mimarisi üzerinde kurgulanır. Elektronik belge yönetim sistemleri nesne tabanlı programlama dilleri ile geliştirildiğinden, nesneler geliştiriciler tarafından tanımlanır. Tanımlanan nesneler geliştiriciler kontrolündedir. İhtiyaca göre şekillendirilebilirler. Elektronik belge yönetim sistemlerinde söz konusu nesneler belge tabanlı çalışma olduğundan sürekli olarak evrakların belge hali kullanıcıya sunulmaktadır. Bir diğer ifadeyle evraklar kaydedilirken belge hali de ayrıca oluşur.[26] Herhangi bir kurumda merkezi bir yere konumlandırılan ve kuruma bağlı tüm birimler bağlanılan sunucu ile elektronik belge yönetim sistemi kullanılmaktadır.[27] Tek bir sunucu ve birçok istemciden oluşan bu yapı web tabanlı arayüz ile sağlanmaktadır. Web tabanlı yazılımlar, tarayıcı yüklü ve uygulama sunucusuna erişim yetkisi olan bilgisayarlarca yapılır. Yazılıma erişim IP bazlı kısıtlanabilmektedir.[28] Bu da çalışan sayısı fazla olan kurumların bu yazılımı kullanmasını kolaylaştırmaktadır.

[26] Abdulcebar On ve Necaatin Barışçı, "Web Tabanlı Elektronik Belge Yönetim Sistemi," The Second International Symposium on Innovative Technologies for Engineering and Science, ISITES2014, Karabük Üniversitesi, 18-20 June 2014, ss. 1951-1956, (Çevrimiçi) http://isites.info/PastConferences/ISITES2014/ISITES2014/papers/B6-ISITES2014ID328.pdf, 14 Mayıs 2019.

[27] Turksat Bilişim, "Belgenet," (Çevrimiçi) https://bilisim.turksat.com.tr/, 18 Mayıs 2019.

[28] Havelsan A.Ş., **Evraka Elektronik Doküman ve Belge Yönetim Sistemi, Ürün Açıklaması Dokümanı**, s. 4, (Çevrimiçi) http://www.havelsan.com.tr/files/files/document/2732018151047452_bilgi-ve-iletisim-teknolojileri-evreka.pdfa, 18 Mayıs 2019.

3.1.2. Belge Kullanım Süreci

Belgelerin üretiminden sonra üretilen belgelerin kullanımını şu şekilde açıklayabiliriz: Öncelikle EBYS'ler için belgelerin arşivlendiği bir havuza sahip olması gerekir. Fiziksel olarak, havuz bir veya daha fazla ağ tabanlı veritabanı sunucusunda bulunabilir, ancak sistemin kullanıcılarına tek bir merkezi havuz olarak görünür. EBYS kullanıcılarının, kullanıcı erişim haklarının durumuna göre havuza erişimleri sağlanır. Merkezi bir havuz yanında havuz içinde klasör yapısı da söz konusudur. Bu klasör yapısı, sistem yöneticilerinin belgelerin sistemde nerede arşivlendiğini sistematik olarak kategorize etmelerine izin vermektedir. Hiyerarşik bir klasör yapısının kullanılması, yöneticinin örgütsel yapıyı, işletme işlevli yapıyı, proje temelli yapıyı veya mülkiyet temelli yapıyı temsil etmesini ya da arşivlemenin kolaylaştırılması için dört yapının bir kombinasyonunu temsil etmesini sağlar. Bu noktada bir depolama alanı ve depolama alanı içinde klasör yapısı kullanım için önemlidir. Bundan sonra sistemdeki tüm belgelerin, belgeleri sistematik bir şekilde arşivlemek için üstveriler yardımıyla ve kullanıcıların arama ve erişim mekanizmalarını kullanarak gelecekte belgeleri bulmalarına yardımcı olmak için, klasör yapısında belgelerin sınıflara ayrılması ve dizine alınması gerekir. Sınıflandırma, dizin ve üstveri kullanımı sonrası tüm bunlar için önemli olan güvenlik konusu belgelerin kullanımı için en önemli konulardandır. EBYS'lerin hem kurumun kendi güvenliği hem de ilgili mevzuata uygunluk için belgelerin arşivlenmesi konusunda katı bir güvenlik politikası belirlemesi gerekir. Elektronik belgeler, yalnızca kurum içindeki yetkili kullanıcıların bunlara kurum içi ve/veya kurum dışı erişebileceği şekilde güvence altına alınmalıdır. EBYS yöneticileri, sistemdeki kayıt güvenliğini kolayca ayarlayabilmeleri ve sürdürebilmeleri gerekir.[29] Bütün bunlara bağlı olarak elektronik ortamda belge oluşturmanın, kullanmanın ve saklamanın dört yaygın konumu vardır. Bunlar;[30]

- Bireylerin belgelerin oluşturulmasını ve kullanılmasını kontrol ettiği kişisel bilgisayarlar;

[29] Azad Adam, **Implementing Electronic Document and Record Management Systems**, New York, Auerbach Publications, 2008, s. 17-18.

[30] International Records Management Trust, "Module 3: Managing The Creation Use And Disposal Of Electronic Records," **Training in Electronic Records Management**, Ed. Laura Millar, London, 2009, s. 15.

- Bireylerin belge oluşturmayı denetlediği, ancak bu belgeleri kuruluştaki diğer kişilerle paylaştığı paylaşılan bilgisayar sunucuları;
- Merkezi kontrol ile paylaşılan sunucular,
- Tüm bireylerin belge oluşturma ve yönetme prosedürlerini oluşturdukları ve elektronik belge veya belge yönetimi yazılımı kullanan paylaşımlı sunucular-dır.[31]

Belge kullanım sürecinde bu paylaşımlı noktaların bilinmesi imha sürecindeki belgelerin tüm bu noktalardan silinmesinin göz önünde bulundurulmasını mümkün kı-lar.

3.1.3. İmha ve Koruma Süreci

EBYS'ler belgelerin belirli bir süre için saklanılmasını veya süresiz olarak sak-lanılmasını gerektirir. Belgelerin niteliğine bağlı olarak belirlenen süre dolduğunda il-gili belgeler değerlendirmeye alınır. Bu değerlendirme, özellikle bireysel ve kurumsal olarak hassas bilgileri içeren belgeler içinse veya üçüncü kişilerin bu belgelerdeki ve-rileri birey veya kurum aleyhine kullanma riski varsa söz konusu belgeler güvenli bir şekilde imha edilir. Nitekim bir belgenin imhası söz konusu ise imhadan sonra bu bel-genin hiçbir şekilde ibrazı söz konusu olamaz. Örneğin bir bankanın müşterisine sun-duğu bankacılık hizmetleri açısından düşünülebilir. Bankanın müşterileri hesaplarını kapattıklarında, müşteri hesaplarının ayrıntılarına ilişkin bilgi ve belgeyi belirli bir süre boyunca kayıt altında tutmak zorunda kalacaktır. Türkiye'de bankalardaki hesap-lar kapandıktan sonra saklama süreleri 10 yıldır. Daha sonra, hesap kapanış tarihinden itibaren, sistem müşteriyle ve hesaplarıyla ilgili tüm detayları gelecekte on yıla kadar kayıt altında tutmalıdır. Bu süre dolduktan sonra, sistem organizasyon kurallarına bağlı olarak müşteri kayıtlarının tamamen güvenli bir şekilde sistemden silmeli ve yok

[31] Bu konumlarda söz konusu paylaşımlı sunucular, ağ sürücüleri olarak da bilinen genellikle sözcük işlem belgeleri, taranan ve fotoğraf görüntüleri, ses, video, elektronik tablolar, sunumlar ve ve-ritabanları gibi içerikleri depolamak ve paylaşmak için kullanılır. (National Archives and Records Ad-ministration (NARA), "Bulletin 2012-02," (Çevrimiçi) https://www.archives.gov/records-mgmt/bulle-tins/2012/2012-02.html, 7 Temmuz 2019).

etmelidir.[32] Kamu kurumları açısından saklama süreleri dolan belgelerin imha edilmesi bankacılık örneğinde olduğu gibi yasal bir zorunluluktur. İmha edilmeyecek olan ve belirli değerlerine göre süresiz tutulan belgeler de devlet arşivlerine devri sağlanmaktadır. Bunun yanı sıra belgelerin silinmesini gerektiren aşağıdaki durumlar da söz konusu olabilir. Bunlar;[33]

- İkili anlaşma gereği silme,
- Yeniden biçimlendirme,
- Depolama ortamı arızası ve değişimi,
- Dosya transferleri ve
- Sistemler arasında eskime ya da taşınma için depolama ortamının değişimidir.

Elektronik belgelerin silinmesi ve imha edilmesi süreci elektronik belge yönetim politikasına dâhil edilmelidir. Silme / imha talebi, bu talebin değerlendirecek yetkili otorite tarafından onaylanmalıdır. Yetkili makamdan izin alındığında uygun silme / imha işlemi uygulanır. Örneğin İspanya'da üç farklı silme/imha sürecinden bahsedilmektedir.[34] Bu aşamalar yasal yükümlülükler, kurumsal görünüm ve anlamsal görünüm açısından da aşağıdaki şekilde belirtilmiştir.

Silme Seviyesi 0: Standart işletim sistemi komutlarını kullanarak belgelerin sistemden kaldırılmasını sağlar. Örneğin bir dosyayı silmek veya SQL silmek gibi. Bu seviye, yetkisiz bilgilerin ifşa edilmesine karşı garanti vermez.

Silme Seviyesi 1: Verilerin normal sistem işlevleri veya dosya kurtarma programları kullanılarak yeniden oluşturulamamasını sağlamak için verilerin bir depolama ortamından kaldırılmasıdır. Veriler hala kurtarılabilir olabilir, ancak bu özel laboratuvar tekniklerini veya ileri düzeyde yardımcı programları gerektirir.

[32] Adam, **Implementing Electronic Document and Record Management Systems**, s. 18.

[33] eDocuments, "Deletion/Destruction of e-Documents," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/index9bef.html?page_id=54, 14 Ekim 2019.

[34] eDocuments, "Deletion/Destruction of e-Documents,"

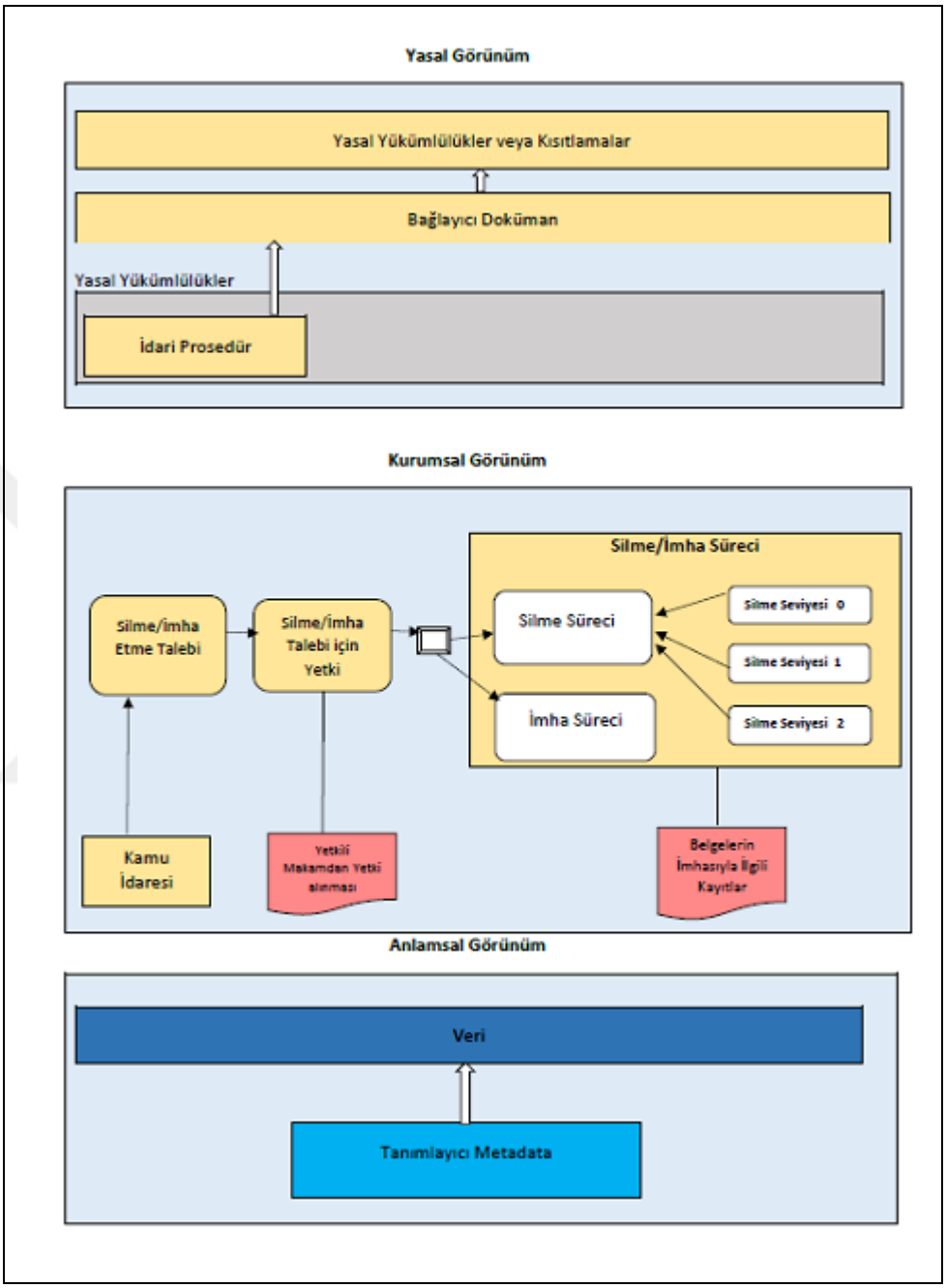
Silme Seviyesi 2: Verilerin veya bilinen belgelerin herhangi birinin kullanılmasıyla verilerin yeniden yapılandırılamaması amacıyla bir depolama aygıtından verilerin veya hassas belgelerin kaldırılmasıdır.

İmha: Depolama ortamının fiziksel olarak tahrip edilip kullanımının engellenmesidir.

İmha ve koruma sürecinde belgelerin imha edilmesi veya süresiz saklanılması öncelikle yasal zorunluluklar çervesinde şekillenmektedir. Daha sonra kurumsal öncelikler öne çıkar. Bundan sonrası için de teknik bilgi gelir ki belgelerin imhası bu teknik bilgiye bağlıdır.[35]

[35] eDocuments, "Deletion/Destruction of e-Documents,"

Şekil 3.5: Elektronik Belgelerin Silinmesi/İmhası Süreci



(**Kaynak:** eDocuments, "Deletion/Destruction of e-Documents," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/index9bef.html?page_id=54, 14 Ekim 2019.)

3.2. ELEKTRONİK BELGE YÖNETİM SİSTEMLERİNE İLİŞKİN YAZILIM İZLERİ

Yazılım izleri; uygulama izleri, veri tabanı izleri, yazılım izleri, format izleri, sürüm (versiyon) izleri, kopya ve duplikasyon izleri olarak aşağıda ayrı başlıklar halinde değerlendirilmiştir.

3.2.1. Uygulama İzleri

Bu uygulamalarda metin editörleri, sunumlar, elektronik tablolama, masaüstü hazırlanmış belgeler gibi çeşitli araçlarla belgeler üretilebilir. Elektronik belge yönetim sistemlerinde belge yönetimine ilişkin uygulamalar da bulunmaktadır. Bu uygulamaların ürettiği belgelerin de kurum saklama planlarına dâhil edilmesi göz ardı edilmemelidir. Kurumların belgeleri saklama planları çerçevesinde hangi belgenin ne kadar süre saklanacağı noktasında etkin yönetme araçları sunması gerekir. En önemli fonksiyonları otomatik saklama sürelerini sağlayabilmeleridir.[36] Bu uygulama izlerine bağlı olarak söz konusu araçlarla üretilen belgelerin saklama planlarına dâhil edilmemesi, izlere gerek kalmadan belgelere kendisine erişim sağlanmasını mümkün kılar. Böyle bir durumda imha edilmesi gereken belgeler imha edilmeden varlığını sürdürebilir. Bu belgelerin belirlenmesi için saklama kodlarına bağlı olarak aramalar yapılabilir. Saklama koduna sahip olmayan belgeler yeniden kodlanır ve saklama planlarıyla ilişkilendirilir.

3.2.2. Veri Tabanı İzleri

Veri tabanı, "çeşitli amaçlar için yönetilebilen şekilde düzenlenmiş, yapılandırılmış ve depolanmış verinin bir yazılım aracılığıyla erişilen ve güncellenen bilgiler"[37] olarak ifade edilmektedir. Kurumlardaki üretilen verinin önemli bir kısmı veri tabanlarında tutuluyor olabilir. EBYS'lerde veri tabanlarındaki belgelerin silinmesi sadece bağlantı linklerinin silinmesiyle yapılmaktadır. Linkleri silinen belgeler veri tabanlarında varlığını sürdürmeye devam eder. Kurtarma programlarının veri tabanlarındaki silinmiş bilgiye erişim sağlaması buralardaki silinen veriye ilişkin izlerden kaynaklan-

[36] AIIM, **Recommended Practice Report**, s. 17.
[37] Pearce-Moses, **A Glossary of Archival and Records Terminology**, s. 106.

maktadır. Örneğin ileri yönde kurtarma (forward recovery) ile "dosyaya yapılan değişikliklerin kronolojk olarak kaydedilmesiyle elde edilen veriyi kullanarak ve önceki bir sürümü güncelleştirerek bir dosyanın verilen bir duruma yeniden getirilmesi"[38] mümkün olabilmektedir. Bunun haricinde geri yönde kurtarma (backward recovery) ile de veri tekrar elde edilebilir. Buna örnek olarak "bir dosyanın verilen bir duruma, bu durumda olduğu zamandan beri dosyaya yapılan değişiklikleri geriye alarak yeniden getirilmesi veya daha sonraki bir sürümü ve günlük kayıt dosyasını kullanarak verinin eski sürümünün yeniden oluşturulması"[39] verilebilir.

3.2.3. Yazılım İzleri

EBYS, belgelerin üretilmesi, saklanılması ve korunması ile erişimine olanak sağlamasıyla sadece bir yazılım değil birçok bileşeni olan bir yapıdır. Bu bileşenler çeşitli yazılımlarla belge yönetimine katkı sağlamaktadır. Bu yazılımlar zaman içinde eskimeye[40] (obsolescence) uğrar ve yeni yazılımlara ihtiyaç duyulur. Eskiyen yazılım verinin okunamaması ve anlaşılamamasına neden olur.[41] Kurumlar yeni yazılımları kullanırken geride kalan eski yazılımlarda veri izlerinin kalacağını unutmamalıdırlar. Bunun için de eski yazılımların güvenli silme veya yazılım imha yoluyla tedbir almaları ve bu tedbirleri imha süreçlerine katmaları gerekir.

3.2.4. Format İzleri

Format, bir varlığa ait katman veya yapı olarak ifade edilmektedir.[42] Amerikan Arşivciler Derneği sözlüğüne[43] göre de verinin değişimi, depolanması ve sunumu için kullanılan yapı olarak açıklanmıştır. Format, özel, özel olmayan, açık kaynak ve açık standart formatları olmak üzere dörde ayrılır:[44] Elektronik belge yönetimi amaçları için kullanılacak bir dosya formatı seçerken, özel, özel olmayan, açık formatların ve açık

[38] TSE, **Bilişim Terimleri Sözlüğü**, s. 88.
[39] **A.g.e.**, s. 17.
[40] Yazılım eskimesi aynı donanım eskimesi gibi düşünülebilir. Donanım eskimesi tezin ilgili kısımlarında belirtilecektir.
[41] NAI, **Digital Recordkeeping**, s. 16.
[42] The InterPARES 2 Project, "Glossary," 2019, (Çevrimiçi) http://www.interpares.org/ip2/ip2_term_pdf.cfm?pdf=glossary, 10 Ocak 2019.
[43] Pearce-Moses, **A Glossary of Archival and Records Terminology**, s. 176.
[44] Minnesota Historical Society, "Electronic Records Management Guidelines, File Formats," (Çevrimiçi) http://www.mnhs.org/preserve/records/electronicrecords/erfformats.php 10 Temmuz 2019.

standartların belgelerin erişilebilirliğini ve hesap verebilirliğini uzun vadede nasıl etkileyebileceğini anlamak açısından önemlidir.

Özel (Proprietary) formatlar, sadece bir yazılım geliştirici tarafından kontrol edilip desteklenen formatlardır. Örneğin Microsoft Word (.DOC) formatı gibi.

Özel (Non- Proprietary) olmayan formatlar, bu formatlar birden fazla geliştirici tarafından desteklenen ve farklı yazılım sistemleriyle erişim sağlanan formatlardır. eXtensible Markup Language (XML) (Genişletilebilir İşaretleme Dili) kamu evrakı için kullanılan yaygın bir formattır.

Açık kaynak formatları, kullanıcılar veya diğer geliştiricilerin uygun gördükleri kaynak kodu kullanıma veya modifikasyona açık olan herhangi bir programı ifade eder. Açık kaynak formatları, genellikle standart bir kurum tarafından tutulan verilerin depolanması için halka açık spesifikasyonların standart bir kurumla yerine getirilmesiyle mümkün olur. Açık formatlar hem özel hem de açık kaynaklı yazılımlar tarafından kullanılabilir.

Açık standart formatları, halka açık olan spesifikasyonlar (açık kaynaklı formatlar) kullanılarak oluşturulur. Yazılım kaynak kodları özel kalsa da, standardın kullanılabilirliği, diğer geliştiricilerin başka bir yazılımla etkileşime giren veya bunun yerine ikame edilen donanım ve yazılım çözümleri oluşturmasına izin vererek uyumluluğu arttırır.

EBYS içinde yukarıdaki çeşitlere bağlı olarak, metin dosya ve formatları, grafik dosya ve formatları, veri dosyaları, elektronik tablo dosyaları, video ve ses dosyaları, işaretleme dilleri/formatları gibi birçok format çeşidi bulunabilir.[45]

Metin dosya ve formatları, metin dosyaları çoğunlukla kelime işlem yazılım programlarında üretilir. Metin dosyasının yaygın olan türleri şunlardır:

- Özel formatlar, Microsoft Word dosyaları gibi olan bu formatlar oluşturuldukları yazılımın uzantısını taşır.
- Zengin metin formatı (Rich Text Format-RTF), çeşitli uygulamalar tarafından desteklenir ve biçimlendirme talimatlarıyla (sayfa düzeni gibi) kaydedilir.

[45] **A.y.**

- Taşınabilir Doküman Formatı (Portable Document Format- PDF) dosyaları, metin ve grafikler de dâhil olmak üzere sayfanın bir görüntüsünü içeren PDF dosyaları salt okunur dosya paylaşımı için yaygın olarak kullanılır. Adobe Acrobat, bugüne kadar, diğerlerinin kullanımına rağmen, en popüler PDF dosya uygulamasıdır.
- Taşınabilir Doküman Formatı (Portable Document Format-PDF/A) dosyaları, PDF/A[46], elektronik belgelerin uzun süreli arşivlenmesi için standart dosya formatı olarak PDF'nin bir alt kümesidir. Dosyalar %100 bağımsızdır ve doküman bilgileri için dış kaynaklara ihtiyaç duymaz.

Grafik dosya formatları, bir görüntüyü saklar (örneğin fotoğraf, çizim) ve vektör tabanlı ve raster tabanlı (Bitmap) olmak üzere iki temel türe ayrılır;

- Vektör tabanlı grafik formatlarında dosyalar bir görüntüyü matematiksel formüller olarak saklar. Vektör görüntü programları, görüntüyü bozulma olmadan görüntülemek ve ölçeklendirmek için bu matematiksel formülü kullanır. Yaygın vektör tabanlı dosya formatları da türlere ayrılmaktadır. Bunlar;
  - Çizim Değişim Biçimi (Drawing Interchange Format-DXF), bilgisayar destekli tasarım yazılım programlarında yaygın olarak kullanılan dosyalardır. Mühendisler ve mimarlar tarafından sıklıkla kullanılır.
  - Kapsüllenmiş PostScript (Encapsulated PostScript-EPS) dosyaları, masaüstü yayıncılık yazılım programlarında yaygın olarak kullanılır.
  - Bilgisayar Grafikleri Meta Dosyası (Computer Graphics Metafile - CGM): Birçok görüntü odaklı yazılım programında (Photoshop gibi) yaygın olarak kullanılan ve yüksek derecede dayanıklılık sunan dosya formatlarıdır.
  - Şekil dosyaları (Shapefiles-SHP), ESRI[47] şirketinin coğrafik bilgi sistemleri uygulamaları, topolojik olmayan geometriyi saklamak için vektör koordinatlarını ve özellikler için de nitelik bilgisini kullanır.

[46] Ayrıca bkz: ISO, **19005-1:2005 Document management -- Electronic Document File Format For Long-Term Preservation -- Part 1: Use of PDF 1.4 (PDF/A-1).**

[47] İngiltere kaynaklı coğrafik bilgi sistemlerinde yazılım noktasında küresel etkiye sahip bir şirket. Ayrıntılı bkz: ESRI (Çevrimiçi) https://www.esriuk.com/en-gb/home, 11 Temmuz 2019.

- Raster tabanlı grafik formatları, görüntüyü bir piksel koleksiyonunda saklar. Raster grafikler aynı zamanda bitmaplenmiş görüntüler olarak da adlandırılır. Raster grafiklerin ölçeklendirilmeleri bozulmayı da beraberinde getirir. Raster tabanlı dosya biçimlerinin yaygın türleri şunlardır:
  - Bitmap (BMP) dosyaları, kelime işlem uygulamalarında en sık kullanılan nispeten düşük kaliteli sıkıştırılmamış dosyalardır.
  - Etiketli Görüntü Dosyası Formatı (Tagged Image File Format-TIFF) dosyaları birçok farklı yazılım programında kullanılabilir ve genellikle yüksek kaliteli bir ana görüntü için tercih edilen biçimdir. Sıkıştırılmamış veya kayıpsız sıkıştırma özelliğine sahiptir.
  - Birleşik Fotoğraf Uzmanları Grubu (Joint Photographic Experts Group - JPEG) dosyaları, dijital fotoğrafçılık için kullanılan çok yaygın bir formattır. JPEG'ler ayrıca Internet dağıtımı ve fotoğrafların dosya paylaşımı için tercih edilen formattır. Sıkıştırıldıklarında kayıplar yaşanabilir.
  - Birleşik Fotoğraf Uzmanları Grubu (Joint Photographic Experts Group-JPEG2000). Dalgacık teknolojisine dayanan çoklu sıkıştırma teknikleriyle gelişen bir formattır. Kayıpsız sıkıştırma özelliğine sahiptir.
  - Grafik Değişim Formatı (Graphics Interchange Format-GIF) dosyaları, Internet'te düz renkli alanlara sahip grafikler ve logolar için yaygın olarak kullanılır. Renk sınırlamaları nedeniyle, fotoğraflar bu formatla doğru şekilde sunulmaz. GIF, düşük çözünürlüklü animasyonlar için de kullanılabilir. (PNG, GIF'in renk sınırlamalarını iyileştirmiştir.) Kayıpsız sıkıştırma özelliğine sahiptir.
  - Taşınabilir Ağ Grafiği (Portable Network Graphic-PNG) dosyaları, GIF'in yerini almak üzere tasarlanmış patentli fakat lisanssız olan bir dosya türüdür. GIF'ten daha yüksek kaliteli dosyalar üretir. PNG formatı, özellikle Internet'te metin veya çizgi resim içeren görüntüler için tercih edilir. PNG formatı da kayıpsız sıkıştırma özelliğine sahiptir.

Veri dosya formatları, veri tabanı yazılımı programlarında oluşturulur ve bu nedenle genellikle özel (proprietary) formatlarda sunulur. Veri dosyaları, ayrı bilgi unsurları içeren alanlara ve tablolara bölünür. Yazılım bu ayrı bilgi unsurları arasındaki

ilişkiyi kurar. Veri dosyaları metin dosyalarına dönüştürüldüğünde bölünmüş olan alan ve tablo ilişkileri kaybolur. İlişki kurmak zorlaşır.

Elektronik tablo (Spreadsheet) dosyaları, hücrelerin içindeki sayıların değerini ve bu sayıların ilişkilerini depolar. Örneğin, bir hücre diğer iki hücreyi toplayan formülü içerebilir. Veri dosyaları gibi, elektronik tablo dosyaları da çoğunlukla oluşturuldukları yazılım programının özel (proprietary) formatında sunulur. Bağımsız e-tabloları Veri Değişim Biçimi'nde (Data Interchange Format-DIF) bir metin dosyası olarak kaydederek veriler farklı elektronik tablo programları arasında paylaşılabilir, ancak sayıların değeri ve ilişkisi kaybolabilir.

Video ve ses dosya formatları, bu dosyalar hareketli görüntüler (örneğin, sayısallaştırılmış video, animasyon) ve ses verileri içerir. Bunlar genellikle özel (proprietary) yazılım programlarında oluşturulur ve izlenir ve özel (proprietary) formatlarda saklanır. Yaygın kullanılan dosya formatları arasında QuickTime (.MOV), Windows Media Video (.WMV) ve Hareketli Resim Uzmanları Grubu (Motion Picture Experts Group-MPEG) formatları (.MP3); .AVI ve .WAV dosyaları bulunur.

İşaretleme dilleri/formatları (Markup languages), dosyanın içeriğini görüntülemek veya anlamak için gömülü komutlar içerir. Web üzerinden bilgi iletmek ve paylaşmak için araçlar sağlarlar. Aşağıdaki işaretleme dili dosya formatları, standart olarak World Wide Web Consortium (W3C) tarafından desteklenmektedir.

- Standart Genelleştirilmiş İşaretleme Dili (Standard Generalized Markup Language -SGML), dünyada kamu idarelerinde kullanılan ortak bir biçimlendirme dili olup uluslararası bir standarttır. Aşağıda açıklanan HTML ve XML, SGML'den türetilmiştir.
- Bağlantılı (Köprü) Metin İşaretleme Dili (Hypertext Markup Language - HTML), World Wide Web'deki bilgilerin çoğunu görüntülemek için kullanılır. Sunum, önceden tanımlanmış etiketlerin kullanımıyla içerikle birleştirildiğinden, HTML'nin kullanımı basittir, ancak kapsamı sınırlıdır. Aşağıda açıklanan XHTML ve XML gibi diğer biçimlendirme dilleri daha fazla esneklik sunar.

- Genişletilebilir İşaretleme Dili (eXtensible Markup Language - XML), bilgi yönetimi ve paylaşımı için popülerlik kazanan SGML'ye dayalı nispeten basit bir dildir. XML, SGML ile ilişkili karmaşıklıklardan kaçınırken XHTML'den daha fazla esneklik ve kontrol sağlar.
- Genişletilebilir Bağlantılı Metin İşaretleme Dili (eXtensible Hypertext Markup Language -XHTML), XML'de bulunan esnekliği HTML ile ilişkili kullanım kolaylığı ile birleştirir. Katı XHTML kuralları tutarlılığı artırır ve kendi formatlama etiketlerini oluşturma becerisi sağlar. Benzer kuralları paylaştıkları için, XHTML'yi XML'e dönüştürmek, HTML'i XML'e dönüştürmekten daha kolaydır.

Kendiliğinden değişen belgeler (Self-modifying), bazı belgeler kullanıcı müdahalesi olmadan kendi kendine değişebilmektedir. Örneğin, geçerli tarihi otomatik olarak görüntüleyen bir "alan" veya "kod" içeren kelime işlem veya elektronik tablo belgelerinde bu durum yaygındır. Belgenin yenilenmesi verildiği tarihe göre değişmektedir. Çoğu durumda, "alan" veya "kod", bir belgenin görünümünü kökten değiştirecek şekilde değişebilir. Bütün bunları tetikleyen nedenler kullanılan yazılımlardır. Buna benzer eksiklerin tamamlanması EBYS açısından belgenin güvenirliği ve gerçekliğini ortadan kaldırdığı için dikkat edilmesi gerekmektedir.[48]

EBYS içinde yukarıdaki çeşitlere bağlı olarak, metin dosya ve formatları, grafik dosya ve formatları, veri dosyaları, elektronik tablo dosyaları, video ve ses dosyaları, işaretleme dilleri/formatları gibi birçok format çeşidini barındırabilme özelliklerine sahip olması hem avantaj hem de dezavantaj sağlar. Avantaj olarak, günümüz bilgi teknolojine dayalı tüm ürünlerin EBYS içinde yer alabileceği ve yönetilebileceğinin mümkün olmasıdır. Dezavantajı ise bu kadar çeşitliliği gelecek teknolojilere taşımak için gerekli bilgi teknolojisi alt yapısı tüm kurumlarda mümkün olup olmayacağıdır. Mümkün olursa mali yükümlülüğünün tartışılması gerekir. Ayrıca bu çalışma bağlamında eski teknolojiyi yeni teknolojiye uygun hale getirirken geride kalan formatların nasıl imha edileceği de gereklidir. Bu sebeple format çeşitliliğinin bilinmesi ve imha prosedürlerine dâhil edilmesi kurumların sorumluluğundadır.

[48] European Communities, **MoReq2001**, s. 43.

3.2.5. Sürüm (Versiyon) İzleri

Versiyon, daha önceki bir formdan genellikle küçük olan farklılıklardır.[49] EBYS içinde doküman yönetim modülü içinde genellikle sürüm kontrolü de bulunmaktadır. Özellikle otomatikleştirilmiş bir ortamda, belgelere erişimi ve değiştirmeyi kontrol etme ve revize edildiğinde belgenin sürümlerini izleme teknikleri[50] olarak ifade edilen sürüm kontrolü sistemlerde zorunlu yazılım isteri olarak bulunması gereklidir. TS 13298: 2015'te bu durum;

> "*Sisteme dâhil edilmiş dokümanların farklı versiyonları korunabilmelidir. Versiyonların korunması iki farklı metot ile yapılabilir.*
>
> *• Dokümana ait tüm versiyonlar ayrı bir doküman olarak düşünülür ve sisteme dâhil edilir. Ancak bir dokümana erişim sağlandığında tüm versiyonlarının varlığından kullanıcı haberdar edilir.*
>
> *• Dokümana ait versiyonlar orijinal dokümanın altında versiyon kronolojisi ile tutulur. Böylece kullanıcı doküman üzerindeki değişiklikleri ve bu değişikliklerin kimler tarafından ne zaman yapıldığını izleyebilir."*

şeklinde net olarak ifade edilmiştir. Ancak bu isterler zorunlu değil seçmeli olarak işaretlenmiştir. Bu isterin EBYS yazılımında bulunması isteğe bağlıdır. Zorunlu bir şart olarak görülmemektedir.

Versiyon kontrolü belgenin imhası söz konusu olduğunda daha da önemli hale gelmektedir. Çünkü mevcut sürümde silinen belge, önceki versiyonlarda olduğu gibi durabilir. Bu da önceki sürümlerde bulunan tüm belgelerin asli belgenin izleri olarak karşımıza çıkmasına neden olur. Bu izlerin imha edilmeden belgenin tamamen imha edildiğini söyleyemeyiz. Tüm sürümlerin imha sürecine dâhil edilmesi, bunun için de sürüm kontrolü veya takibi gereklidir. Oluşabilecek izlerden biri de elektronik belge yönetim sistemlerindeki versiyonlardan kaynaklanan kopyalar veya bağlantılardır. Çünkü EBYS, bir belgeye ilişkin tüm dokümanları tek bir kayıt olarak tutabilir. Hatta her versiyona ait dokümanı bir belge olarak da tutabilir veya dokümanı tüm versiyonlar için ayrı ayrı bir belge olarak tutabilir.[51] Versiyon takibi için öncelikle standartlarda zorunluluk olmalıdır. Ayrıca uluslararası çalışmalar değerlendirildiğinde ABD'de sürüm kontrolü ile ilgili patentli ürünlerde durumun değerlendirildiği anlaşılmaktadır.

---

[49] Pearce-Moses, **A Glossary of Archival and Records Terminology**, s. 401.
[50] **A.y.**
[51] European Communities, **MoReq2001**, s. 41.

Örneğin Richard A. Hug ve Leon Presser'in sürüm yönetim sistemi (Version Management System)[52] adlı patentli çalışmaları EBYS içinde sürüm kontrolünün sağlanması noktasında yardımcı olabilir. Çalışmaya göre "tercihen bir dijital ortamda saklanan birden fazla dokümanın saklanması ve alınması için bir doküman işlemcisi ile birlikte çalışan bir sürüm yönetim prosedürünü içerir. Bir belgenin orijinal bir sürümü, önceki her bir sürüm belgesindeki farklılıkları temsil eden delta olarak formatlanmış veriler olarak belgenin sonraki sürümleriyle ortak bir dosyada saklanır." Buluşun imha açısından önemine baktığımızda sisteme eklenen modülle, kullanıcının bir elektronik tablo belgesinin tamamını veya bir bölümünü bir proje grubundan silmesine izin vermektedir. Sürüm açılır kutusunda listelenmek suretiyle, yetkili kullanıcı tarafından istenilen tüm belge sürümünün veya sürümlerinin tamamı imha edilebilmektedir. Sürüm yönetim sisteminde sürümlere ait tüm listelerin tutulması ve silinebilmesi imha teorisi açısından anlamlıdır. ABD Savunma Bakanlığının (United States of America Department of Defense) hazırladığı elektronik belge yönetim sistem yazılımlarına ilişkin standartta "versiyon yönetim sistemi"nde olduğu gibi sürümlerin listelenmesinin ve seçilmesinin mümkün olması teknik bir kriter olarak istenmiştir.[53]

3.2.6. Kopya ve Duplikasyon İzleri

Belge kopyaları EBYS içinde belgenin en belirgin izleri olarak karşımıza çıkar. Bu izlerin bilinmesi ve imha süreçlerine dâhil edilmesi önemlidir. Kopya, herhangi bir yöntemle, bir belgenin orijinalinin çoğaltılmasıdır.[54] Kopyalarla ilgili Avrupa Birliği EBYS modelinde açıklayıcı bilgiler mevcuttur. MoReq2010'da her varlığın bağımsız veya atomik olduğu kabul edilir. Bu özellik birlikte çalışabilirliği destekler ve varlıkların farklı belge sistemleri arasında transferine izin verir. Her belge, üstveri, etkinlik geçmişi, bileşenleri ve erişim kontrol listesinden (veya eşdeğeri) oluşur. Özellikle bir

[52] Richard A. Hug ve Leon Presser, **Version Management System**, United States of America Patent, Patent Number: 5,806,078, September 8, 1998. (Çevrimiçi) https://patentimages.storage.googleapis.com/87/f0/fa/71287d769cc9e5/US5806078.pdf, 11 Temmuz 2019.

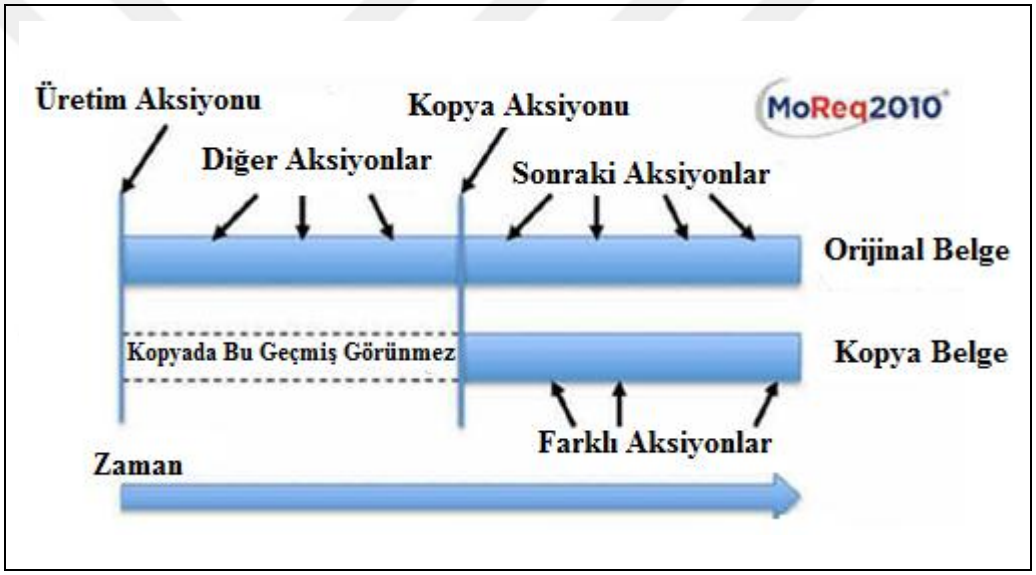
[53] United States of America Department of Defense (USA-DoD), **DoD 5015.2-STD: Electronic Records Management Software Applications Design Criteria Standard**, Department Of Defense Chief Information Officer, 2007, s. 38.

[54] California Records & Information Management (CalRIM), **Electronic Records Management Handbook**, 2002, s. 50, (Çevrimiçi) https://www.documents.dgs.ca.gov/osp/recs/ermhbkall.pdf, 11 Temmuz 2019.

kaydın etkinlik geçmişi, kaydın ilk kez MoReq2010 uyumlu belge sistemi (MoReq2010 Compliant Records System-MCRS)'nde oluşturulduğundan bu yana gerçekleşen önemli olayları gösterir.

Bu belgelerin orijinalliğini belirleyen önemli bir bileşen olan kaydın ispatını sağlar. MCRS içinde, ilk kaydın olay geçmişini çoğaltmadan bir kayıt diğerinden kopyalanırsa, ikinci kayıt tam bir kaydı temsil etmez. Birbirlerinin özdeş kopyaları olsalar bile, ikinci kaydın olay tarihinde, kopyanın oluşturulduğu noktaya kadar bir boşluk görülür. Bu durumu açıklayıcı şekil aşağıda verilmiştir.

Şekil 3.6: Orijinal Belge ve Kopya Belge Arasındaki Aksiyonlar

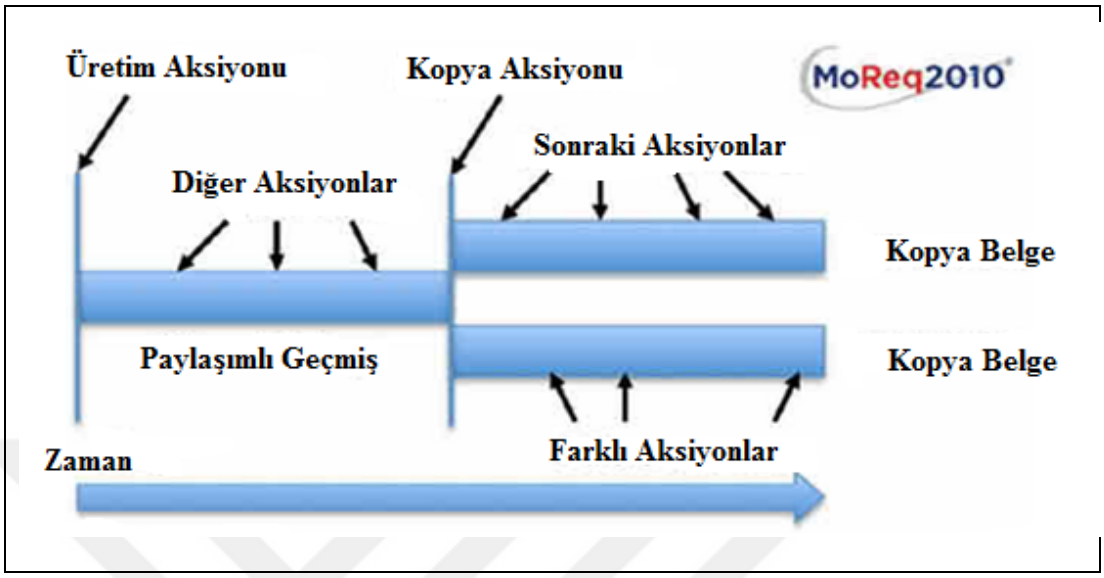


(Kaynak: DLM Forum Foundation, MoReq2010, s. 81.)

Şekil 3.6'da herhangi orijinal bir kayıttan kopya yapıldığında, kopya olan kayıt olay geçmişinin bir kısmını kaybeder ve orijinal ile aynı özelliklere sahip olmaz. Bu nedenle, MoReq2010® kayıtların kopyalanması için bir hüküm sunmaz, bunun yerine bir çoğaltma işlemi gerektirir. Çoğaltma, kaynakla aynı üstverilere sahip yeni bir kayıt oluşturmaz, aynı zamanda kaynak kaydın etkinlik geçmişinin bir kopyasını ekler. Çoğaltma işlemini takiben hiçbir kayıt orijinal, kopya olarak kabul edilemez.[55] Her iki belgenin de orijinal olduğu aşağıdaki şekilde gösterilmektedir.

[55] **A.y.**

Şekil 3.7: Kopya Belgelerin Orijinal Belgeyle İlişkili Aksiyonları



(**Kaynak:** DLM Forum Foundation, MoReq2010, s. 82)

Şekil 3.7'de bir kayıt çoğaltıldığında, çoğaltma anına kadar aynı geçmişe sahip iki orijinal kaydın bulunmasına eşdeğerdir. Bir MCRS'deki bir kaydı çoğaltmak için birincil amaç, aynı kaydın birden fazla kümede bulunmasına izin vermektir. Bunun gerçekleştiği yerde, kaydın her bir ayrı görünümü, kendi sınıflandırması, tasfiye programı, asıl ilişkili olduğu kök belgeler ve başka bir yere ait olmayan alt belgeler (parent aggregation), bileşen varlıkları, erişim kontrolleri, etkinlik geçmişi, unvanı, açıklaması ve diğer üstveriler bulunur. Bir kayıt çoğaltıldığında, MCRS kaydın içeriğini çoğaltmayı seçebilir veya her kopya için aynı içeriği kullanan bir işaret edici göstergeyi sistemda tutabilir. MCRS kaydın içeriğinin iki ayrı örneğini yaparsa, içeriğin "fiziksel olarak ayrı" olduğu söylenir. MCRS işaret edici gösterge kullanıyorsa, içeriğin "mantıksal olarak ayrı" olduğu söylenir. Her iki durumda da, içeriğin fiziksel veya mantıksal olarak ayrık olup olmadığına bakılmaksızın, bir kayıt imha edildiğinde, kalan kopyalar ve içerikleri tamamen etkilenmemelidir. MCRS, işaretçiler kullanılarak içeriği yalnızca mantıksal olarak ayırırsa, yok edilen kaydı içeriğe bağlayan işaretçiler silinmeli, ancak son yinelenen kayıt yok edilinceye kadar içeriğin kendisi silinmemelidir.[56]

[56] **A.g.e.**, s. 82.

3.3. ELEKTRONİK BELGE YÖNETİM SİSTEMLERİNE İLİŞKİN DONANIM İZLERİ

Donanım izleri, Internet/Intranet izleri (tarayıcı (arama motorları) izleri, işletim sistemlerine ilişkin izler, farklı uygulama izleri) ağ izleri, sunucu (server) izleri, depolama (storage) izleri, yedekleme (backup) izleri, erişim izleri, yazıcı/tarayıcı izleri, mobil izleri, bulut izleri, elektronik (dijital) imza izleri ve taşınma, dönüşüm, transfer (belge devri) izleri olmak üzere 11 başlık altında incelenmiştir. Internet/Intranet izleri başlığı ise kendi içinde tarayıcı (arama motorları) izleri, işletim sistemlerine ilişkin izler, farklı uygulama izleri olmak üzere 3 farklı başlığa ayrılarak değerlendirilmiştir.

3.3.1. İnternet/İntranet İzleri

İntranet, belirli bir kurum veya kuruluştaki kullanıcılarla sınırlandırılmış bir bilgisayar ağı, özellikle de web teknolojisini kullanarak kurum içindeki bilgiyi yaymaya yönelik ağ hizmetleri [57] olarak ifade edilmektedir. Diğer bir kaynağa göre intranet genellikle bir kuruluşa ait, yalnızca kuruluşun üyeleri, çalışanları veya yetkilendirilen diğer kişiler tarafından erişilebilen bir kuruluşa ait olan TCP / IP protokollerini [58] (internet) temel alan bir ağdır.[59] Bir intranet, genel olarak halka açık olmadığı için internetten ayrılır. İntranet bazen kurum dışındaki bazı kullanıcılara sınırlı erişime izin veren kapalı ağlar içerir, böyle bir sisteme genellikle extranet denir.[60] İntranet izleri, kuruma ait tüm bilgisayarlardaki depolama alanlarında bulunabilir. Yine söz konusu bilgisayarlara takılan tüm harici depolama aygıtları da kuruma ait belgeleri bulundurabilir. Bu durumu yönetmek için kurumların kendi intranet politikaları benimsemeleri gerekir. Bu politikalarda kuruma ait belgelerin periyodik olarak silinmesi için kurumsal hiyerarşi içindeki belirli kişilere yetki verilmelidir. Kurum belge yöneticisi Intranet'te bulunan belge ve izlerini belirli sürelerle imha etmelidir. İmha sürecinde kurumdaki

[57] Pearce-Moses, **A Glossary of Archival and Records Terminology**, s. 216.

[58] TCP/IP protokolleri (Transmission Control Protocol / Internet Protocol): İki ana bilgisayar arasında bir bağlantı kuran iki cihaz arasında veri iletimi için kabul edilen bir biçimdir. (American Bar Association, **Record Retention And Destruction Current Best Practices**, 2003, s. 143).

[59] American Bar Association, **Record Retention And Destruction Current Best Practices**, 2003, s. 143, (Çevrimiçi) https://apps.americanbar.org/buslaw/newsletter/0019/materials/recordretention.pdf, 28 Aralık 2017.

[60] Pearce-Moses, **A Glossary of Archival and Records Terminology**, s. 157-158.

tüm personelin kendileri için gerekli olan belgeleri ayrı ve bağımsız bir dosyaya koymaları istenmelidir. Kurumdaki tüm bilgisayarlardaki bilginin silinmesiyle süreç devam etmelidir. Bu silme işlemi kurumun intranet sayfalarındaki bilgiyi de kapsamalıdır.

İntranetteki dosya formatları, dosya sistemlerindeki okunamayan veri, silinmiş veri veya üzerine yazılmış veri gibi alanlardan da belge izleriyle karşılaşılabilir. İntranetteki izleri işletim sistemlerine bağlı olarak değişkenlik gösterir. Örneğin Microsoft Windows işletim sisteminde index.dat, Internet Explorer web tarayıcısı tarafından kullanılan bir veri tabanı dosyasıdır. Bu veri tabanında dosyalar dört farklı türde birçok kayıttan oluşur. Bunlar; HASH, URL, LEAK ve REDR'dir.[61] Bu kayıtların silinmesi için tarayıcı, Windows, Macintosh Apple ve sistemdeki uygulama izlerinin bilinmesi ve silinmesi mecburiyet olarak yansıtılmalıdır.

3.3.1.1. Tarayıcı (Arama Motorları) İzleri

Günümüzde kullanılan Internet Explorer, Firefox, Chrome, Opera, Safari, Avant, Chromium, Chrome Canary, ChromePlus, SRWare Iron and Comodo Dragon, Yandex, Microsoft Edge, Yaani, gibi birçok tarayıcı vardır. Bu tarayıcılarda birçok izler bulunabilir. Bu tarayıcılar üzerindeki muhtemel izlerin bulunabileceği yerler aşağıda listelenmiştir:[62]

- Tüm Index.dat dosyaları (Internet Explorer 8 ve 9'daki yeni index.dat dosyaları dahil: PrivacIE, TldCache ve CompatCache dosyaları) ve SuggestedSites.dat dosyası.
- Geçici İnternet dosyaları (a.k.a. Internet önbelleği)
- Çerezler (Cookies)
- UserData kayıtları, DOM depolama ve HTML5 veri tabanları
- Tüm tarayıcılarca desteklenen bütün çerezler (evercookies)
- Tarayıcı geçmiş kayıtları
- Firefox ve Chrome'daki Compact (vacuum) SQLite veri tabanları

[61] "What is in the Index.dat files?" (Çevrimiçi) https://www.milincorporated.com/a3_index.dat.html 12 Temmuz 2019.

[62] Mil Incorporated, "Mil Shield," (Çevrimiçi) https://www.milincorporated.com/milshield2.html, 12 Temmuz 2019.

- IE görüntü boyutları önbellek (MSIMGSIZ.dat dosyaları)
- IE kimlik avı filtresi önbelleği
- IE arama kayıtlarının varsayılanlara geri yükleme
- AutoComplete formları ve şifreleri
- Geçmiş veri formları,
- İndirme geçmişi
- En son kullanılan indirme klasörü
- Ana sayfayı (IE, Firefox, Opera, Safari, Chrome'da) ve arama sayfanızı (IE ve Firefox'ta) geri yükleme
- Arama geçmişi
- Kayıtlı şifreler
- Crash oturumu kurtarma bilgisi
- Flash çerezleri (yerel paylaşılan nesneler).
- Firefox, Opera, Chrome ve Avant için birden fazla tarayıcı profilini destekleme
- Internet Explorer için aşağıdaki araç çubukları: Google Araç Çubuğu, Yahoo Araç Çubuğu, ICQ Araç Çubuğu, Bing Araç Çubuğu, Windows Live Araç Çubuğu (ve daha eski MSN araç çubuğu), AOL Araç Çubuğu, IE7Pro eklentisi (çökme oturumu kurtarma bilgisi) ve MyWaySearch PopSwatter Araç Çubuğu.
- Firefox için aşağıdaki araç çubukları: Google Araç Çubuğu, Yahoo Araç Çubuğu, AOL Araç Çubuğu.

Tarayıcılardaki izler silinmeden belgenin silindiğini söylemek mümkün olmaz. Riskleri tamamen olmasa da en aza indirgemek için bu izlerdeki verinin de silinmesi veya imha edilmesi önemlidir.

3.3.1.2. İşletim Sistemlerine İlişkin İzler

İşletim sistemleri belge imha sürecinde önemli bir iz depolama alanıdır. Dünyada yaygın olarak kullanılan üç işletim sistemi vardır. Bunlar; Microsoft Windows, macOS ve Linux'tur. Türkiye'de kamu kurumlarında çoğunlukla Microsoft Windows

işletim sistemi kullanılmaktadır. Windows işletim sistemleri[63] kullanan kurumlar için aşağıda sıralanan izlerin silinmesi belge imhasının tam olarak yapılması açısından önemlidir. Windows 7, Windows 8, Windows 8.1 için geçerli olan izler, Windows 10 için de geçerlidir. Ancak Windows 10'un farklı bir iz yeri olarak Windows 10'la çalışan Microsoft Edge tarayıcı izlerinin göz ardı edilmemesi önemlidir. İzlerin silinmesine yönelik kullanılan yazılımlar da Windows gibi farklı sürümleri günceli yakalamak adına geliştirmektedirler. Örneğin Mil Shield 7.2 isimli yazılım 2009 yılında piyasaya sürülürken, daha sonraları Mil Shield 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1 sürümleri vardır. 29 Temmuz 2015 tarihinde piyasaya sürülen Windows 10 ile beraber, Mil Shield 9.0 da 31 Aralık 2015 tarihinde piyasaya sürülmüştür.

- Son belgeler geçmişi
- Windows shell en son kullanılan (MRU) klasör kayıtları.
- Genel dosya iletişim kutularının en son açılan dosya listesi
- Windows 7 Explorer yazılan yol (typed paths) geçmişi.
- Windows shell dosya ve bilgisayar arama geçmişi
- Başlat menüsü Çalıştırma geçmişi.
- En sık kullanılan Başlat menüsü (MFU) programları listesi (Windows Başlat menüsünün sol tarafındaki liste).
- Tüm UserAssist kullanım bilgileri.
- Düşük düzeyde Geri Dönüşüm Kutusu (yalnızca Windows Shell aracılığıyla değil)
- Windows geçici dosyaları
- Windows panosu
- Başlat menüsünde yeni programların vurgulanmasını devre dışı bırakma
- Windows Vista küçük resim (thumbnails) önbelleği
- İnternet şifreleri (WinInet önbellek bilgileri)
- Windows DNS önbelleği

[63] Windows 7, 14 Ocak 2020 tarihinde 10 yıllık kullanımdan sonra Microsoft tarafından güncellenmeyeceği açıklanmıştır. Söz konusu tarihten sonra Windows 7 kullanan bilgisayarların, teknik destek, yazılım güncelleştirmeleri ve güvenlik güncelleştirmeleri desteğini alamayacakları ifade edilmektedir. (Microsoft, "Windows Support," (Çevrimiçi), https://support.microsoft.com/en-ph/help/4057281/windows-7-support-will-end-on-january-14-2020, 31 Ekim 2020).

- Aktif Kurulum geçici klasörleri
- İçerik Dizini oluşturucu kataloğu
- Hazırda bekleme dosyası.
- Hafıza dökümü dosyaları
- Orphan ChkDsk dosya parçaları
- Günlük kurulum dosyaları
- Sistem hatası mini döküm dosyaları
- Windows Hata Bildirimi arşiv dosyaları
- Windows Hata Bildirimi sıra dosyaları
- Regedit geçmişi
- Windows kaydedilen aramalar (.search-ms dosyaları)
- Windows sayfa dosya kapanması

3.3.1.3. Destek Uygulamalara Ait İzler

Destek uygulama izleri 6 kısımda incelenebilir. Bunlar; medya oynatıcıları, fotoğraf araçları, indirme araçları, arşivleyiciler, Office programları ve diğer programlardır. Aşağıda bunların başlıklar altında ayrıntılı listeleri verilmiştir. Tüm uygulamalar bir iz olarak düşünülebilir. Dolayısıyla tüm bu izlerin silinmesiyle tam bir imhadan söz edilebilir.

Medya Oynatıcılar: Adobe Flash Professional, Anole Media Player, Any Video Converter, Applian Flv Player, Avant DVDDivX Player, Avi Previewer, ATP Player, BSplayer, Core Player, Corel Video Studio Pro, Cyberlink Power Director, Debug Mode Wax, DivX Player, Easy Video Converter, Elecard MPEG Player, Flash Player Pro, Flv Player, Free iPod Video Converter, Free YouTube to MP3 Converter, Free Flv Converter, GOM Player, Haihaisoft Universal Player, KMPlayer, MPlayer, Media Player Classic, Movie Magician, Need4 Video Converter, Pazera Free Flv to Avi Converter,	**Fotoğraf Araçları:** 3D Photo Browser, Able Image Browser, ACDSee, AD Picture Viewer, Adobe ImageReady, Axialis IconWorkshop, Concept Draw, Corel Paint Shop Pro, FastStone Image-Viewer, First Impression, Irfan View, Markosoft Image Viewer, Memories On Tv, Nikon View, MS Paint, MS Photo Editor, Paint.NET, Panorama Composer, Photo Manager, Photo Scape, Photo Watermark Professional, Photolightning, PhotoPhilia, Photoshop Album, Photoshop Elements, Picasa, Polyview, Retouch Pilot, Sib Image Viewer, Slide

PowerDVD, Power2Show Media Player, QuickTime, RealPlayer, Riva Flv Player, TubePlay, VLC Player, WinDVD, Winamp, Windows Media Player, Windows Movie Maker, Xilisoft video Converter, Zoom Player, Kodekler[64] (Codec) MP3, WMA, RealVideo, RealAudio, DivX, XviD gibi. Ve diğerleri (bazıları güncelliklerini ve popülerliklerini yitirmişlerdir)	Show Pilot, Snagit, SnapTouch, SWiSH, Widdbit Viewer.
İndirme Araçları: BitComet, CuteFTP, Download Accelerator (DAP), eMule, FlashGet, Free Download Manager, Fresh Download, GetRight, LeechGet, Net Vampire, Orbit Downloader, UltraGet Video Downloader, VDownloader, Vuze, YouTube Downloader.	**Arşivleyiciler:** 7-Zip, IsoBuster, IZArc, PicoZip, Power Archiver, TUGZip, WinAce, WinRAR, WinZip.
Ofis Programları: Access Snapshot Viewer, Adobe Acrobat, Adobe Reader, Cute PDF, Foxit Reader, Macromedia Homesite, Microsoft Office, Microsoft Visio, Microsoft OneNote, MS Works, OpenOffice, Outlook Express, PDF Creator, TextPad, Windows Mail, Windows Live Mail, WordPad.	**Diğer Programlar:** AceHTML, Alcohol 120, Google Deskbar, Google Desktop, Google Earth, ImgBurn, Microsoft Management Console, Nero Burning ROM, Offline Explorer Pro, PowerISO, Remote Desktop, Skype, SpyBot Search & Destroy, Tivo Desktop, Virtual Dub, WebZip, WebSite eXtractor, WinIso, WinWSD WebSite Downloader, XMLSpy.

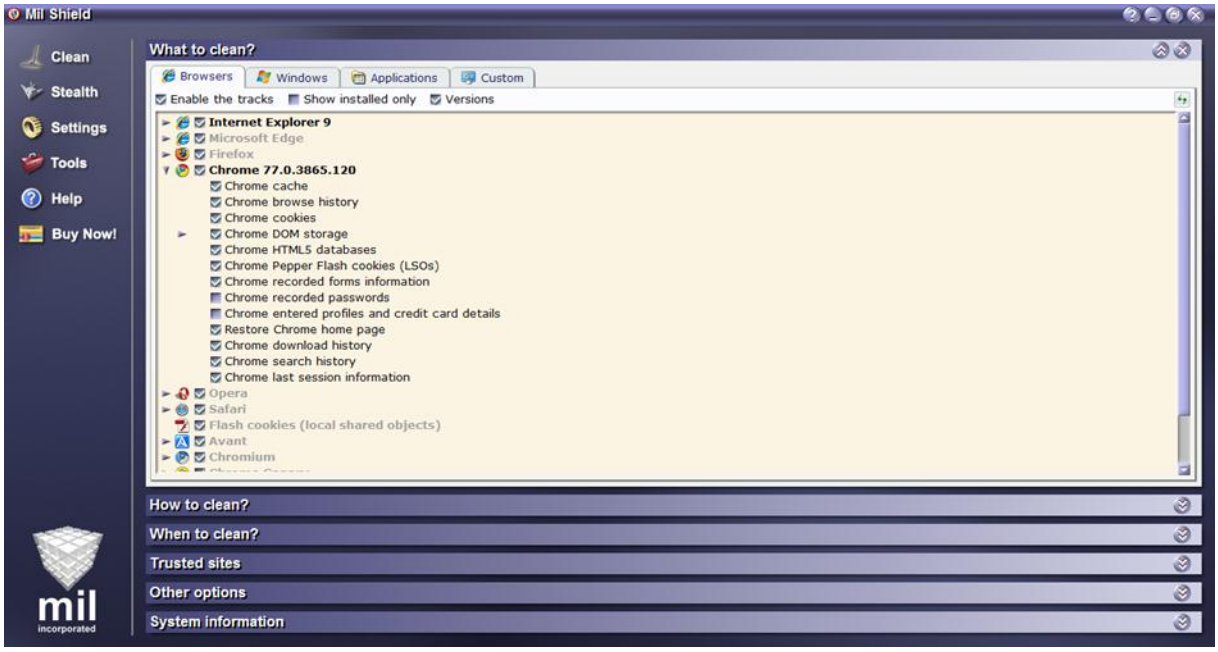
Her ne kadar karışık gibi görünse de tüm bu izlerin imha programları kullanılarak silinmesi mümkündür. En popüler olanları MilShield, BitRaser, Blancco File Eraser, WipeDrive Home, Eraser olarak sıralanabilir. Bunların en büyük özelliği ise işlem sonunda silme raporu vermeleri ve bir şeylerin değiştirilmesine, açılmasına, çıkarılmasına veya hasar görmesine izin vermemesidir.[65] Detaylı yazılımlar listesi araştırmanın dördüncü bölümü olan *Dünyada ve Türkiye'de Elektronik Belge İmha Politikaları,*

[64] Lifewire, "What Is a Codec and Why Do I Need It?" (Çevrimiçi) https://www.lifewire.com/what-exactly-is-odec-2483426, 1 Kasım 2019.

[65] Aruna Attri, "10 Best File Eraser Software 2019," (Çevrimiçi) https://www.stellarinfo.com/blog/best-file-eraser-software/ 1 Kasım 2019.

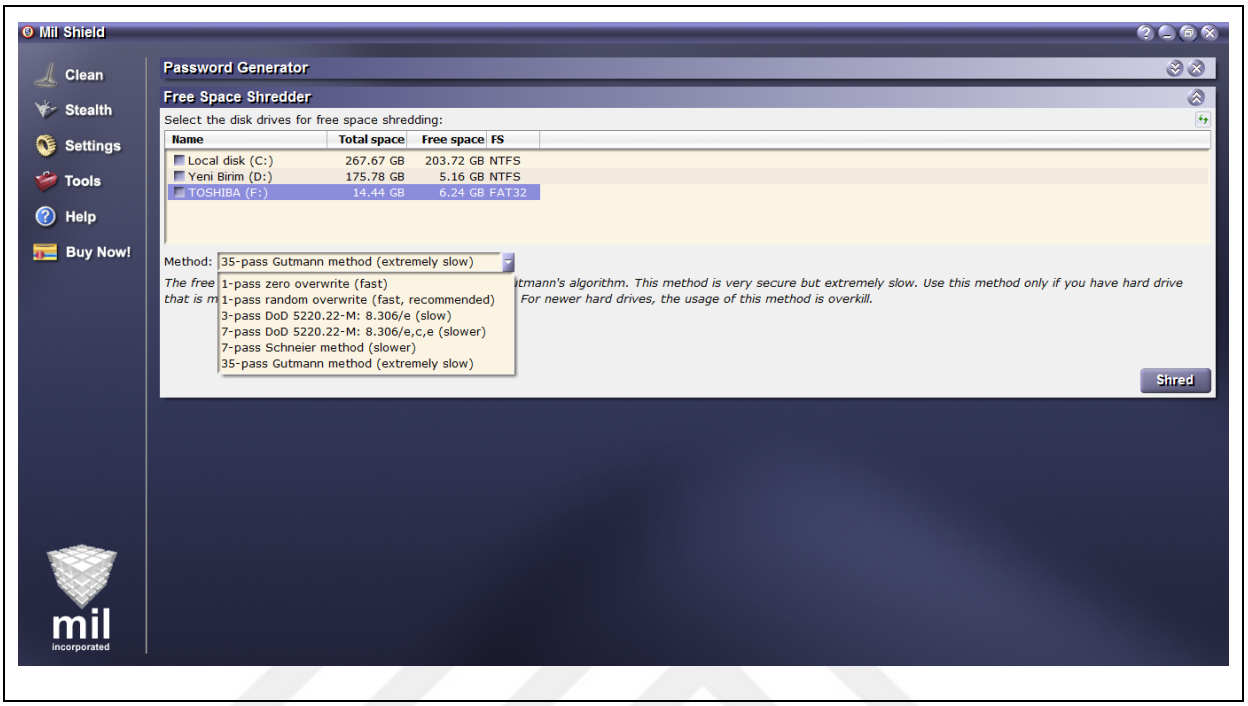
Teorileri ve Uygulamaları'nda belirtilmiştir. Burada sadece birine ait ara yüz görüntüsü verilmiştir.

Şekil 3.8: İntranet/İnternet İzlerinin Silinebileceği Yazılım Görüntüsü



(**Kaynak:** Mil Incorporated, "Mil Shield," (Çevrimiçi) https://www.milincorporated.com/milshield2.html, 12 Temmuz 2019.)

Şekil 3.9: İntranet/İnternet İzlerinin Çeşitli Yöntemlerle Silinme İşlemi



(**Kaynak:** Mil Incorporated, "Mil Shield," (Çevrimiçi) https://www.milincorporated.com/milshield2.html, 12 Temmuz 2019.)

Ekran görüntüsünde silmeye ilişkin yöntemler kısmında belirtilen üzerine yazma teknikleri ve bu tekniklere ilişkin standartlar çalışmanın dördüncü bölümünde detaylı olarak açıklanmıştır.

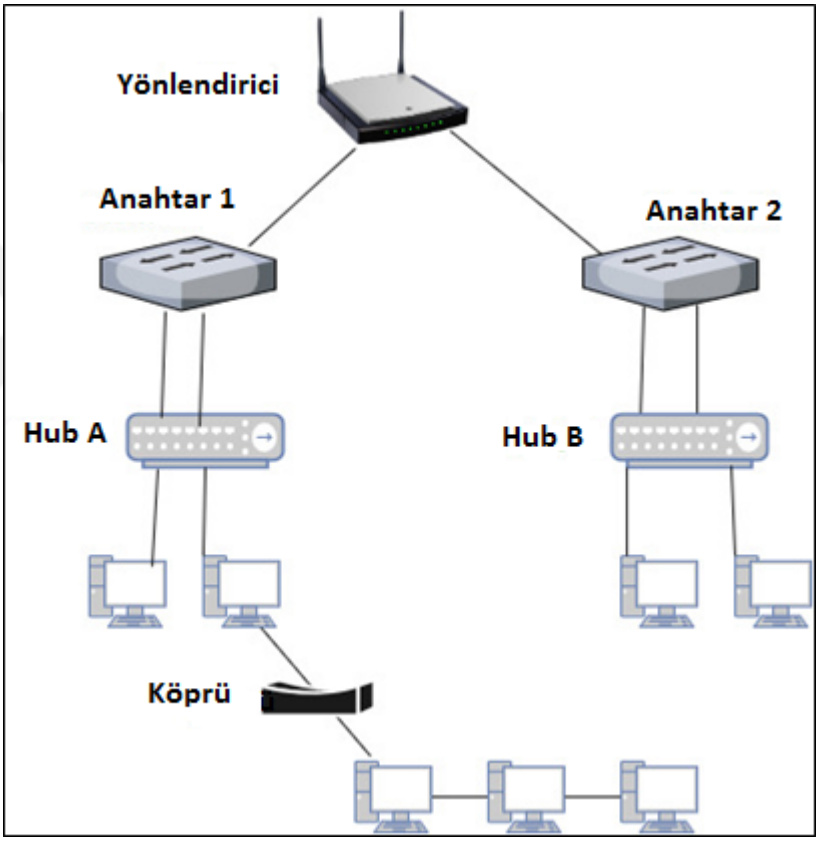
3.3.2. Ağ İzleri

Ağ, "*birbirine bağlı dalların ve düğümlerin düzenlenmesi*"[66] olarak tanımlanmaktadır. Bilgisayar ağında, bilgisayarlar ve iletişim cihazları ağdaki varlıklar olarak düşünülmektedir.[67] EBYS yazılımları, Yerel Alan Ağı (Local Area Network -LAN), Geniş Alan Ağı (Wide Area Network-WAN), diğer ağ topolojisi ve Ağ İşletim Sistemini (Network Operating System-NOS) çalıştırması beklenmektedir.[68] Ağların anlaşılması ağ çeşitlerin ve ağ araçlarının anlaşılmasını gerektirmektedir. Ağlar LAN, WAN, MAN, Sanal Özel Ağ (Virtual Private Network-VPN), SAN gibi çeşitlere ayrılmaktadır.

[66] TSE, **Bilişim Terimleri Sözlüğü**, s. 143.
[67] **A.y.**
[68] USA-DoD, **DoD 5015.2-STD**, s. 47.

Ağ araçlarına baktığımızda, hub (hub), tekrarlayıcı (repeater), köprü (bridge), anahtar (switch), yönlendirici (router), ağ geçitleri (gateways) ve brouter[69] (köprü-yönlendirici) gibi birçok araca sahiptir.[70] Bunlar haricinde, Kanal Servis Ünitesi / Veri Servis Ünitesi (Channel Service Unit/Data Service Unit -CSU/DSU), Network interface cards (NICs), ISDN adapters Wireless access points (WAPs), Modems, Transceivers (media converters) ve Firewalls gibi bileşenleri de vardır.[71]

Şekil 3.10: Yerleşik Ağ Sistemleri



(**Kaynak:** GeeksforGeeks, "Network Devices," (Çevrimiçi) https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/, 15 Temmuz 2019.)

[69] Brouter, bir ağ köprüsü ve bir yönlendiricinin tek bir üründe birleştirilmesidir (TechTarget, "Brouter," Çevrimiçi) https://searchnetworking.techtarget.com/definition/brouter, 1 Kasım 2019).

[70] GeeksforGeeks, "Network Devices," (Çevrimiçi) https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/, 15 Temmuz 2019.

[71] **Networking Components and Devices**, (Çevrimiçi) https://sureshvcetit.files.wordpress.com/2019/03/network-components.pdf, 15 Temmuz 2019.

Yönlendiriciler, anahtarlar, güvenlik duvarları ve kablosuz erişim noktaları gibi yerleşik ağ sistemlerinde, içinde depolanan yapılandırma verileri ve yazılımlar bulunur. Bu bilgiyi saklamak için kullanılan hafıza tipi, bir devre kartına lehimlenmiş flash bellek çiplerini, çıkarılabilir flaş kartlarını ve sabit disk sürücülerini içerir. Sistemler, genellikle bir Komut Satırı Arabirimi (CLI) aracılığıyla kontrol edilir (asenkron bir RS-232[72] bağlantısı veya bir ağ arayüzü üzerinden bir ssh / telnet sanal terminal bağlantısı kullanılarak erişilebilir). Bazı durumlarda, cihaz yerleşik bir web sunucusu tarafından sağlanan bir web arayüzü vasıtasıyla da yapılandırılabilir ve kontrol edilebilir. Ne yazık ki, konfigürasyon verileri için kullanılan depolamaya genellikle üreticinin sağladığı metotlar dışında erişilemez, bu nedenle cihazın konfigürasyonunu silmeye çalışırken satıcının sağladığı metotların konfigürasyon verilerini gerçekten silip silmemesi gerektiğini bilmek önemlidir.[73]

Asıl problem ise yeni ürünlerin piyasaya sürülmesiyle kullanımda olan ürünlerin devre dışı bırakılmasıdır. Eski ürünlerde kurumlar için önemli bilgiler yer alıyorsa, haliyle bunların imhası da önemlidir. Hiçbir kurumun kendine özgü bilgilerin başkalarının eline geçmesini istemesi düşünülemez.[74]

Tablo 3.1: Ağ Araçlarının Temizlenmesi

Ağ Araçlarının (Yönlendiriciler ve Anahtarlar) İmha Süreçleri	
Birinci Kademe (Clear):	Yönlendiriciyi veya anahtarı üreticisinin varsayılan fabrika ayarlarına getirmek.
İkinci Kademe (Purge):	Çoğu yönlendirici ve anahtar, yalnızca birinci kademe silme özelliklerini taşır. Bazı yönlendiriciler ikinci kademe silmeyi destekleyecek yetenekleri de sunabilir, ancak bu yetenekler cihazın donanım ve ürün bilgisine özgüdür ve dikkatli uygulanmalıdır. Veri kurtarma işleminin olanaksız olmasından ve cihazın dosya işaretleyicilerini normal bir silme işlemiyle gerçekleştirmediğinden emin olmak için cihaz üreticisine başvurmak gerekir. Bu kademede cihaz üzerine yazma veya blok silme işlemi gerçekleştirilir. Eğer uygun değilse üçüncü kademeye geçilmelidir.

[72] RS232, günümüzde maliyetinin az olmasından dolayı kullanımı devam etmekle beraber, USB, Ethernet gibi yeni araçlar RS232'nin yerini almış durumdadır (Realpars, "What Is RS232 and What Is It Used for?" (Çevrimiçi) https://realpars.com/rs232/, 1 Kasım 2019).

[73] Magnus Larsson, "Sanitization of Embedded Network Devices Investigation of Vendor's Factory Reset Procedures," **Unpublished Master Thesis**, KTH Royal Institute of Technology School of Information and Communication Technology (ICT) Department of Communication Systems, Stockholm, Sweden, 2015, s. 1.

[74] OceanTech, "Network Equipment Recycling and Data Destruction," (Çevrimiçi) https://www.oceantech.com/2015/01/09/network-equipment-data-destruction/, 15 Temmuz 2019.

Üçüncü Kademe-İmha (Destroy):	Kıyma (shredding), parçalama (disintegrate), toz haline getirme (pulverize), veya cihazı lisanslı bir yakma şirketi veya kuruluşunda yakmak (incinerate).
Notlar:	Ağ araçları çıkarılabilir depolama alanı içerebilir. Depolama alanı, alana özgü teknikler kullanılarak çıkarılmalı ve imha edilmelidir.

(Kaynak: NIST SP 800-88, Guidelines for Media Sanitization, s. 27-28)

3.3.3. Sunucu (Server) İzleri

Sunucu, "*bir bilgisayar ağında, iş istasyonlarına, kişisel bilgisayarlara veya diğer fonksiyonel birimlere paylaşımlı hizmetler sağlayan fonksiyonel birim*"[75] olarak tanımlanmaktadır. Tanımda geçen paylaşımlı hizmetlere örnek olarak dosya sunucuları, yazıcı sunucuları, e-posta sunucuları verilebilir. Sunucular kişisel bilgisayarlardan farklı olsa da, birçok yönden sunucu donanımı masaüstü donanımından çok farklı değildir. Her ikisi de güç kaynakları, bellek ve CPU'lar gibi aynı temel bileşenlerden yapılmıştır. Sunucu donanımındaki her bir bileşen, kişisel bilgisayarlarda bulunanlardan daha gelişmiş olma eğilimindedir. Sunucular bazen ayrıca yedekli ve / veya çalışırken değiştirilebilir bileşenleri de kullanırlar.[76] Sunucular fiziksel olarak tower, rack ve blade olmak üzere üç farklı türe ayrılmaktadır.[77]

Tower (standart) sunucuların görünümü bilgisayar kasasına benzer. Standart bir sunucusu, tek bir sunucu olarak kullanılmak üzere tasarlanmıştır ve dik, bağımsız bir kabine yerleştirilir. Tower adı verilen dolap, kule stili bir masaüstü bilgisayarın kabine benzer boyutlardadır. Standart sunucular, genellikle rafa monte edilen raf (rack) sunucularından veya blade sunuculardan farklıdır.

Rack (raf) sunucular, birden fazla sunucuyu barındıracak şekilde tasarlanmıştır ve küçük alanlara sığacak şekilde özel olarak yapılmıştır. Genellikle üst üste istiflenirler, bu da cihazların soğutulmasını zorlaştırır, ancak ölçeklenebilirlik söz konusu olduğunda büyük bir avantaj sağlar. Ayrıca yığılmış model, ağ kaynaklarını birleştirmeye ve alan gereksinimlerini en aza indirmeye yardımcı olur. Raf tipi bir sunucu, esas olarak sunucu olarak kullanılan bir bilgisayardır ve raf adı verilen bir çerçeveye

[75] TSE, **Bilişim Terimleri Sözlüğü**, s. 197.
[76] Dealna, "Three Types of Server Hardware," (Çevrimiçi) https://dealna.com/en/Article/Post/1391/Three-Types-of-Server-Hardware, 17 Temmuz 2019.
[77] **A.y.**

kurulmak üzere tasarlanmıştır. Raf, vidalarla yerinde tutulan bir donanım birimini sabitlemek için tasarlanmış bölmeler olarak bilinen çoklu montaj deliklerinden oluşur.

Blade sunucular, her ne kadar tasarım olarak raf sunucularına benzese de, daha incedirler ve aynı zamanda daha pahalıdırlar. Bir blade sunucu, sunucu blade'leri olarak bilinen çoklu ince, modüler EC kartlarını barındıran bir sunucu kasasıdır. Her blade, genellikle tek bir uygulamaya tahsis edilmiş bir sunucudur. Sunucu bıçakları tam anlamıyla işlemciler, bellek, tümleşik ağ denetleyicileri ve diğer giriş / çıkış (IO) bağlantı noktaları içeren bir karttaki sunuculardır.

Kurumların fiziksel olarak hangi sunucu türünü seçecekleri kurumsal ihtiyaçlara bağlıdır. Yer, para, cihaz ısınması gibi problemler hangisinin seçileceği konusunda belirleyici rol oynar. Fiziksel olarak üçe ayrılan sunucular, türleri bakımından da farklılık arz eder. Genel olarak dosya, yazıcı ve veri tabanı sunucuları olarak ayrılabilirler. Özel olarak da web sunucu, proxy sunucu, özelleştirilmiş (dedicated) sunucu, uygulama sunucusu, bulut sunucu gibi türlere ayrılırlar.[78] Her bir sunucu türünün farklı görevi vardır. Dosya sunucusu, dosyaları depolamaya ayrılmış bir bilgisayar ve depolama aygıtı olarak çalışır. Ağdaki herhangi bir kullanıcı dosyalarını sunucuda depolayabilir. Yazdırma sunucusu, bir veya daha fazla yazıcıyı yöneten bir bilgisayar ve bir ağ sunucusu ile çalışır ve ağ trafiğini yönetir. Veri tabanı sunucusu, veri tabanı sorgularını işleyen bir bilgisayar sistemiyle çalışır. Genel anlamdaki türleri bu şekilde çalışırken özel anlamda da farklı çalışmaktadır. Bu farklılıklar aşağıda açıklanmıştır.[79]

Web sunucuları, web sayfalarını sunan (veya hizmet veren) bilgisayarlardır. Her web sunucusunun bir IP adresi ve muhtemelen bir etki alanı adı vardır. Kamu ürünü yazılım ve ticari paketler dâhil olmak üzere pek çok web sunucusu yazılım uygulaması vardır

Proxy sunucusu, Web tarayıcısı gibi bir istemci uygulaması ile gerçek bir sunucu arasında çalışan bir sunucudur. Proxy sunucularının iki ana amacı vardır: performansı iyileştirmek ve istekleri filtrelemek.

[78] Webopedia, "Server," (Çevrimiçi) https://www.webopedia.com/TERM/S/server.html, 17 Temmuz 2019.

[79] **A.y.**

Özelleştirilmiş (dedicated) sunucular, ağın gereksinimlerini karşılamak için ayrılmış tek bir bilgisayardır. Örneğin, bazı ağlar, diğer tüm bilgisayarlar arasındaki iletişimi yönetmek için bir bilgisayarın bu işe tahsis ayrılmasıdır.

Bir uygulama sunucusu, kullanıcılar ve bir kuruluşun arka uç iş uygulamaları veya veri tabanları arasındaki tüm uygulama işlemlerini yapan bir programdır. Bu tür bir sunucu genellikle karmaşık işlem tabanlı uygulamalar için kullanılır.

Bulut sunucuları, müşterilerin İnternet üzerinden gelen taleplerin karşılanması için kullanılır. Tek bir sunucu veya sanal sunucu tarafından sağlanmak yerine, bir bulut içeren birden çok bağlı sunucu tarafından sağlanır.

Sunucular verinin yönetilip işlenmesine ve saklanmasına yardımcı araçlardır. Bu araçların masaüstü bilgisayarlar gibi özellikler taşıması, bir tür masaüstü bilgisayar gibi görünmesini sağlamaktadır. EBYS içindeki imha teorisi açısından değerlendirildiğinde hem donanımsal hem de yazılımsal varlık ve izlerinin güvenli bir şekilde silinmesini zorunlu kılmaktadır. Açıklanan her bir izin sunucular için düşünülmesi önemlidir. Kullanımı devam eden sunucularda imha edilmek istenen bilgi ve belgeler için imha yazılımları kullanılması gerekirken, kullanım dışı olan sunucuların öncelikle yazılımsal olarak içeriğinin temizlenmesi daha sonra da fiziksel imhası güvenli imhanın gereği olarak görülmektedir. Sunuculardaki izler, sunucunun sahip olduğu her bir bileşendeki verilerdir. Her bir bileşen imha amaçlı temizlenmedikçe veya fiziksel olarak yok edilmedikçe bilginin varlığına erişim sağlanabilir.

3.3.4. Depolama (Storage)

Depolama bu çalışma kapsamında bilgi ve belgelerin aktif ve yarı aktif oldukları zamanları boyunca bulundukları ortamı ifade etmek için kullanılmaktadır. Belgeler aktif ve yarı aktif oldukları süre zarfında çeşitli ortam ve araçlarda bulunabilir. Bu araçların bir kısmı geçici faaliyet gösterirken diğer kısım daha uzun süreli saklanılması gereken belgelerin muhafazası için kullanılır. Bu saklama alanlarındaki belgelerin saklama planlarına göre yaşam süreleri belirlenir. Saklama süreleri tamamlandıktan sonra imha edilmesi gereken belgelerin hiçbir şekilde iz bırakılmadan ortamlardan silinmesi

gerekir. İmha edilen ortamlardaki belgelerin yerine yeni belgeler tutulacaksa imha süreci ona göre şekillenir. Eğer ortam veya araçlar çeşitli sebeplerle kullanılmayacaksa bu ortam ve araçların fiziksel imhası da gereklidir.

Bilgi ve belgelerin saklandıkları ortam ve araçlar özelliklerine göre çeşitlere ayrılmaktadır. Bu çeşitlilik uygulanacak imha yöntem ve tekniğini de belirlemektedir. Saklama ortam ve araçları aşağıdaki tabloda belirtilmiştir.

Tablo 3.2: Ortam Saklama Araçları

Manyetik medya	**Optik medya/WORM (write once read many)**	**Depolama araçları (Solid state device-SSD)**
Manyetik bant (Magnetic tape) Sabit sürücüler (Hard Disk Drive-HDD) Sabit sürücüler (Solid State Drive-SSD) Disketler (Floppy disks)	CD-R'ler (Compact disk-recordable) DVD-R'ler (Digital versatile disc-recordable)	Rastsal erişim belleği (Random-access memory- RAM) Salt okunur hafıza (Read-only memory -ROM) Akıllı kartlar Flash bellek

(**Kaynak:** Yazar tarafından derlenmiştir.)

Saklama ortam ve araçlarından kendi içinde ana bellek (main memory) ve yedek bellek (backing storage) şeklinde ikiye ayrılır:[80]

Ana bellek, RAM ve ROM'un diğer bir ismidir. Genellikle verileri geçici olarak saklamak için kullanılır. Ana bellek, CPU tarafından işlenirken verileri depolamak için kullanılır. Veri hafızaya alınabilir ve çok hızlı bir şekilde tekrar okunabilir.[81]

Yedek bellek, kullanılmadıklarında veya bir bilgisayar değiştirildiğinde, programları ve verileri depolamak için kullanılır. Programlar ve veriler gerektiğinde, ana

[80] Revision World, "Storing Data, Devices and Media," (Çevrimiçi) https://revisionworld.com/gcse-revision/ict/hardware/storing-data-devices-and-media, 17 Temmuz 2019.

[81] Quizlet, "ICT-3.Storage Devices and Media," (Çevrimiçi) https://quizlet.com/138092983/ict-3storage-devices-and-media-flash-cards/, 18 Temmuz 2019.

belleğe kopyalanır, ancak yine de yedek depolamada kalırlar. Manyetik teyp sürücüleri, disket sürücüleri ve sabit disk sürücüleri, tüm yedekleme depolama cihazlarına örnektir.[82]

Manyetik depolama ortamı ve araçlar, verileri küçük mıknatıslanmış noktalar şeklinde depolar. Bu noktalar, çok küçük elektromıknatısların yarattığı manyetik alanlar kullanılarak oluşturulur, okunur ve silinir. Manyetik depolama araçları aşağıda ayrıntılı olarak açıklanmıştır.[83]

- Hard Diskler: Hard diskler, çok büyük bir depolama kapasitesine sahiptir. Çok miktarda veri depolamak için kullanılabilirler. Hard diskler rastsal erişim aygıtlarıdır ve veri erişim hızları çok yüksektir.
- Sabit Hard Diskler: Bir bilgisayar kasasına yerleştirilmiş bir sabit disk, 'sabit' olarak bilinir. Hemen hemen her bilgisayarda sabit bir disk bulunur. Sabit olan diskler, neredeyse tüm bilgisayarlar için ana yedekleme depolama aygıtı olarak işlev görür, çünkü dosyalara neredeyse anında (rastsal erişim ve yüksek erişim hızlarından dolayı) erişim sağlarlar.
- Taşınabilir Hard Diskler: Taşınabilir bir hard disk, sabit sürücüye USB veya benzeri bir bağlantı kullanılarak erişilmesine izin veren bazı elektronik parçaların yanı sıra küçük bir kasaya yerleştirilen bir sürücüdür. Taşınabilir hard diskler, bilgisayardan bilgisayara çok büyük miktarlarda veri taşınmasına izin verir.
- Manyetik Bant: Manyetik bant, yüksek kapasiteli, seri erişim ortamıdır. Seri erişim ortamı olduğundan, kasetteki tek tek dosyalara erişmek yavaştır. Bantlar, büyük miktarda verinin depolanması gereken yerlerde, ancak tek tek dosyalara hızlı erişimin gerekli olmadığı yerlerde kullanılır. Veri yedeklemek için kullanılır.

[82] Revision World, "Storing Data, Devices and Media," **a.y.**
[83] Quizlet, "ICT-3.Storage Devices and Media," **a.y.**

- Disket: Çıkarılabilir, taşınabilir, ucuz, düşük kapasiteli (MFD-2HD 3.5 gibi) depolama ortamıdır. Disketler, bilgisayarlar arasında az miktarda veri aktarmak veya küçük dosyaları yedeklemek için kullanılan rastsal erişim aygıtlarıdır. Erişim süreleri yavaştır.
- Zip Diski: Diskete benzeyen, ancak daha yüksek kapasiteli (zip 100, zip 250, veya zip 750 gibi), çıkarılabilir ve taşınabilir bir depolama ortamıdır. Zip diskleri, verileri yedeklemek veya büyük dosyaları bilgisayarlar arasında taşımak için kullanılan rastsal erişim cihazlarıdır.
- Jaz Diski: Yüksek kapasiteli (Iomega jaz diskleri gibi), sabit sürücü teknolojisine dayalı çıkarılabilir ve taşınabilir bir depolama ortamıdır. Jaz diskleri, verileri yedeklemek veya büyük dosyaları bilgisayarlar arasında taşımak için kullanılan rastsal erişim cihazlarıdır.

Optik Depolama Araçları/Ortamları: Optik depolama aygıtları, verileri ışık kullanarak okur ve nokta desenleri olarak kaydeder. Bir lazer ışını normal ışık kaynağıdır. Depolama ortamı üzerindeki veriler, lazer ışını ortam yüzeyinden sıçrayarak okunur. Eğer ışın bir noktaya çarparsa -nokta olmasaydı- olacağından farklı şekilde geri yansıtılır. Bu fark tespit edilebilir, böylece veriler okunabilir. Optik depolama araçları aşağıda ayrıntılı olarak açıklanmıştır.[84]

- CD-ROM: Kompakt Disk - Salt Okunur Bellek (CD-ROM) diskleri yaklaşık 800 MB veri tutabilir. Veriler değiştirilemez (geçici değildir), bu nedenle yanlışlıkla silinemez. CD-ROM'lar rastsal erişimli cihazlardır.
- DVD-ROM: Çok Yönlü Dijital Disk - Salt Okunur Bellek (DVD-ROM) diskleri yaklaşık 4,7 GB veri tutabilir (çift katmanlı bir DVD'nin iki katı veri tutabilir). DVD-ROM'lar rastsal erişimli cihazlardır.
- Blu-Ray: Blu-Ray diskleri DVD'lerin yerine geçen son dönemlerde yaygın olarak kullanılan bir depolama aracıdır. Bir Blu-Ray disk, 25-50 GB (tek katman), veri tutabilir (çift katmanlı bir Blu-Ray disk söz konusu verinin iki katı kadar veri tutabilir. 50-100 GB kadar). Blu-Ray diskleri rastsal erişimli cihazlardır.

[84] Quizlet, "ICT-3.Storage Devices and Media," **a.y.**

- HD DVD: Yüksek yoğunluklu DVD (HD-DVD) diskler yaklaşık 15 GB veri tutabilir (çift katmanlı bir HD-DVD bunun iki katı tutabilir). HD-DVD'ler rastsal erişimli cihazlardır.
- CD-R ve DVD-R disklerde veri işlenir ancak silinmez. Disk doluncaya kadar veri eklemeye devam edilebilir, ancak herhangi bir veri kaldırılamaz veya disk tam olarak tekrar kullanılamaz.
- Yeniden Yazılabilir CD (Compact Disc-ReWritable, CD-RW) ve Yeniden Yazılabilir DVD (Digital Versatile Disc-ReWritable, DVD-RW) diskler, CD-R'lar ve DVD-R'ların aksine, üzerlerinde veri işlenebilir ve ayrıca silinebilir, böylece diskler yeniden kullanılabilir.
- DVD-Rastsal Erişim Belleği (DVD-RAM) diskleri yeniden yazılabilir bir DVD türüdür. Genellikle bir disket tarzı durumda gelir. DVD-RAM diskleri normal bir DVD'ye benzer bir kapasiteye sahiptir ve 4.7 GB veri tutar. DVD-RAM diskleri rastsal erişimli cihazlardır.
- Flash bellek (Flash Memory), Elektronik Olarak Silinebilen Programlanabilir Salt Okunur Bellek (EEPROM) türüdür. Flash bellek geçici değildir (ROM gibi), ancak içinde depolanan veriler de silinebilir veya değiştirilebilir (RAM gibi).
- Taşınabilir Hafıza Kartı (Memory Stick) geçici olmayan, rastsal erişimli depolama aygıtlarıdır. Bu küçük cihazların her birinde, bir USB arayüzüne bağlı bir flash bellek bulunur. Bilgisayara takıldığında bir sürücü olarak görünür. Daha sonra dosya eklenebilir, silinebilir. Bilgisayarlar arasında herhangi bir tür dosyayı taşımak için kullanılır.
- Dijital cihazların çoğu (kameralar, cep telefonları, MP3 çalarlar, vb.) kompakt, geçici olmayan veri depolaması gerektirir. Flash bellek kartları bunu sağlar ve çeşitli şekil ve boyutlarda görülebilir. Cep telefonlarında, telefon numarası, telefon rehberi, kısa mesaj vb. içeren bir Abone Kimlik Modülü (Subscriber Identity Module, SIM) kartı bulunur. Yine cep telefonlarında dâhili hafızada belge, resim, video, ses kaydı, çeşitli uygulamalar vb. bilgiler de tutulabilir.

Manyetik ve optik ortamları ve araçlarının imha edilmesi *Elektronik Belgenin (Sanal Nesnenin) İmhasına Yönelik Yöntem ve Teknikler* bölümünde açıklanmıştır. Bu ortam ve araçların bıraktığı izler ise karmaşık bir konudur. Optik ortamlardaki bazı araçlarda üzerine yazma gibi verinin tamamen yok edilmesi mümkün görünse de bu araçların fiziksel olarak imhası kesin bir çözümdür. Optik ortamın hem kapasite açısından yüksek olmaması hem de maliyet açısından uygun oluşu imha edilen belgelerin bulunduğu ortamın da imha edilmesine yardımcı olmaktadır.

Manyetik ortamın optik ortam gibi fiziksel olarak imha edilmesi çoğu zaman uygulanmayabilir. Yüksek kapasiteli ve maliyetli olmaları fiziksel imhayı daha da zorlaştırmaktadır. Bu nedenle tekrar kullanımı durumunda silinmiş veriye ait izlerin bulunmaması gerekir. Bunun için de manyetik araç veya ortamların nasıl çalıştığını anlamak yerinde olur. Gelişen teknolojiyle beraber saklama ve depolama ürünleri de gelişmektedir. Eskiyen teknolojiyi yeni ürünlerle uyumlu hale getirmek için eskiden yeniye bir veri aktarımı yapılmaktadır. Bu veri aktarımı yapıldıktan sonra eskiyen teknolojideki verinin silinmesi için format atılmaktadır. Format işletim sistemiyle (OS) içerik arasında bağlantıyı koparmaktadır. Farklı işletim sistemleri ayrılmış kümeleri birleştirmek için farklı yöntemler kullansa da format atmak işi zorlaştırmaktadır. Ancak format atmak da içeriğin tamamen silinmesini sağlamaz. Aksine format atıldıktan sonra da içeriğe erişim mümkündür. Her ne kadar işletim sistemleri içeriğe erişemez olsa da içeriğe erişebilecek çeşitli programlar mevcuttur. Format atma haricinde verileri silmenin bir yolu da dosya ve dizinleri silmektir. Bu yöntemde işletim sistemi dosya veya klasör ismin ilk harfini "?" (soru) işaretiyle değiştirir. Bu işlem sonunda dosya ve dizin silindi olarak işaretlenir. Söz konusu dosya veya dizin alanı genel kullanım için açılmış olur. Ancak silindi olarak gösterilen dosya veya dizin olduğu gibi durmaktadır. Dikkate alınması gereken bir diğer husus, ortamdaki verilerin düzenlenmesi ile ilgilidir. Ortam, genel kullanıma tahsis edildikten sonra kullanılabilir kümelerin havuzunun bir parçası haline gelen sabit boyutlu kümeler halinde düzenlenir. Silinen dosya veya klasörlerin içeriği, toplanan kümelerden birini veya birkaçını kullanan yeni verilerle potansiyel olarak ortamda kalır. [85]

[85] ICS JMR, "Wipe Out Storage Devices Part 1," (Çevrimiçi) https://ics-iq.com/blog/wipe-out-storage-devices-part-1/, 17 Temmuz 2019.

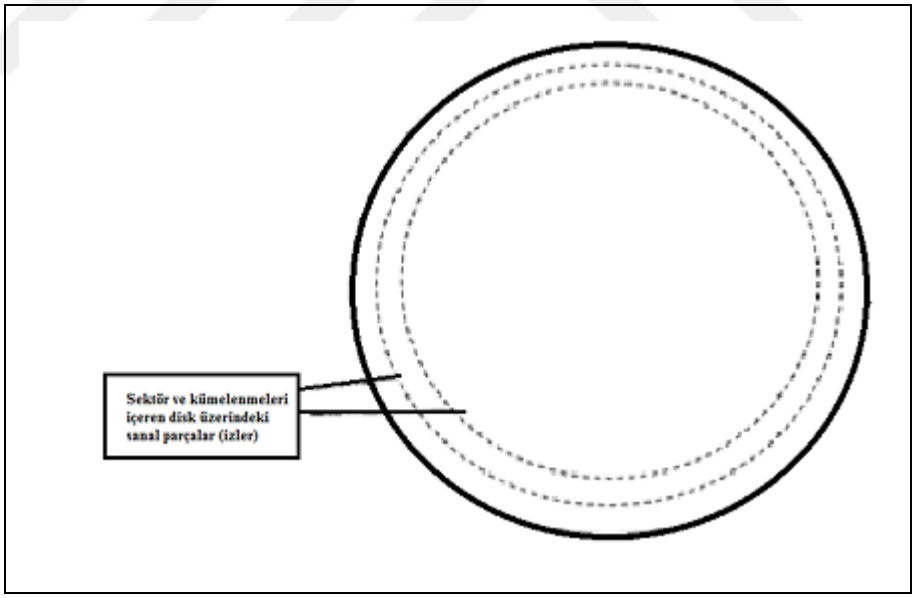
Kümelerin boyutu, sabit olarak kabul edilmekle birlikte birkaç olası boyuta sahiptir (en az 2K bayttan -4 sabit sürücü sektörü- en fazla 64K bayta kadar). Bir kümenin boyutu genellikle sürücü bölümlemesi sırasında Windows tarafından otomatik olarak belirlenir ve sürücü boyutundan türetilir (sürücü ne kadar büyükse, küme boyutu o kadar büyük olur). Tipik bir dosya rastsal bir boyuta sahip olduğundan, kümeyi tamamen doldurması mümkün değildir. Örneğin, "Test1" olarak adlandırdığımız ve 15.6K bayt olan bir dosya düşünülebilir. Bu dosya, 4K kümesiyle yapılandırılmış bir sabit diskte 4 kümeyi (diyelim ki 241, 242, 243 ve 244) işgal eder. Son küme, dördüncü olan, 3.6K bayt Test1 verisini içerir (15.6K – 3.6K=12K). Şimdi, kullanıcının Test1 dosyasını sildiğini ve işletim sisteminin de 4 kümesini ayırdığını varsayalım. Kullanıcı şimdi yalnızca 12.1K bayt olan ancak 4 kümeyi kaplayan yeni bir "Test2" dosyası üretmiş oluyor. Diyelim ki, bu örnek adına, işletim sisteminin aynı kümeleri (241, 242, 243 ve 244) yeni Test2'ye atadığını varsayalım. Şimdi son küme, Test1 ve yeni dosyadan .1K bayt ve eski ve silinen dosyadan Test1 3.5K bayt artık verilerini içerir. Yeni ayrılmış dosya Test 2 tarafından kullanılmayan zincirdeki son kümenin bu alanına pasif alan (Slack Area) denir. İşletim sistemi dosyanın boyutunu takip ettiğinden, pasif alandaki bilgiyi dikkate almaz ve normal kullanımda bir sorun yaratmaz. Bununla birlikte, eski bir sürücüden veya eski bir bilgisayardan kurtulan ve verilerinden hiçbirini bu sürücüde veya bilgisayarda bırakmak istemeyen bir kullanıcı için bir sorun haline gelir. Bunun için tüm sektörlerde sektör sektör veri kalıbı ile üzerine yazma işlemi yapılması, geriye herhangi bir bilgi bırakmamak adına güvenli sayılabilir. Bununla birlikte, diskte, parçalar arasında halen kalan veri enerjisinin bulunduğunu bilmemiz gerekir. Bu bilgi, sürücüyü sökmeden ve çok pahalı araçlar kullanmadan alınamaz.[86]

Sabit disk ortamından bilgileri silmenin veya yok etmenin bir diğer önemli yönü, parçalar arasında kalan veri enerjisiyle ilgilidir. Sabit disk ortamındaki bilgiler manyetik enerji olarak kaydedilir. Parçalar fiziksel olarak ortama kazınmamıştır; sanal izler olarak vardır. Sanal parça olarak adlandırılırlar çünkü bir parçanın konumlandırma bilgileri veri akışına gömülüdür ve veriler tekrar yazılsa bile değişkenlik gösterebilir.

[86] **A.y.**

Aşağıdaki (Şekil 3.9) gösterildiği gibi, medya ortamına yapılan her yeni yazma geçişinde, önceki yazma geçişlerinden gelen bazı düşük seviyeli enerji diskte kalır. Okuma sırasında, sürücünün elektroniği, okuma kafasını tabakanın ortasına yerleştirmek ve sadece yüksek enerji bilgisini dikkate almak üzere tasarlanmıştır. Geriye kalan enerji, genel gürültüye eklenir, ancak büyük bir sorun olarak kabul edilmez. Bununla birlikte, özel araçlarla, "artık" olarak kalan bilgilerin önemli kısımlarını önceki yazma geçişlerinden alabilmektedir. Hedef bilgi üzerine yazma işleminin sayısı ve başarısı, geriye kalan bilginin en aza indirgenmesini sağlar. Çünkü ilgili geçişten sonra yazılan bütün üzerine yazma veri kalıpları, geriye kalan artık veri enerjisinden gelen bilgilerin yeniden inşası için de önemlidir. ABD Savunma Bakanlığı (DoD), "00" ile değiştirilen 6 "FF" geçişi ve ardından "F6" ile yedinci geçiş olarak sabit disk ortamının elektriksel olarak silinmesi şartını belirtir. Ayrıca de-manyetize etme işlemini gerçekleştirecek araçlara da ihtiyaç duyulur.[87]

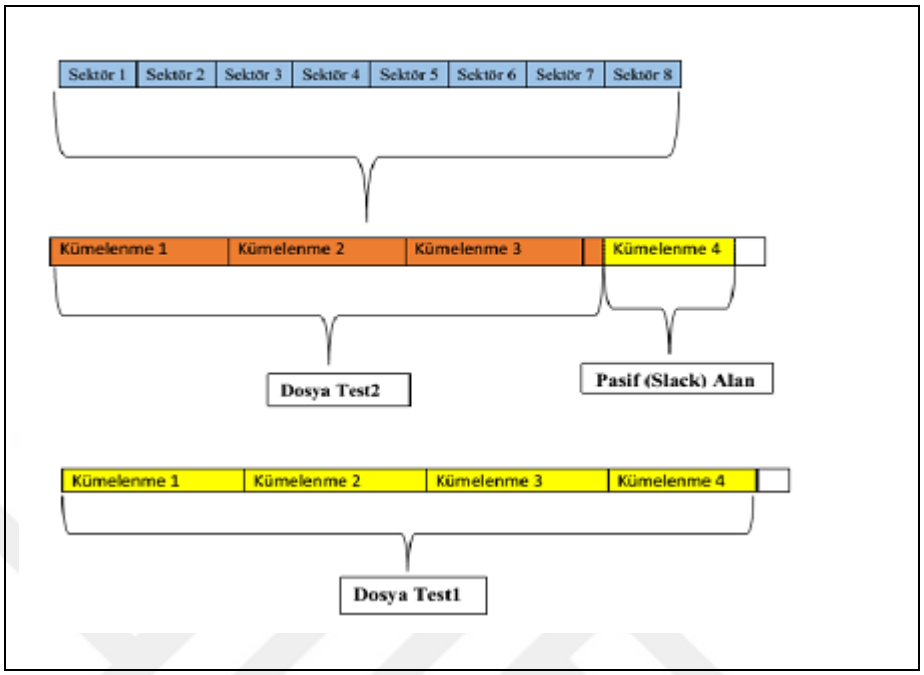
Şekil 3.11: Disk Sürücüsü Ortamına Tek Bir Yüzeyden Bakış



(**Kaynak:** ICS JMR, Wipe Out Storage Devices Part 1)

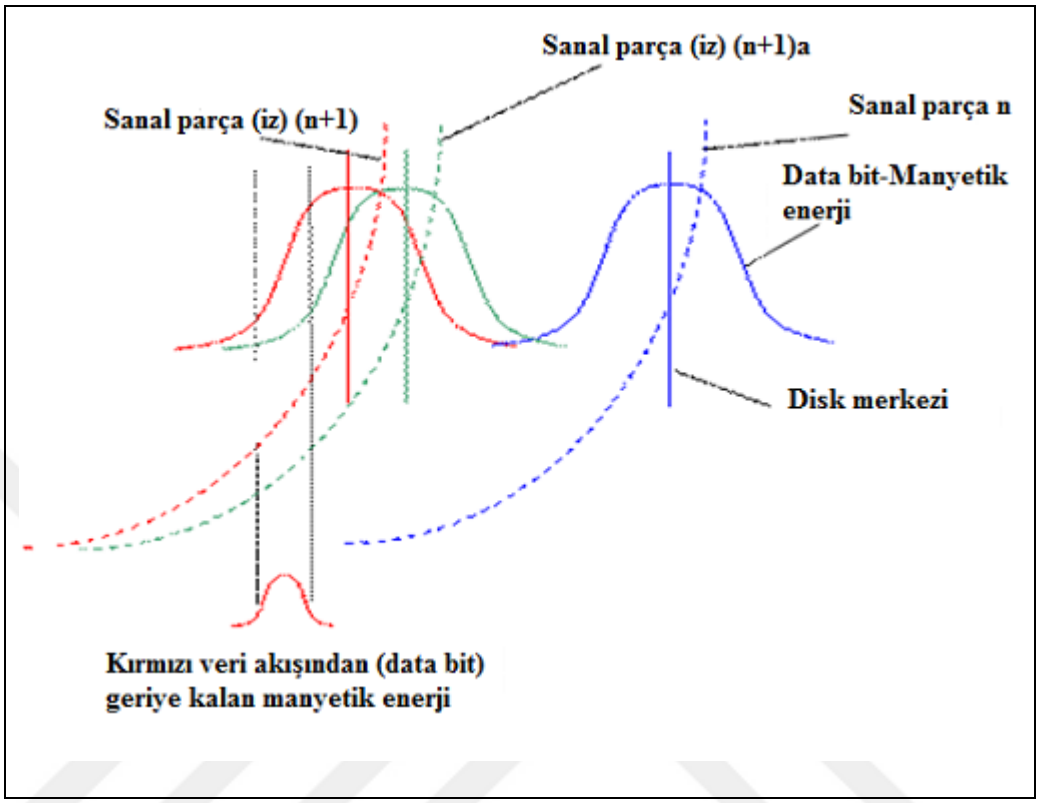
[87] **A.g.m.**

Şekil 3.12: Disk Sürücüsü Sanal Sektör ve Kümeler



(**Kaynak:** ICS JMR, Wipe Out Storage Devices Part 1; Yazar tarafından Türkçe olarak yeniden hazırlanmıştır.)

Şekil 3.13: Disk Sürücüsündeki Veri Enerjisine Ait İzler



(Kaynak: ICS JMR, Wipe Out Storage Devices Part 1; Yazar tarafından Türkçe olarak yeniden hazırlanmıştır.)

Bunun için Tablo 4.6'da açıklanmış imha yazılım programlarının kullanılması mecburidir. Kullanılacak yazılımın hiçbir şekilde veriye ait iz bırakmaması için yazılım özellikleri ve yazılımın kullandığı imha metotlarının hangi imha standardına göre hazırlandığını bilmek önemlidir. Bazı imha yazılımları hem yazılımsal hem de donanımsal olarak silinen veriyi geri getirme kabiliyetine sahip olabilir. Bazılarında ise hiçbir şekilde yazılımsal veya donanımsal geri dönüşü olmayacak şekilde veri tamamen imha edilir. Yazılımlar arasındaki bu farklılık yazılımın hangi imha standardına göre hazırlandığı ile ilişkilidir. Yazılımsal ve donanımsal olarak veri erişimi mümkün olmayan yazılımların tercih edilmesi kurum politikalarında yer almak zorundadır.

Depolamaya ilişkin kullanılan bazı kavramları da burada kısaca açıklamakta yarar vardır. Bu kavramlar; NAS (Network Attached Storage), SAN (Storage Area Network) ve DAS (Direct Attached Storage)'dır. NAS, ağa bağlı depolama, SAN, veri depolama ağları ve DAS ise doğrudan bağlı depolama anlamlarına gelmektedir. Kısaca şu şekilde açıklamak yerinde olacaktır:

- NAS: NAS ünitesi, ana üniteye sahip bir bilgisayar ve bir ağa bağlı depolamadan oluşur. Bu depolama birimi, FreeNAS, FreeBSD ve daha pek çok özellikli işletim sistemine sahip bir veya daha fazla sabit disk içerir. İstemciler, NFS gibi protokolleri kullanarak verilere erişebilirler. İşletim sisteminden bağımsız olarak veri paylaşımı sağlar. Kullanılabilirliği artırmak için, birden fazla dosya kopyası birden fazla konumda saklanır. Ayrıca, gerekli bant genişliğini ve erişim süresini azaltır. NAS'ta veriye dosya ve üstveri ile erişilir.[88]
- SAN: Blok düzeyinde depolama ile yüksek hızlı depolama sistemi sağlar. Bununla birlikte, istemci dosya düzeyinde erişim sağlamak için SAN'ın üstüne dosya sistemi yükleyebilir. SAN normalde performansı ve hızı iyileştirmek için fiber kanalla bağlanır. SAN'da dosya paylaşımı işletim sistemine bağlıdır. SAN'da, kullanılabilirliği arttırmak için birden fazla konuma çoğaltılan blok yoluyla verilere erişilir. SAN, TCP / IP üzerinden SCSI, AoE, FcoE ve daha pek çok protokolü kullanır.[89]
- DAS: Sunucuya doğrudan bağlanan SCSI arabirimi veya fiber kanalı aracılığıyla bir depolama yapılabilen bir araçtır. Basit yapısı, düşük maliyetli oluşu avantajları olarak sayılabilir. Ancak gerçek anlamda ağ yükünü paylaşma anlamında zorlukları arttırması büyük maliyetlere sebep olabilir, ayrıca bakımları da maliyetlidir.[90] Basit anlamda bir veya daha fazla disk sürücüsünün doğrudan bir sunucu bilgisayara bağlanmasıyla çalışabilen sistemlerdir.[91]

---

[88] Amol Jaikar v.d., "Performance Analysis of NAS and SAN Storage for Scientific Workflow," Conference: 2016 International Conference on Platform Technology and Service (PlatCon), (Çevrimiçi) http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7456814&isnumber=7456759, 17 Temmuz 2019, DOI: 10.1109/PlatCon.2016.7456814.

[89] **A.g.m.**

[90] Lihua Geng, "The Research of Digital Library Mass Information Storage System Architecture," International Symposium on Computers & Informatics (ISCI 2015), s. 1860, (Çevrimiçi) https://download.atlantis-press.com/article/17628.pdf, 17 Temmuz 2019, DOI: 10.2991/isci-15.2015.245.

[91] Turgay Saraçoğlu, Veri Depolama Ağları ve Yeni Gelişen Teknolojiler, 2006. (Çevrimiçi) http://www.if.com.tr/pages/images/makaleler/if-makale-0603-1.pdf, 18 Temmuz 2019; Cengiz Aydın, "Elektronik Belgelerin Arşivlenmesi ve Erişim," **Yayımlanmamış Doktora Tezi**, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, 2010, s. 77.

Kurumların hizmet sunduğu elektronik ortamlar için farklı ihtiyaçları ve gereksinimleri vardır. Bir kurum için maliyet sorunsa, DAS'ın seçilmesi makul olabilir, kurumun sanal ortamı küçük ve veri çoğaltma gibi gelişmiş özellikler gerektirmiyorsa ayrıca maliyet problem ise DAS iyi bir tercih olabilir. Büyük ölçekli sanal ortamlarda hizmet veriliyorsa NAS veya SAN daha uygun olabilir. Çok sayıda sanal ana bilgisayarı klonlama yeteneğine ihtiyaç duyuluyorsa, NAS daha iyi bir seçenektir. Ancak, en yüksek düzeyde kullanılabilirlik ve esneklik gerekiyorsa SAN daha uygun olacaktır.[92] İmha açısından değerlendirildiğinde NAS'ın birden fazla dosya kopyasının farklı konumlarda bulundurması dikkat çekicidir. Bu da silinmesi gereken dosyaların tüm kopyalarının silinmesini gerektirir. Bu açıdan NAS'a bağlı tüm depolama alanlarının temizlenmesi güç olabilir.

3.3.5. Yedekleme (Backup) İzleri

Yedekleme,[93] "orijinal verilerin silinmesi veya zarar görmesi durumunda, dosyaların geri yüklenebilmesi için, bant veya disk gibi depolama ortamlarında tutulan yazılım veya veri dosyalarının bir kısmının veya tamamının bir kopyası"[94] olarak tanımlanmaktadır.

Yedekleme, arşivleme sistemlerinin aksine verileri kısmen ya da tamamen diğer aktif verilerle birlikte kullanılacak mevcut bir aktif sisteme geri yüklemeyi düşünmez. Yedekleme sistemleri, bazı felaketlerin bir sonucu olarak kaybolan ya da bozulmuş olan aktif sistemleri tamamen geri yüklemek için tasarlanmıştır. Bu nedenle, çevrimdışı arşivlerde depolanan veriler genellikle aktif sisteme geri yüklenip aranabilirken, yedekleme dosyalarının aranması genellikle sistemden aktif veri almayı veya sistemi

[92] Chris Evans, "DAS vs. NAS vs. SAN: Which is best for virtual storage?", 2009, (Çevrimiçi) https://www.computerweekly.com/tip/DAS-vs-NAS-vs-SAN-Which-is-best-for-virtual-storage, 18 Temmuz 2019.

[93] Yabancı literatürde yedeklemenin karşılığı olarak kullanılan backup veya back up kavramlarının iki farklı yazılışı söz konusudur. Bilgi teknolojileri literatüründe yedekleme anlamında genellikle archive (arşiv) de kullanılır.

[94] Pearce-Moses, **A Glossary of Archival and Records Terminology**, s. 45.

"klonlamayı" gerektirir.[95] Yedeklemede temel kuralın yedeklemenin farklı yerlerde olmasıdır. Farklı yerlerle ilgili olarak 3 yerin belirlenmesi ideal olarak görülmektedir.[96]

Yedekleme kendi içinde çeşitli yöntemlere ayrılmaktadır. Bu yöntemler aşağıda açıklanmıştır:[97]

Tam yedekleme (full), seçilmiş olan tüm dosya ve klasörlerin kopyalanmasıdır. Tam bir yedekleme yapıldıktan sonra aşağıdaki yedeklemelerden biri seçilebilir.

Artımlı yedekleme (incremental), yalnızca bir tam yedek veya bir artımlı yedekten sonraki yapılan değişiklikleri içerir. Artımlı bir serideki ilk yedekleme her zaman bir diferansiyel yedeklemedir; ancak bundan sonra, her artımlı yedekleme yalnızca bu son artımlı yedeklemeden bu yana yapılan değişiklikleri içerir.

Bundan sonra her artımlı yedeklemenin boyutu genellikle diferansiyel yedeklemeden daha küçüktür ve yapılması daha hızlıdır. Bu, çok sık artımlı yedeklemeler yapılmasını sağlar ve daha sonra gerektiğinde veri tabanını daha kesin bir noktaya geri yüklemeye yardımcı olur. Ancak, artımlı yedeklemelerle verileri geri yüklemek daha uzun sürebilir. Genel olarak, örneğin, t zamanına kadar olan verileri geri yüklemek için, tam yedeklemeyi geri yüklemekle başlanır ve sonra artımlı yedeklemeleri t süresi için alınan artımlı yedekleme yüklenir.

Diferansiyel yedekleme (differential backup), tam bir yedeklemeden sonra verilerdeki tüm değişiklikleri içerir. Örneğin, belirli bir zamana kadar yapılan yedeklemeyi yüklemek için öncelikle tam bir yükleme yapılır. Daha sonra gelinen zamana kadar olan tüm değişiklikler yüklenir. Sadece son değişiklikleri takip ettiği için hem alansal olarak hem de hızlılık açısından yarar sağlar. Geri yükleme yapılırken önceki tam ve

[95] "Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production," Sedona Conference, 2003; Akt: Pearce-Moses, **A Glossary of Archival and Records Terminology**, s. 45.

[96] Pegeen Turner, "Electronic Records Retention and Destruction," 2014, (Çevrimiçi) https://www.lawyersmutualnc.com/risk-management-resources/articles/electronic-records-retention-and-destruction, 19 Temmuz 2019.

[97] **MySQL Enterprise Backup User's Guide (Version 4.1.3)**, "4.3.3 Making a Differential or Incremental Backup," 2019, (Çevrimiçi) https://docs.oracle.com/cd/E17952_01/mysql-enterprise-backup-4.1-en/mysqlbackup.incremental.html, 20 Temmuz 2019.

artımlı yedeklemelerini istemesi dezavantajdır. Yedekleme yöntemleri arasındaki farklılıklar aşağıdaki tabloda gösterilmiştir.[98]

Tablo 3.3: Özellikleri Açısından Yedekleme Yöntemlerinin Karşılaştırılması

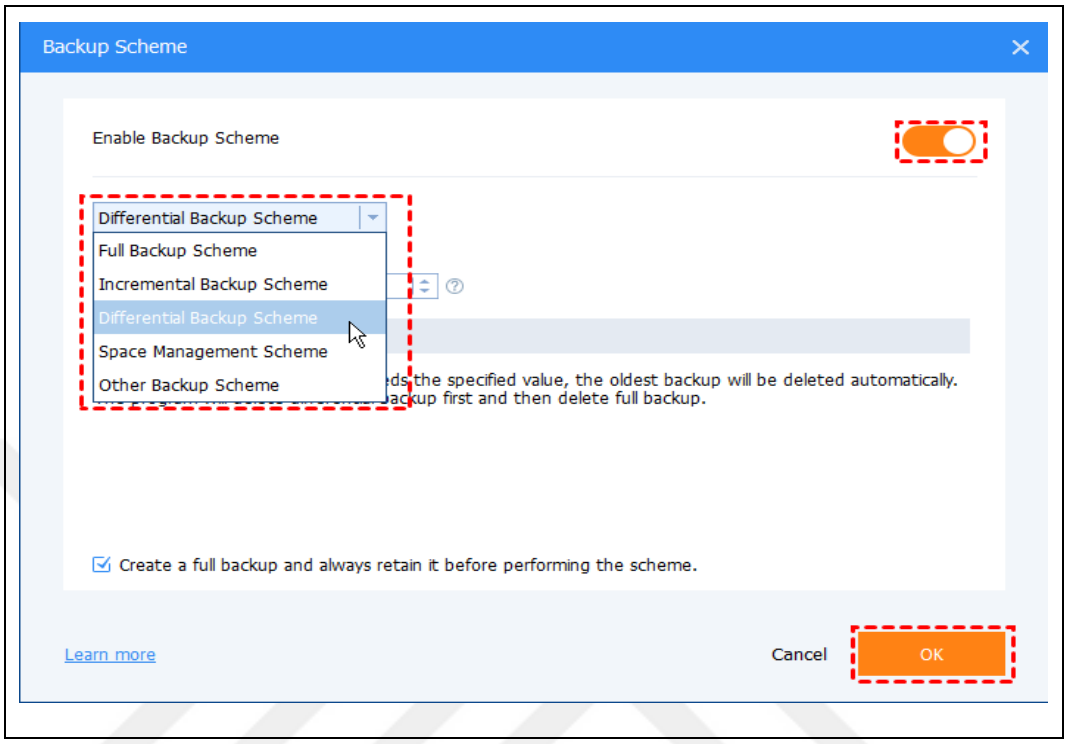
Yöntemler	**Yedekleme Verisi**	**Yedekleme Süresi**	**Görüntü Saklama Alanı**	**Geri Yükleme Hızı**
Tam Yedekleme	Tüm veri	En uzun sürede	En fazla miktarda	En yavaş
Artımlı Yedekleme	Alınan son tam yedeklemeden itibaren bütün değişiklikler veya eklenenler	Diğer yedeklemelere göre ortalama sürede	Diğer yedeklemelere göre ortalama miktar	Diğer yedeklemelere göre ortalama hız
Diferansiyel Yedekleme	Alınan son tüm veya artımlı yedeklemeden itibaren bütün değişiklikler veya eklenenler	En kısa sürede	En az miktarda	En hızlı

(**Kaynak:** AOMEI Backupper, " Backup Scheme," (Çevrimiçi) https://www.backup-utility.com/screenshot/en/adv/backup/popup/enable-backup-scheme.png)

Yedeklemenin bu çeşitlere bağlı olarak planlı yapılması önemlidir. Bu planlar belirli bir zaman aralığını kapsayacak şekilde yapılır. Saatlik, günlük, haftalık, aylık gibi zaman aralıkları belirtilebilir. Yedekleme yönteminin seçilmesi ve bu seçimin belirli bir zaman aralığında olmasının istenmesi günümüz yedekleme yazılımlarıyla sağlanabilmektedir. Yazılımda hangi yedekleme yöntemin seçileceği tercih olarak sunulmaktadır. Aşağıdaki ekran görüntüsü söz konusu tercihleri göstermektedir.

[98] AOMEI Backupper, "Backup Scheme," (Çevrimiçi) https://www.backup-utility.com/screenshot/en/adv/backup/popup/enable-backup-scheme.png, 21 Temmuz 2019.

Şekil 3.14: Backup Şeması



(**Kaynak:** Backup Scheme, (Çevrimiçi) https://www.backup-utility.com/screenshot/en/adv/backup/popup/enable-backup-scheme.png, 15 Temmuz 2019.)

Yedekleme yazılımlarının varlığı yedeklemedeki izleri de beraberinde getirmektedir. Kullanılacak olan yazılımın yedekleme yaparken daha önceki yedeklemeleri saklayıp saklamadığı izler açısından önemlidir. Yukarıda gösterilen ekran alıntısında eski yedeklemelerin otomatik olarak silineceği belirtilmiştir. Kurumların bu yazılımları tercih ederken eski yedeklemelerin silinip silinmediğini, eğer siliniyorsa hangi yöntemin kullanıldığını, silme işleminden sonra silinmiş veriye erişimin mümkün olup olmadığını bilmeleri zorunludur. Kurumlar bu bilgileri varsa anlaşmalı bir yazılım firmasıyla paylaşmaları, eğer yoksa bilgi işlem birimlerinin bu konuyla ilgili farkındalığının olup olmadığı noktasında iletişim halinde olmak ve bu birimlerin konuya dikkatini çekmek yararlı olacaktır.

Yedeklemeye ilişkin izler yedeklemelerin kendisidir. Her bir yedekleme bir iz anlamına gelmektedir. Mevcut yedeklemeden önceki yedeklemelerde silinen bir belgenin silinmeyip mevcutta yer alması, varlığından habersiz imha edilmiş belgelerin

sistem içinde yer almasına neden olacaktır. Hazırlanacak olan saklama planlarına yedekleme kopyalarının dâhil edilmesi gerekir. Saklama süreleri sonunda yedekleme kopyalarının da imha edilmesi göz ardı edilmemelidir.

3.3.6. Erişim İzleri

Erişim; (1) kataloglar, indeksler, erişim araçları veya diğer araçları kullanarak ilgili bilgileri bulma yeteneği, (2) yasal olarak belirlenmiş gizlilik, mahremiyet ve güvenlik izni kısıtlamaları dâhilinde kullanım (danışma veya başvuru) bilgisini bulma ve alma izni, (3) depolama ortamından bilgi elde etmenin fiziksel süreçleri[99] olmak üzere üç şekilde tanımlanmaktadır. Erişim, tanımlardan da anlaşılacağı üzere gizlilik, mahremiyet ve güvenlik izni ile depolama ortamından alınan bilgileri kapsamaktadır. Erişim, yetkili ve yetkisiz erişim olarak iki şekilde ele alınabilir. Bunların açıklanması konunun belge izleri açısından anlamlı olmasını sağlayacaktır.

Yetkili erişim, bilgiye erişime güvenli bir yol sağlama amacını taşır. Kimliklendirme ve doğrulama yetkili erişimde güvenliğin temel unsurlarıdır. Bir kurumdaki tüm kullanıcılar kimliklendirme ve doğrulamaya dâhildir ve bunların kurum politikasında yer alması gereklidir. Kimliklendirme ve doğrulamada "gerçek kişiler olan kullanıcılar" sisteme giriş (log in) yapmak istediklerinde bir kimlik tanımlayıcı ve şifre ile giriş yapabilmektedir (kimlik tanımlayıcısı ve şifre haricinde özel araçlar veya biyometrik doğrulama araçlarının kullanımı mümkündür).[100] Kişilerin yetkili olarak sistemlere erişimi;

- Fiziksel bilginin bulunduğu yerlere erişimi;
- Veri oluşturma, okuma, düzenleme veya silme[101] gibi fiziksel belgeler ve dosyalar dâhil olmak üzere dosya sistemi izinlerini;
- Program çalıştırma hakkı gibi program izinlerini;

---

[99] Pearce-Moses, **A Glossary of Archival and Records Terminology**, s. 2.

[100] The Government Communications Security Bureau, **The New Zealand Information Security Manual**, 2019, s. 197-212, (Çevrimiçi) https://www.nzism.gcsb.govt.nz/assets/NZISM/pdf/NZISM-V.3.2-Jul-2019.pdf, 22 Temmuz 2019.

[101] Silme işlemi resmi belge olma özelliği taşımayan, belgelerin üretilmesine yardımcı verinin silinmesine yönelik işlemi ifade etmektedir. Resmi belgelerin silinmesi saklama planları dışındaki resmi belgelerin silinmesini gerektiren durumlarda kurumsal hiyerarşideki yetkili kişilerin yasal çerçevedeki ortak kararı ile yapılabilir.

- Veri tabanındaki bilgileri alma, yazdırma veya güncelleme hakkı gibi veri haklarını kapsamaktadır.

Yetkili olarak sisteme erişim sağlayan kullanıcılar, sistem içindeki rolleri ve ait olduğu grubu tanımlayan bir profil içinde yer almalıdır. EBYS kapsamında bulunan elemanların erişim hakları TS 13298 (2015)'e göre tasnif dışı, hizmete özel, özel, gizli ve çok gizli olmak üzere beş kademede tanımlanmıştır.[102] Bu tanımlamalar yetkili erişim çerçevesinde değerlendirilmektedir.

Yetkili erişimde izler açısından dikkat edilmesi gereken hususlar vardır. Bunlar sistem içinde tanımlanmış kimlik ve şifre ile sisteme giriş yapabilen kullanıcıların bilgilerinin korunmasını böylelikle yetkili erişim altında yetkisiz erişime karşı tedbirler geliştirilmesini zorunlu kılar. Özellikle kurumsal politikalarda sisteme erişim sağlayan kimlik tanımlayıcıları ve şifrelerinin sistem içinde saklanılmasına izin vermemelidir. Bu düzenleme yetkili kullanıcı tanımlayıcılarının bilgilerinin korunması yanında, ayrıca kimlik doğrulama bilgilerinin güvenli bir şekilde iletilmesi, geçerli bir sistem kullanıcısı kimliği altında bir sisteme erişmek için bir saldırgan tarafından ele geçirme ve ardından kimlik doğrulama bilgilerinin kullanılması riskini azaltır. Bu da kurumların sistem kimlik doğrulama verilerinin kurum ağlarına veya tüm kamu sistemindeki ağlara geçerken korunmasını da sağlayacaktır. Politika ve düzenlemelerde yetkili erişimde şifre kullanımı ve değişikliklerini izlemek için bir sistemin varlığı da önemlidir. Yetkili erişim izleri için olaylar ve bilgiler şunları içermelidir:[103]

- Kullanıcı tanımlayıcısı
- Başarılı ve başarısız girişler
- Şifre değiştirme prosedürlerinin kullanılması
- Kullanıcıların geçici olarak pasif hale getirilmesi (erişimi engelleme gibi)
- Tarih/Zaman
- Bilginin bulunduğu fiziksel konum

[102] **TS 13298**, s. 20.

[103] Ohio Electronic Records Committee, **Ohio Trustworthy Information Systems Handbook**, 2011, s. 24. (Çevrimiçi) http://ohioerc.org/wp-content/uploads/2014/09/TISHandbook1.pdf, 25 Şubat 2019

- Erişim deneyicisinin kamera kayıtları veya fotoğrafı vb.

Bu bilgiler dışında kullanıcıları ve çevrimiçi eylemlerini günlüğe kaydetmek ve izlemek için bir sistem bulunmalıdır. Bu sistem denetim bilgilerini kapsamaktadır. Denetim bilgileri şunları içerebilir:[104]

- Log-in detayları (tarih, saat, fiziksel konum, vb.),
- Dosya / Belge oluşturma,
- Erişilen dosya / belge tanımlayıcıları ve beraberindeki aktivite (silme, değiştirme, hassasiyet / güvenlik seviyesinin değiştirilmesi),
- Erişilen cihaz kimlik tanımlayıcıları,
- Yazılım kullanımı,
- Basılı çıktı üretimi,
- Basılı çıktıda önemli bilgilerin görülmemesi için işaretlerin (hassas bilgi işaretlerinin ve etiketleme mekanizmalarının kapatılması dâhil) geçersiz kılınması ve
- Depolama aygıtlarına alınan çıktıların denetimi.

Bu bilgiler yetkili kullanıcıların bilgi ve belgenin bulunduğu ortam ve erişim araçlarını kapsamaktadır. Bu denetim izlerinin en azından aşağıdaki bilgileri kaydetmesi beklenir:[105]

- Belge tanımlayıcı,
- Kullanıcı tanımlayıcı,
- Tarih/Zaman
- Kullanım (Örneğin, üretim, sağlama, erişim, değiştirme, silme) dır.

Yetkili erişim dışında yetkisiz erişimler de söz konusu olabilir. Yetkisiz erişimin ilk örneğini 1969 yılında MIT (Massachusetts Institute of Technology)'de görmekteyiz. Öğrencilerin yazılım ve donanımı daha iyi veya daha hızlı çalıştırmak adına yaptıkları yazılım ve donanım değişiklikleri tarihteki ilk bilgisayar hackleme olayı olarak

[104] **Ohio Trustworthy Information Systems Handbook**, s. 24.
[105] **A.y.**

bilinmektedir.[106] 1969 yılından sonra da farklı tarihlerde önemli bazı kurumların (FBI, NASA gibi) hacklendiği bilinmektedir. Yetkisiz erişim olarak ifade edilebilecek olan hackleme vb. saldırıların günümüz yazılım ve donanım teknolojisiyle daha da arttığı ve bunlara yönelik tedbirlerin alınmasının zorunluluk haline geldiği önemli bir konudur. Türkiye'de bu saldırılara karşı geliştirilen ve elektronik belge yönetim sistemleri için hazırlanan rehberde saldırganların sisteme yetkisiz erişim yöntemlerinden bahsedilmektedir. Söz konusu rehber, Türk Standartları Enstitisünün *Elektronik Doküman ve Belge Yönetim Sistemi Koruma Profili*[107] olarak 24 Temmuz 2014 tarihinde yayınlanmıştır. Hazırlanan rehberde, saldırganların sahte veya çalınmış bir kimlikle sisteme yetkisiz erişim yapabileceği ifade edilmektedir. Bu girişimin çalıntı bir kimlik, sahte bir IP adresi, gibi yöntemlerle yapılabileceği de açıklanmaktadır. Saldırganın bu yöntemleri bazı zaaflarından dolayı yapabileceği ve bunların varsayılan kullanıcı adı ve şifrelerin değiştirilmemesi, basit şifrelerin kullanılması, gerçek sistemde test hesaplarının pasifleştirilmemesi, dosya yükleme özelliğinin yeterli derecede kontrole tabi tutulmaması olarak sırlanmaktadır. Söz konusu rehberde, saldırganın daha önceki veya aktif bir kullanıcının kalıntı verisinden veya dâhili ve harici sistem iletişimi esnasında oluşan kalıntı verilerden faydalanabileceği de dile getirilmiştir.[108]

Yetkisiz erişimlerin önüne geçmek adına kurum ve kuruluşlar sahip oldukları bilgi ortamını uygun şartlarda korumakla sorumludurlar. Genellikle yasadışı bir bilgi toplama kaynağı, uygun olmayan şekilde elden çıkarılan basılı kopya ortamları için uygun olmayan şekilde imha edilmemiş elektronik ortamların elde edilmesini sağlayabilir veya bilgilerin gizliliğine uygun olmayan bir şekilde imha edilmemiş ortamla-

[106] "The History of Hacking," (Çevrimiçi) http://plaza.ufl.edu/ysmgator/projects/project2/history.html, 11 Kasım 2019.

[107] "2013/4890 sayılı Bakanlar Kurulu Kararı doğrultusunda yayımlanan 06/20/2013 tarihli ve 28683 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren Ulusal Siber Güvenlik Stratejisi ve Eylem Planında, TSE bilgi güvenliği alanında ulusal standartlar hazırlamakla görevlendirilmiştir. Bu kapsamda, TSE'ye bağlı Ulusal Siber Güvenlik Özel Komitesi oluşturulmuş ve ihtiyaç duyulan pek çok teknik konuda standartlar ve rehber dokümanlar hazırlanmıştır" söz konusu rehber de bu çalışmaların bir ürünüdür (Türk Standartları Enstitüsü, **Elektronik Doküman ve Belge Yönetim Sistemi Koruma Profili**, **Sürüm 1.3.1**, 2014, s. 8 (Çevrimiçi) https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/2231/09012015111018-3.pdf, 8 Kasım 2019).

[108] Türk Satnadartları Enstitüsü, **Elektronik Doküman ve Belge Yönetim Sistemi Koruma Profili, Sürüm 1.3.1.**, s. 17.

rın klavye ve laboratuvar rekonstrüksiyonu yoluyla elde edebilir. Medya, kağıt formundaki geri dönüşüm kutularını, ekipman onarımı satıcılarına ve acil durumlara cevaben diğer sistemlere hot swap[109] işlemi yaparak kurumsal kontrolün içine ve dışına yayılabilir.[110] Bunun dışında hack ve brute force[111] gibi illegal kaynaklarca erişim söz konusu olabilir. Bunların hepsi sistem için yetkisiz erişim olarak bilinmektedir.

Yetkisiz erişimde elektronik ortamındaki bilginin silinmesi ve imhası kurumların ve kişilerin mahremiyetinin sağlanmasında önemli bir unsurdur.[112] ABD kanun kodlarında mahremiyet, "Kişisel gizliliği ve özel bilgileri koruma araçları da dâhil olmak üzere, bilgiye erişim ve bilginin ifşasına ilişkin yetkili kısıtlamaları korumak…"[113] olarak tanımlanmıştır.

Erişim izlerinde; sistem erişimi (system access), ayrıcalıklı erişim (privileged access), uzaktan erişim (remote access) olmak üzere üçe ayrılır. Bu üç erişimin etkinlik günlüğü ve denetimi belge izlerine ilişkin bilgiyi de vermektedir.[114]

3.3.7. Yazıcı/Tarama Cihazı İzleri

Elektronik ortamda belgelerin güvenliği ve izlenebilirliği kritik öneme sahiptir ve zaman zaman, istenen hukuki güvenlik şartlarını yerine getirmez. Belgelerin izlenebilirliği ile ilgili önemli bir unsur olan yazıcılar/tarayıcılar belgelerin izlenebilirliği açısından açıklanması gereken bir konudur. Bir belge kâğıda yazdırıldığında, belgenin erişim hakkına göre (tasnif dışı, hizmete özel, özel, gizli, çok gizli) bir güvenlik ve / veya gizlilik sorunu ortaya çıkar. Bu sorun basılı belgelerin (çıktı alınan) takibinin yapılmasıyla çözüme kavuşur. Bir belgenin orijinalliğini korumanın geleneksel bir

---

[109] Hot Swap, Sistem normal işlevini yerine getirirken, sistemi durdurmadan hatalı bir ünitenin değiştirilmesi ve yerine yenisinin eklenmesidir. Hot swaplar tipik olarak insanlar tarafından gerçekleştirilen fiziksel işlemlerdir. (Tom Clark, **Designing Storage Area Networks: A Practical Reference for Implementing Fibre Channel IP SANs**, Second Edition, Addsion-Wesley, Boston, 2003, s. 436.)

[110] **NIST 800-88**, s. 5.

[111] Dr. Öğr. Üyesi M. Fahri Furat ile yapılan görüşmede dile getirilmiş olup kaba kuvvet anlamında kullanılan bir kavram.

[112] U.S. Department of Commerce, National Institute of Standards and Technology (NIST), **NIST Special Publication 800-88 (Revision 1): Guidelines for Media Sanitization**, Haz. Richard Kissel v.d., Gaithersburg, 2014, s. 5, (Çevrimiçi) http://dx.doi.org/10.6028/NIST.SP.800-88r1, 23 Mart 2018.

[113] United States Code, **TITLE 44—Public Printing and Documents**, Sec. 3542, s. 147-148, (Çevrimiçi) https://www.govinfo.gov/content/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44.pdf, 21 Temmuz 2019; Akt: **NIST 800-88**, s. 5

[114] **The New Zealand Information Security Manual**, 2019, s. 197-212.

yöntemi, belge kopyalandığında (örneğin bir fotokopi yoluyla) orijinal belge üzerinde bulunabilecek bir filigran belgenin orijinalliğini tanımlamada yardımcı olabilir. Ancak bu filigranların verilen bir belgenin orijinal olup olmadığını göstermesi dışında, herhangi bir izlenebilirlik göstergesi sağlamaz. Örneğin, belgeyi kimin kopyaladığını göstermez.[115]

Bu problemin çözülmesi için ABD'de belgenin izlenebilirliğini sağlayan bir yöntem geliştirilmiş ve bu yöntemin patenti alınmıştır. Yöntem, bir doküman çoğaltılmış ise bunun kim tarafından yapıldığı ve dokümanın ne zaman çoğaltıldığını göstermektedir.[116] Yöntem, belgenin tüm kullanım bilgilerini tutması yanında bir görüntüleme aparatıyla da belge izlenebilirliğini sağlamaktadır. Yöntem, önceki belge kullanım bilgisini içeren bir bütünleşik veri depolama mekanizmasına sahip bir birinci belgenin temin edilmesini ve görüntüleme cihazına güncel kullanıcı bilgisinin sağlanmasını ayrıca mevcut kullanıcı bilgisinin, önceki doküman kullanım bilgisine, dokümanın bütünleşik veri depolama mekanizmasında eklenmesiyle yerine getirmektedir.[117] Kullanılan sunucu ve görüntüleme aparatı elemanları temsili olarak aşağıda verilmiştir.[118]

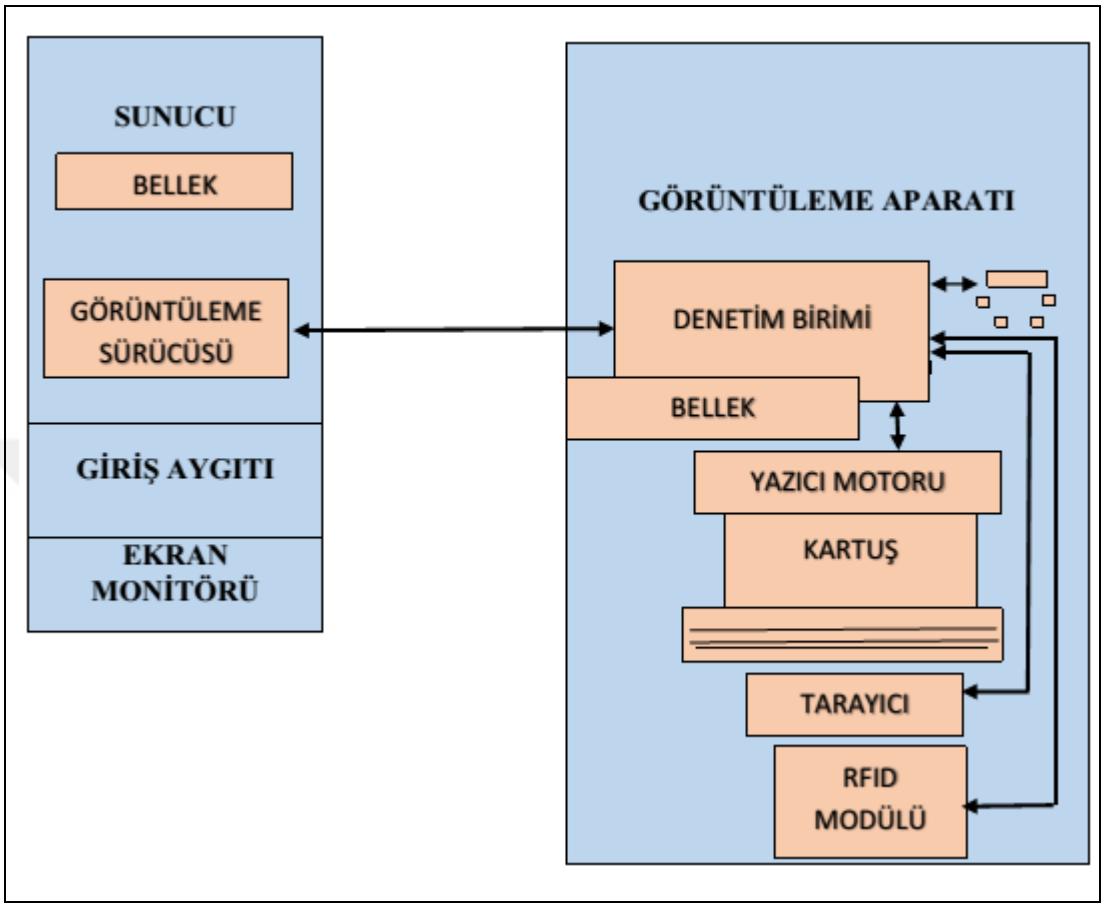
[115] Kevin Patrick Goffinet ve Timothy S. Seevers, **Method For Providing Document Traceability**, United States of America, Patent Number: US 2006/0265332 A1, Nov. 23, 2006.

[116] Yöntem, çok işlevli yazıcılar tarafından yapılan tüm işlemler dâhil olmak üzere bir kâğıt dokümanın geçmişi izlenebilmektedir. İzleme işi birleşik veri depolama mekanizması olarak isimlendirilen yazılım ve donanımla sağlanmaktadır. Bu mekanizmada önceki belge kullanım bilgisi yanında güncel kullanıcının belgeye ilişkin güncel aksiyonları da tutulmaktadır. Güncel kullanıcı bilgisi belgenin önceki kullanım bilgisine de eklenmektedir. Böylelikle belgenin önceki kullanım bilgisi ile güncel kullanım bilgisi zincir olarak birleşik veri depolama mekanizmasında söz konusu belgeyle ilişikli olarak sağlanmaktadır.

[117] **A.g.p.**

[118] **A.g.p.,** s. 2, şekil 1.

Şekil 3.15: Çıktı İzlenebilirliği Yöntemi



(**Kaynak:** Kevin Patrick Goffinet ve Timothy S. Seevers, Method For Providing Document Traceability, United States of America, Patent Number: US 2006/0265332 A1, Nov. 23, 2006; Yazar tarafından Türkçe olarak yeniden hazırlanmıştır.)

Yöntem özellikle EBYS'ler için aşağıdaki yararları sağlamaktadır:[119]

- Mevcut buluşun bir avantajı, bir belgenin orijinali gibi işlenmesinin, işlemin belgenin kendisine yerleştirildiği bir gösterge ile izlenebilmesidir.
- Bir başka avantajı, bir belgenin orijinalinden kopyalanan bir belgenin, bir ikinci kopya belgeyi oluşturmak için kendisinin kopyalanması durumunda, o zaman, bu çoğaltma işlemiyle ilişkili yeni mevcut kullanıcı bilgisinin, önceki belge kullanım bilgisine eklenmesidir. Kopyalanan ilk belgede hem önceki

[119] **A.g.p.**

doküman kullanım bilgisi hem de yeni geçerli kullanıcı bilgisi ikinci kopyalanan belgeye de eklenir.

Yöntemin bu yararlar haricinde aşağıdaki belgenin imha edilme süreçlerine de katkıları vardır:

- Saklama süresi sonunda imha edilmesi gereken bir belgenin çok işlevli yazıcılar/tarayıcılarla çoğaltılıp çoğaltılmadığı bilinir.
- Çoğaltılan bir belgenin kim tarafından yapıldığı bilinir.
- Sistem dışında belgenin kaç farklı kopyasının olduğu bilinir.
- Belgenin imha edileceği bilinip öncesinde çeşitli kopyaların alımını minimize ederek belgenin iz bırakmaması açısından çaydırıcı bir rol üstlenir.

3.3.8. Mobil İzleri

Mobil iletişim insanoğlunun hayatıyla bütünleşmiştir. Bireyler artık mobil araçlar olmadan kendilerini rahat hissetmemektedirler. Çok önceleri telefonların en popüler fonksiyonları arama ve mesaj göndermekten ibaretti. Günümüzde akıllı telefonlar insanların öğrenme, kazanma ve eğlenme aracı haline geldi. Bunlar mobil platformların gelişimi ile mümkün oldu. 20. yüzyılın sonlarında hayatımıza girmeye başlayan mobil uygulamalar, 21. yüzyılın başlangıcında mobil içerik ve uygulamalarıyla hızlı bir pazar gelişimi yakaladı. Akıllı telefonlar için işletim sistemleri (Windows Mobile, Symbian, RIM, Android, Mac iOS), standart cep telefonlarının geleneksel programlama ortamının aksine, üçüncü taraf yazılımların geliştirilmesinin önünü açmış oldu. Mobil üreticiler, ürünlerinin daha fazla satışını sağlamak için gün geçtikçe yeni özellikler ve programlar sunmaya başladı. Çünkü araştırmalar (Juniper Research), cep telefonlarının satışının dünya ekonomisinde önemli bir yer alacağını söylemekteydi. Mobil kullanıcılar telefonları kendilerine özelleştirmek için daha fazla işlev, fırsat ve seçenek talep etmeye başladıkça, mobil operatörler de kullanıcılarına yönetilebilir ve kazançlı bir yolla katma değerli içerik sağladı. Mobil geliştiriciler ise kullanıcıların taleplerini sınırlama olmaksızın karşılamak adına daha güçlü mobil uygulamalar sunmaya başladı. Son olarak, ahize üreticileri cihazlarını daha işlevli hale getirmek için uygun, güvenli ve istikrarlı bir platform ortaya koymak istediler. 1983 yılında ticari olarak satılabilen Motorola DynaTAC 8000X ilk cep telefonu özelliği taşır. İnternetin

kullanımı ile birlikte etelefon geliştiricileri telefonları internete uyumlu hale getirmek için WAP (Kablosuz Uygulama Protokolü, Wireless Application Protocol) kullanmaya başladılar. WAP kablosuz iletişim kullanan uygulamalar için kullanılmaktaydı. WAP'ın zamanla yetersiz kalması, belleklerin ucuzlaması, pillerin daha uzun süre kullanımı ve kompakt işletim sistemlerinin (Windows, Linux gibi) ortaya çıkmasıyla çeşitli farklı özel platformlar ve bunlar için uygulamalar söz konusu olmaya başladı. Bunlardan ilk ikisi Palm işletim sistemi (günümüzde Garnet işletim sitemi) ve RIM Blackberry işletim sistemidir. Nokia, Sony Ericsson, Motorola ve Samsung için Symbian işletim sistemi geliştirildi. 2007 yılında Apple'ın (iPhone iOS) işletim sistemini geliştirmesiyle işletim sistemleri arasında rekabet iyice arttı. Google'ın Android işletim sistemi de 2008 yılında geliştirilmiş oldu. Günümüzde son iki işletim sistemi yaygın olarak kullanılmaktadır.[120] Türkiye'de özellikle 2009 yılından sonra yaygınlaşan EBYS uygulamaları, bu uygulamaların mobil tabanlı uygulamalar olarak da geliştirilmesini zorunlu kıldı.

Mobil uygulama, akıllı telefon veya tablet bilgisayar gibi bir mobil aygıtta çalışmak üzere tasarlanmış bir tür uygulama yazılımıdır. Mobil uygulamalar, kullanıcılara standart bilgisayarlarda bulunan programlara benzer hizmetler sunmaktadır. Uygulamalar PC'lere göre genellikle küçük ve daha sınırlı fonksiyonlara sahip bireysel yazılım birimleridir.[121]

Standart sistemin mobil versiyonu olarak sunulan EBYS arayüzleri, kullanıcıların mobil cihazlarla her yerden her zaman sisteme erişimini mümkün kılmaktadır. Erişim imkânının birçok yöntemi bulunmaktadır. Mobil 4G, 4.5G, 5G, kablosuz LAN, Bluetooth gibi birçok farklı kanalla erişim sağlanabilmektedir. Mobil araçların çok sık kullanılması, özellikle de EBYS uygulamalarının mobil tabanlı olarak sunulması bel-

[120] John F. Clark, "History of Mobile Applications: Theory and Practice of Mobile Applications," (Çevrimiçi) http://www.uky.edu/~jclark/mas490apps/History%20of%20Mobile%20Apps.pdf, 14 Kasım 2019.

[121] Technopedia, "Mobile Application (Mobile App)," (Çevrimiçi) https://www.techopedia.com/definition/2953/mobile-application-mobile-app, 25 Temmuz 2019.

gelerin güvenirliği ve gerçekliğini riske sokmaktadır. Bu riskler arasında siber güvenlik riski, veri güvenliği riski ve sistem güvenliği riski gibi riskler sayılabilir.[122] Özellikle veri güvenliği ile ilgili riskte imha edilmiş veriye yetkili erişim kanalıyla veya yetkili erişim sistem açıklarıyla veya doğrudan saldırı ile erişim sağlanabilir. Mobil cihazlarla sosyal medya uygulamalarının yaygın olarak kullanıldığı facebook, instgram, twitter, flickr vb. kanallar güvenlik riskini daha da artırmaktadır. Günümüzde sosyal medya platformları olan ve yukarıda açıklanan ortamların arşivlenmesi kişi ve veri güvenliğinin getirdiği bir gereklilik olarak da görülebilir.

Masaüstü uygulamalarına verilen teknik ve güvenlik desteğinin mobil cihazlara sınırlı ölçüde verilebilmesi ve bu cihazların kişilerle birlikte her ortamda bulunabilmesinden dolayı kaybolma veya çalınma riskinin olması da mobil cihazların daha büyük bir risk taşıdığını göstermektedir.[123] Mobil cihazların bıraktığı izleri cihazın güvenli kullanımı, cihazda internet kullanımı ve e-mail kullanımı olmak üzere 3'e ayırabiliriz:[124]

Cihazın güvenli kullanılmamasından kaynaklanan izler, bu izlerin cihazın kaybolması veya çalınması durumunda oluşabilecek izleri kapsar. Cihazın kaybolması veya çalınması durumunda uzaktan imha etme kabiliyetinin (sistem dışı bırakma) cihazda bulunması verilere ve veri izlerine erişimin engellenmesi açısından önemlidir.

Cihazda e-mail kullanımından kaynaklanan izler; kurumsal bilgi ve belgelerin özel e-mail hesaplarında saklanması veya iletilmesi belgelere ilişkin izler bırakır. Kurumsal mail adresinden özel mail adresine hiçbir mailin yönlendirilmemesi de izler açısından önemlidir. Mail adreslerine fotoğraf yüklenilmesinin yapılmaması da ayrıca dikkat edilmesi gereken hususlardır. Çünkü basit bir fotoğraf yükleme işlemi sırasında bile gizli ve kötü amaçlı yazılımlar yüklenebilir.

---

[122] Yu-fen Jiang ve Ping Wang, "Study on Electronic Records Filing of Mobile Terminal," 4th International Conference on Social Science and Higher Education (ICSSHE 2018), **Advances in Social Science, Education and Humanities Research (ASSEHR)**, C. 181, (Çevrimiçi) https://download.atlantis-press.com/article/25903689.pdf, 25 Temmuz 2019.

[123] Türk Standartları Enstitüsü, **Bulut Bilişim Güvenlik ve Kullanım Standardı (Taslak)**, 2014, s.20, (Çevrimiçi) https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/1202/17032015093613-3.pdf, 21 Temmuz 2018.

[124] Protective Security Requirements, "Mobile and Remote Working," (Çevrimiçi) https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/mobile-and-remote-working/, 25 Temmuz 2019.

Cihazda internet kullanımından kaynaklanan izler; cihazdaki internet tarayıcısının kullanılmasıyla da oluşabilir. Bunun önüne geçebilmek için tarayıcının gizlilik modunda çalıştırılması tedbir olarak görülebilir. Bunun haricinde tarayıcının kullanıcı kimliği ve şifresini[125] kaydetmemesi için otomatik doldurma alanının kapatılması da bir diğer tedbir olarak düşünülebilir. Ayrıca kablosuz internet kullanılan alanlarda EBYS programına girişin yapılmaması da bırakılan izler açısından son derece önemlidir. Son olarak güncelliğini yitirmiş ve kullanım dışı olan cihazların içerik olarak temizlenmesi ve fiziksel olarak imha edilmesi cihaz içindeki bilgi ve izlerin yok edilmesi için zorunludur.

Önemli bir konu da hücresel veri sağlayan firmalardaki mobil bilgilerin saklama süreleridir. Eldeki bilgilerin de saklama planlarına göre imha edilmesi gereklidir. Hangi tür verilerin mevcut olduğunu, verilerin ne kadar süreyle erişilebilir olduğunu ve bu verilerin nasıl analiz edilip açıklanabileceğini bilme yeteneği verinin tamamen imhasında önemlidir. Örneğin ABD'deki 5 ana operatör sağlayıcının hangi bilgileri ne kadar süreyle sakladıkları bilgisi mevcuttur.[126] Türkiye'de mobil hizmetini sağlayan operatörlerin ellerindeki verileri nerede, nasıl ve saklama sürelerinin ne kadar olduğu tam olarak açıklanmalıdır. Kurumsal saklama planları varsa bu planlar sonunda veri ne şekilde imha edilmektedir?, İmha yöntemleri nelerdir? gibi soruların cevap bulması mobil izlerin hizmet sağlayıcı tarafındaki açıkları da ortaya koymaktadır.

3.3.9. Bulut İzleri

Bulut bilişim, "bilişim kaynaklarının ihtiyaç duyulan anda, ihtiyaç duyulduğu kadar kullanılması esasına dayanan, uygulamalar ile altyapının birbirinden bağımsız olduğu ve veriye izin verilen her yerden kontrollü erişimin mümkün olduğu, gerektiğinde kapasitenin hızlı bir şekilde arttırılıp azaltılabildiği, kaynakların kullanımının

[125] Kullanıcı kimlik ve şifre bilgileri yukarıda ifade edilen tedbirler yanında şifre oluşturulurken şifrenin en az 8 karakterli olmasına ve bu karakterlerin harf, sayı ve semboller (yalnızca ASCII standardı karakterleri) içeren herhangi bir kombinasyonu olmasına dikkat edilmelidir. Ayrıca, aksanlı karakterler desteklenmeyeceği unutulmamalıdır. Yine zayıf şifreler (Ör. "sifre123"), aynı hesapta daha önce kullanılan şifreler, boşlukla başlayan veya biten şifreler tercih edilmemelidir (Google, "Güçlü Bir Şifre ve Daha Güvenli Bir Hesap Oluşturma," (Çevrimiçi) https://support.google.com/accounts/answer/32040?hl=tr, 14 Kasım 2019).

[126] Patrick Siewert, "Cellular Provider Record Retention Periods," 2017, (Çevrimiçi) https://articles.forensicfocus.com/2017/04/18/cellular-provider-record-retention-periods/, 25 Temmuz 2019.

kolaylıkla kontrol altında tutulabildiği ve raporlanabildiği bir bilişim türüdür.”.[127] Bulutta verilen hizmetler üç farklı yapıda sunulur:[128]

- Yazılım Hizmeti (Software-as-a-Service, SAAS). İhtiyaç duyulan uygulamaların ve uygulamaların çalışmalarını sağlayacak kaynakların temin edildiği hizmet modelidir. Asıl hedefi yazılım geliştirme, bakım, yönetim ve donanım ücretlerinin düşürülmesidir. Güvenlik, büyük oranda hizmet sağlayıcısı tarafından sağlanır.
- Platform Hizmeti (Platform-as-a-Service, PAAS). Uygulamaların geliştirilip yayınlanması için ihtiyaç duyulan platformun temin edildiği modeldir. Temel amacı, gereken donanım ve yazılım bileşenlerinin satın alınma ve barındırma maliyetini düşürmektir. Bulut müşterisi yazılım ve yazılımın çalışacağı ortam üzerinde kontrole sahiptir. Güvenliğin “tanımlamaya bağlı olarak” bir bölümünden hizmet sağlayıcı, bir bölümünden ise müşteri sorumludur.
- Altyapı Hizmeti (Infrastructure-as-a-Service, IAAS). Uygulamaların geliştirilip çalıştırılması için ihtiyaç duyulan sunucu, yazılım ve ağ ekipmanlarından oluşan temel bilişim altyapısının sağlandığı modeldir. Amacı temel yazılım ve donanımı satın almaksızın, yerine bir hizmet arayüzü ile kontrol edebilmektir. Güvenlik, temel ekipmanlar dışında müşteri tarafından sağlanır.

Bulutun farklı hizmet yapıları yanında çeşitli dağıtım (yayımlama) modelleri de söz konusudur:[129]

- Özel bulut bilişim (Private Cloud), bulut altyapısı, birden çok birimden meydana gelen tek bir kuruluş tarafından özel kullanım için sağlanan hizmettir. Kurum içi veya kurum dışı yönetilebilir ve işletilebilir. “Özel buluta örnek olarak bir hastanenin bütün programlama alt yapısının IAAS’a dönüştürülmesi verilebilir”.[130]

---

[127] TSE, **Bulut Bilişim Güvenlik ve Kullanım Standardı (Taslak)**, s. 5.

[128] **A.g.s.**, s. 11-12.

[129] State Records of South Australia, **Cloud Computing and Records Management, Guideline Version 1**, 2015, s. 13, (Çevrimiçi) https://archives.sa.gov.au/sites/default/files/documentstore/policies-guidelines/Standard/20150706_cloud_computing_and_records_management_final_v1.pdf, 26 Temmuz 2019.

[130] Gamze Bayın, Gözde Yeşilaydın ve Okan Özkan, “Bulut Bilişimin Sağlık Hizmetlerinde Kullanımı,” **Sosyal Bilimler Dergisi**, S. 48, 2016, s. 236.

- Topluluk bulut bilişim (Community Cloud), bulut altyapısı belirli bir kullanıcı topluluğu olan ve görev, güvenlik gereksinimleri, politika ve uygunluk konularında ortak kaygılar taşıyan kuruluşların kullandığı bir modeldir. Ortamın yönetimi ve işletimi bir veya daha fazla kurum tarafından yapılabileceği gibi üçüncü bir taraf veya bunların kombinasyonundan da gerçekleştirilebilir. "Aynı coğrafi lokasyonda yer alan hastane sistemleri örnek olarak verilebilmektedir".[131]
- Genel bulut bilişim (Public Cloud), bulut altyapısı belirli bir kurumdaki veya kurumlardaki çalışanların kullanımı için açık olan ortamdır. Bir işletme, akademik kurum veya devlet kuruluşu veya bunların bir kombinasyonu tarafından sahiplenilebilir, yönetilebilir ve işletilebilir. Bu yöntemde altyapı ve bilişim araçları ortam sağlayıcı tarafından sunulur. "Microsoft, Oracle, Amazon, Google, GoGrid, Google Apps, Salesforce.com genel buluta ilişkin örneklendirilebilir."[132]
- Hibrid bulut bilişim (Hybrid Cloud), bulut altyapısı, benzersiz varlıklar olarak kalmaya devam eden, ancak veri ve uygulama taşınabilirliğini sağlayan standart veya tescilli teknoloji ile birbirine bağlı iki veya daha fazla ve farklı bulut altyapısının (özel, topluluk veya kamu) bir bileşimidir.
- Devlet bulut bilişim (Government Cloud),[133] kamu kurum ve kuruluşlarının tüm birimlerinde kullanılmak üzere bulut tabanlı bilgi teknolojileri için hazırlanmış çerçeve olarak açıklanabilir. Özellikle Birleşik Krallık'ta UK G-Cloud bir model olarak sunulmaktadır. İngiltere hükümetinin, kamu sektörünün önceden onaylanmış tedarikçilerden hizmet satın almalarına izin veren bulut çerçevesi olan UK G-Cloud'un, kamu sektöründe bilgi teknolojisinin dönüşümüne ve modernizasyonuna yardımcı olduğu ifade edilmektedir.[134]

---

[131] **A.g.m.**

[132] **A.y.**

[133] Patricia C. Franks, "Retention & Disposition of Records Residing in a Public Cloud: A Risk Management Approach," International Symposium October 17, (Presentation), 2014, (Çevrimiçi) https://interparestrust.org/assets/public/dissemination/IPT_20141017_InternationalSymposium2_Franks_RetentionDispositionInPublicCloud_Presentation.pdf, 7 Aralık 2017.

[134] Claire Edwards, "UK G-Cloud is A Model Other Countries Should Follow," 2018, (Çevrimiçi) https://www.pinsentmasons.com/out-law/analysis/uk-g-cloud-model-countries-should-follow, 24 Temmuz 2019.

Kurumlar bulut teknolojisini hangi modelini hangi amaçla kullanırsa kullansın belge yönetimi açısından dikkat etmeleri gereken hususlar vardır. Belgelerin değerinin korunması bu hususlara bağlıdır:[135]

- Belgelerin bütünlük, doğruluk ve güvenilirliklerini korumak,
- Belgelerin erişilebilir ve olmasını sağlamak,
- Yetkili olarak emniyetli bir şekilde belgelerin imha edilmesi veya kalıcı bir değere sahipse saklanmasını sağlamaktır.

Servis sağlayıcıların birden fazla yedekleme için belgeleri çoğaltması, bulundukları ülkelerin hukuki zorunlulukları gereği farklı sunuculara kopya göndermesi uygulaması yaygındır. Bu kurumların buluttaki belgelerinin saklama planları nedeniyle imha edilememesi ve zaman aşımına uğramış belgelerin bulundukları her sunucudan gerektiği gibi silinmediği anlamına gelebilir. Özellikle, kişisel veya hassas bilgiler içeren belgeler gibi, imha edilmesi gereken özel bir gereklilik olması durumunda ciddi bir risk teşkil eder.[136] Saklama planlarının ve imha süreçlerinin kolaylaştırılması ve uygulanması belge yönetim sistemlerinin temel gereğidir. Hatta sistemin denetim izlerini veya farklı metotlarla belgelerin tasfiyesini tamamlamaları gerekmektedir.[137]

Türkiye'de bulut bilişimle ilgili Türk Standartları Enstitüsü tarafından 2014 yılında hazırlanan *Bulut Bilişim Güvenlik ve Kullanım Standardı* taslağında veri temizleme yöntemlerinin verinin güvenliğiyle doğrudan ilişkili olduğu belirtilmiş ve NIST'in veri temizleme yöntemlerine yer verilmiştir. Taslakta

> "*Veri Temizleme (Sanitization):……. Temizleme işlemi, verinin üstüne yazılması, manyetik ortamının yok edilmesi, diğer yöntemlerle depolama ortamlarından silinmesi veya ortamın bilgi çıkarılamayacak şekilde imha edilmesi gibi yöntemlerle gerçekleştirilir. Bu işlem yedekleme ve geri yükleme sırasında ya da araçların sıfırlanıp yeniden kullanılması için kullanılabilir. Yaşanan olaylar göstermektedir ki ortamlar çalışmaz hale gelse bile çevrimiçi uygulamalar ve çeşitli araçlarla hassas veriler ele geçirilebilir. Veri temizlemesine yönelik hususlara hizmet sözleşmelerinde yer verilmesi, bu hususta yaşanabilecek muhtemel sorunların önüne geçecektir*."[138]

[135] State Records of South Australia, **Cloud Computing…**, s. 4.
[136] **A.g.r.**, s. 8.
[137] ISO, **15489-1 2001**, s. 10; Akt: Franks, "Retention & Disposition of Records".
[138] TSE, **Bulut Bilişim Güvenlik ve Kullanım Standardı (Taslak)**, s. 22.

şeklinde silme yöntemlerinin belirtilmesi yanı sıra, ortamdan bilgi çıkarılmayacak şekilde imha edilmesine de dikkat çekilmiştir. Yukarıda sıralanan bulut bilişim dağıtım modellerinin seçiminde standartta da ifade edildiği gibi hizmet sözleşmelerinde verinin imhasına yönelik hususlar açık bir şekilde gösterilmelidir. Ayrıca her ne kadar silinmiş olsa da verinin güvenliği söz konusu olduğunda silinmiş verinin de veri güvenliği kapsamında ele alınmasının bilinmesi zorunludur.

3.3.10. Elektronik (Dijital) İmza İzleri

Elektronik imza, işlevsel olarak el yazısı ile atılan imzayla eşdeğerdir. "Elektronik imza" terimi, bir sözleşmeyi veya başka bir belgeye bağlı olan veya mantıksal olarak ilişkili ve belgeye imza atmaya niyetli bir kişi tarafından yürütülen veya kabul edilen elektronik bir ses, sembol veya işlem anlamına gelir.[139] Diğer bir tanıma göre de "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi"[140] ifade etmektedir.

Elektronik imzanın sistem prensibinde elektronik imzalayıcılar, elle atılan imza gibi ünik bir şifreleme anahtarına sahiptirler. Elektronik imza sağlayıcıları, PKI (Public Key Infrastructure, Açık Anahtar Altyapısı) gibi özel bir protokol kullanırlar. PKI, anahtar denilen iki uzun sayı üretmek için matematiksel bir algoritma kullanmasını gerektirir. Bu iki anahtardan biri açık, diğeri ise özeldir. İmza yetkilisi, elektronik olarak bir belgeyi imzaladığında, oluşturulan imza imzalayan tarafından her zaman güvenli bir şekilde tutulan özel anahtar kullanılarak oluşturulur. Matematiksel algoritma bir şifre gibi davranır, imzalı belgede hash (özet) olarak adlandırılan verileri eşleştirir ve bu verileri şifreler. Sonuç olarak elektronik imza şifrelenen bu veridir. Elektronik imza, belgenin imzalandığı zamanla da işaretlenir. Belge imzaladıktan sonra herhangi bir değişikliğe uğramışsa, elektronik imza geçersiz olur. Bu çalışma prensibini gösteren şekil aşağıda verilmiştir.[141]

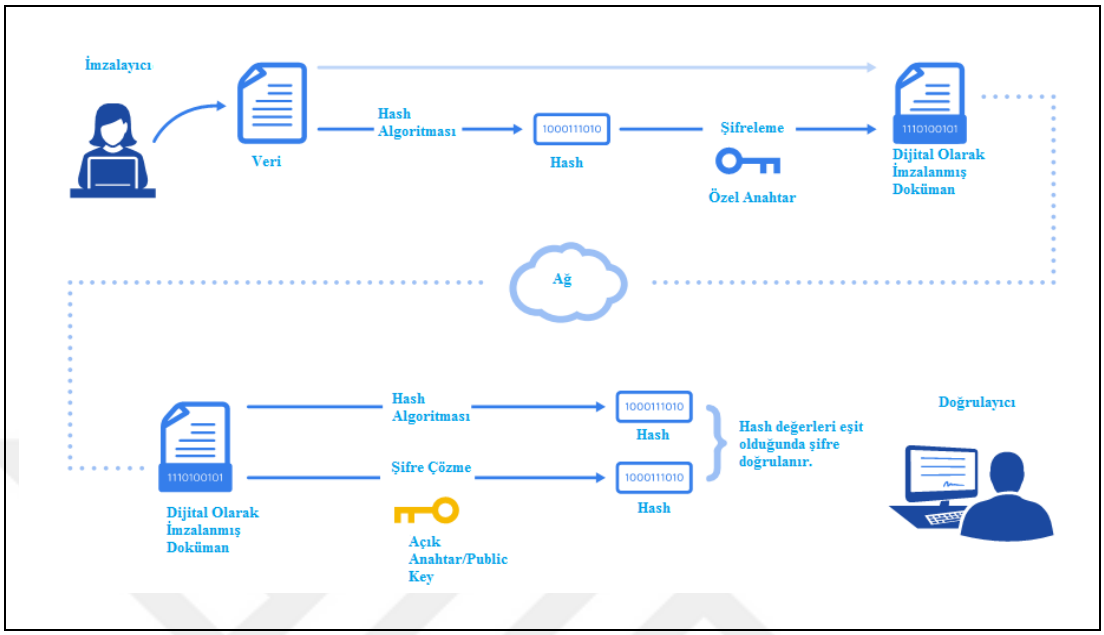
---

[139] U.S. Department of Transportation, Federal Aviation Administration, **Electronic Signatures, Electronic Recordkeeping, and Electronic Manuals- Advisory Circular,** 2016, s. 4, (Çevrimiçi) https://www.faa.gov/documentlibrary/media/advisory_circular/ac_120-78a.pdf, 25 Temmuz 2019.

[140] "5070 sayılı Elektronik İmza Kanunu"

[141] DocuSign, "What are digital signatures?," (Çevrimiçi) https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq, 22 Kasım 2019.

Şekil 3.16: Elektronik İmza Süreci



(**Kaynak:** DocuSign, "What are digital signatures?," (Çevrimiçi) https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq, 22 Kasım 2019; Yazar tarafından Türkçe olarak yeniden hazırlanmıştır.)

Elektronik imzanın belgenin doğruluğu ve bütünlüğü üzerinde eşsiz (unique/ünik) bir benzerliği vardır. Bu benzerlik belgenin orijinalliğini yansıtır. Elektronik imzanın sisteme tanımlanması bazı yazılım ve donanım bileşenlerinin de bulunmasını gerektirir. Özellikle yazılımlar, istemci ve sunucu arasındaki iletişimi sağlar. Ayrıca bu yazılımlar işletim sisteminde ve web tarayıcılarla beraber çalışır.[142] Bu yazılımların barındırdıkları bilgiler, belge izlerini burada da göz önünde bulundurulmasını gerektirmektedir. İmha sürecinde bilgi ve belgenin buralardan da silinmesi gerekir.

Elektronik imza işlemiyle bağlantılı olarak toplanan belirli bilgiler arasında kişisel bilgiler de olabilir. Bu bilgiler, arka plan verilerinin kopyaları, yani kâğıt izi, denetleme ve arşivleme bilgilerinin yanı sıra anlaşmaların farklı coğrafik bölgelerde eri-

[142] Martin Harran v.d., "A Method for Verifying Integrity & Authenticating Digital Media," **Applied Computing and Informatics**, 2017, S. 14, s. 147, DOI: 10.1016/j.aci.2017.05.006.

şimi mümkün olabilir. Çünkü yazılımların çoğu, kullanıcıların elektronik ortamda yerel olarak imzalanan belgeleri yerel olarak kaydetmelerine izin verir. Ayrıca, bir bulut depolama alanı kullanılıyorsa, bu riski ortadan kaldırmak için bulut sağlayıcıyla ikili anlaşmaların olması da bu açıdan gereklidir.[143] Özetle kişisel bilgiler belgeler için iz anlamı taşımaktadır. Bu izlerden belgelere erişimin en aza indirilmesi alınacak tedbirlere bağlıdır.

Tedbirler arasında özet (hash) güvenliğinin nasıl sağlandığı önemlidir. Oluşturulan bir özet sadece bir doküman için geçerlidir veya her bir dokümanın sadece bir özeti vardır. Ancak iki farklı doküman aynı doküman özetine sahipse (yani bir çarpışma söz konusu ise), o zaman bir dokümanın elektronik imzası diğer doküman için elektronik imza olarak kullanılabilir. Bu durumda, doğrulanmış bir elektronik imza, imzalanan dokümanın doğruluğunu garanti etmez, çünkü iki dokümandan birinin geçerli olduğu düşünülebilir. Bu nedenle, elektronik imzalar için kullanılan bir karma işlevi, çarpışma direnci gerektirir. Çarpışma direncinin artırılması kullanılan SHA (Secure Hash Algorithm)'ların yüksek bitli olması zorunlu olmalıdır. SHA'lar arasında SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 bulunmaktadır.[144]

3.3.11. Taşınma, Dönüşüm ve Transfer (Belge Devri) İzleri

Elektronik ortamdaki nesneler, birbirleriyle etkileşimle kullanılabilirler. Bu nesnelerin etkileşimleri teknolojik bileşenlere bağlıdır. Söz konusu teknolojik bileşenler, bit, bayt, karakter kodlama, komut seti mimarisi, baytların fiziksel organizasyonu, parçaların mantıksal organizasyonu, donanımın okunması, giriş/çıkış donanımı, giriş/çıkış yazılımı, çekirdek işletim sistemi, ağ işletim sistemi, ağ protokolleri, farklı istemci

[143] Hayden Delaney ve Briar Francis, "Electronic Signatures and Their Legal Validity in Australia," (Çevrimiçi) https://www.findlaw.com.au/articles/5777/electronic-signatures-and-their-legal-validity-in-.aspx, 27 Temmuz 2019.

[144] **NIST Special Publication 800-107**, Recommendation for Applications Using Approved Hash Algorithms, 2012, s. 8-10, (Çevrimiçi) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf, 22 Kasım 2019.

ortamları, veri söz dizimi, veri yapısı, veri semantiği, veri içeriği, veri değeri, nesnelerin içindeki ve aralarındaki bağlamsal ilişki olarak ifade edilebilir.[145] Bu bileşenlerin taşınması, dönüşümü ve transferi belge izleri açısından önemlidir.

Belgelerin taşınması (migration of records), sistem eskimesinden dolayı belgelerin fiziksel ve entelektüel biçimlerini koruyarak, erişilebilirliklerinin devam etmesini sağlamak için bir sistemden diğerine aktarma işlemi olarak tanımlanmaktadır.[146] Dönüşüm (emulation), eski yazılım veya sistemlerin gelecekteki bilgisayarlarda yürütülmesine izin vermek için yeni donanım ve yazılımın geliştirilmesi yoluyla eski yazılım veya sistemlerin davranışlarının ve sonuçlarının çoğaltılmasıdır.[147] Transfer (belge devri) ise, belgelerin ikincil bir depoya veya arşive taşındığı elden çıkarma işlemidir. Bu nedenle, transfer elden çıkarılan belgelerin eski sistemlerde kalmayacak şekilde imhasını içerir. Transfer taşınma olarak da ifade edilir.[148] Transfer bir diğer tanıma göre ise, "elektronik belgenin, üretildiği kurumdaki saklama süresinin bitiminde başka bir kuruma transfer edileceğini gösterir"[149] şeklinde açıklanmıştır.

Belgelerin taşınması, fiziksel medyanın eskime sorunlarını çözer, dijital belgelerin işlevselliğini korur ve kullanıcıların belgelere tekrar erişmelerini sağlar. Ayrıca, orijinal veri formatının bazı özellikleri geçiş sürecinde korunamayabilir ve bunun sonucunda kullanıcılar, önceki belgelerin tüm özelliklerine erişim sağlayamaz.[150] Belgelerin dönüşümünde yazılımın maliyetli olması ve yüksek yetenekli bilgisayar programcılarının gerekli kodu yazmasının gerekliliği karşılaşılan güçlüklerdir.[151] Dönüşümde yazılım ve donanım değişirken bilgiler orijinal dosya formatında saklanır.[152] Belge devrinde (transfer), belgelerin yaşam döngüleri boyunca, dosyaları ve üstverileri, etkinlikleri azaldıkça ve/veya kullanımları değiştikçe, bir depolama ortamından

[145] Cal Lee, "Emulation, Migration and Long-Term Preservation of Electronic Records," (Çevrimiçi) https://www.asu.edu/ecure/2001/ppt/lee.ppt, 22 Kasım 2019.
[146] The InterPARES 2 Project: Glossary, "Migration of Records," 2019.
[147] **A.g.s.**
[148] DLM Forum Foundation, **MoReq2010**, s. 237.
[149] TSE, **TS 13298:2015**, s. 10.
[150] The United Methodist Church, General Commission on Archives and History, **Guidelines for Managing Electronic Records 2013-2016**, s. 21, (Çevrimiçi) https://www.ctcumc.org/files/fileshare/digital+records+-+gcah.pdf, 1 Ağustos 2019.
[151] **A.g.r.**, s. 21.
[152] New York State Archives, **Preservation of Electronic Records Workbook**, 2011, (Çevrimiçi) http://www.archives.nysed.gov/common/archives/files/workshops_handouts_erecords_preservation.pdf, 1 Ağustos 2019.

veya konumundan diğerine aktarılabilir. Bu aktarım yerel olarak ya ara depoya (near-line), ya çevrimdışı olan bir yere (örneğin bir yerel veya uzak depolama alanına) veya başka bir belge havuzuna veya ulusal arşive devri gerçekleşebilir.[153]

Belgelerin taşınması, dönüşmesi veya transferinde dikkat edilmesi gereken husus belgelerin ilk konumlandıkları yerlerde imhadan sonra iz bırakılmamasıdır. Yukarıda başlıklar halinde anlatılan izlerin bulundukları yazılım ve donanımların tamamının imha sürecinden geçirilmesi gerekir. Bu süreç duruma göre şekillenir. Belgelerin bir sistemden tamamen taşınması bir zorunluluk ve ortam eskimesinden dolayı ise verilerin üzerine yazma dâhil olmak üzere fiziksel imhası da gereklidir. Belgelerin dönüşümünde de aynı süreç geçerlidir. Belgelerin devrinde ise ilk konumlandıkları yer başka belgeler için kullanılacaksa, ortamın üzerine yazma işlemi ardından de-manyetize edilmesi gerekir.

Dikkat edilmesi gereken bir diğer husus da belgelerin kendi kendine değişmesidir (self-modifying). Bu özellikteki belgelerin takibi taşınma, dönüşüm ve transfer sonrası üstverilerden yapılabilmelidir.[154] Bunlara dikkat edilmemesi imha edilmesi gereken bir belgenin imha edilmemesi veya imha edilmemesi gereken bir belgenin imha edilmesine yol açabilir. Bu durumda imha edilmesi gereken belge kendi kendine değişiklik göstererek varlığına ilişkin iz bırakmış olur.

Bunun için de belge ve belge yönetimi arasındaki üstveri bağlantıları tutulur. Belgeye ilişkin üst ve alt hiyerarşi bağlantıları da tutulur.[155] Böylelikle bir elektronik belgeye ilişkin tüm bileşenler tek bir ünitede tek bir işlemde imhası gerçekleşmiş olur.[156]

[153] European Communities, **MoReq2001**, s. 27.
[154] **MoReq2001**, s. 44.
[155] International Council on Archives (ICA), **Principles and Functional Requirements for Records in Electronic Office Environments – Module 2: Guidelines and Functional Requirements for Electronic Records Management Systems**, 2008, s. 45.
[156] **MoReq2001**, s. 42

DÖRDÜNCÜ BÖLÜM

DÜNYADA VE TÜRKİYE'DE ELEKTRONİK BELGE İMHA POLİTİKALARI, TEORİLERİ VE UYGULAMALARI

4.1. ELEKTRONİK BELGE İMHASINA YÖNELİK ULUSLARARASI DÜZENLEMELER

Elektronik ortamdaki verinin imhasıyla ilgili geliştirilen uluslararası birçok düzenleme vardır. Bunları ülkeler bağlamında sınıflandırabiliriz. Söz konusu tüm ülkeler alfabetik olarak Almanya, Amerika Birleşik Devletleri, Avustralya, İngiltere, Kanada, Rusya ve Yeni Zelanda'dır.[1] Bu ülkelerin çoğunda (özellikle askeri kurumların kendine has olmak üzere) birden fazla imha standardı görülmektedir. Aşağıda ilk önce ülkelerin geliştirdikleri standartların özeti verilmiş ardından ayrıntılı olarak alt başlıklar şeklinde açıklanması yoluna gidilmiştir.

Almanya imha standartları:

- Federal Ofis Bilgi Tekniği Güvenliği Standardı (Standard vom Bundesamt für Sicherheit in der Informationstechnik, BSI-VSITR))
- Pfitzner Yöntemi (Pfitzner-Methode)

Amerika Birleşik Devletleri (ABD) imha standartları:

- ABD Ordusu Standardı (U.S. Army AR380-19)
- ABD Savunma Bakanlığı Standardı (Standard of the American Department of Defense, DoD 5220.22 M ve diğer versiyonları)
- ABD Hava Kuvvetleri Sistem Güvenliği (U.S. Air Force System Security Instructions, AFSSI-5020)
- ABD Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology, NIST 800-88)

[1] DGD Deutsche Gesellschaft für Datenschutz GmbH, "Erasure Standards," (Çevrimiçi) https://dg-datenschutz.de/services/data-erasure/data-erasure-standards/royal-canadian-mounted-police-tssit-ops-ii/?lang=en, 29 Mart 2019.

- ABD Donanma Personeli Dokümanı (Navy Staff Office Publication, NAVSO P-5239-26)
- ABD Ulusal Bilgisayar Güvenliği Merkezi Standardı (National Computer Security Center, NCSC-TG-025 Standard)
- Bruce Schneier Algoritması (Bruce Schneier Algorithm)

Avustralya imha standartları:

- Avustralya Bilgi Güvenliği Standartları El Kitabı (Australian Information Security Manual Standard, ISM 6.2.92)
- Peter Gutmann Algoritması (Peter Gutmann Algorithm)

İngiltere imha standartları:

- İngiltere Hükümeti Ulusal Teknik Otoritesi Bilgi Güvencesi Standardı (The UK government's National Technical Authority for Information Assurance Standard, CESG CPA – Higher Level)[2]
- İngiliz HMG Infosec Standardı (British HMG Infosec Standard 5)

Kanada imha standartları:

- Kanada Kraliyet Atlı Polisleri Standardı (Royal Canadian Mounted Police, TSSIT OPS-II)
- Kanada İletişim Güvenliği Kurumu Standardı (Communication Security Establishment Canada Standard, CSEC ITSG-06)

Rusya Federasyonu imha standartları:

- Rus Devlet Standardı (Russian State Standard, GOST R 50739-95 (russ. ГОСТ Р 50739-95))

Yeni Zelanda imha standartları:

- Yeni Zelanda Bilgi ve İletişim Teknolojileri Standardı (New Zealand Information and Communications Technology Standard, NZSIT 402)

[2] Katie Moss Jefcoat, "A Comprehensive List of Data Wiping and Erasure Standards, CESG CPA – Higher Level," 2017, (Çevrimiçi) https://www.blancco.com/blog-comprehensive-list-data-wiping-erasure-standards/, 24 Şubat 2019.

4.1.1. Almanya İmha Standartları

Almanya'nın yaygın olarak bilinen iki imha standardı bulunmaktadır. Bunlar; BSI VSITR ve Pfitzner Yöntemi'dir. Yöntemlerin özelliklerine ilişkin bilgiler aşağıda verilmiştir.[3]

4.1.1.1. Federal Ofis Bilgi Tekniği Güvenliği Standardı (Standard des Bundesamts für Sicherheit in der Informationstechnik, BSI-VSITR)

BSI-VSITR, Alman Bilgi Teknikleri Güvenliği Federal Ofisi (BSI)'nin -bazı veri imha programları tarafından da kullanılan- veri ortamının güvenli bir şekilde silinmesi için kendi oluşturmuş olduğu resmi bir standarttır. VSITR standardı kullanılarak, bir sabit diskteki veya başka bir depolama ortamındaki mevcut bilgilerin üzerine 7 kez yazılmak suretiyle veri imha edilir. Güvenli veri silme yazılımı tabanlı bir yöntem olarak bilinmektedir. VSITR yöntemi veri silme işlemini aşağıdaki yedi adımda gerçekleştirmektedir:

Adım 1: Verilerin üzerine 0 (sıfır) ile yazma;
Adım 2: Verilerin üzerine 1 (bir) ile yazma;
Adım 3: Verilerin üzerine 0 (sıfır) ile yazma;
Adım 4: Verilerin üzerine 1 (bir) ile yazma;
Adım 5: Verilerin üzerine 0 (sıfır) ile yazma;
Adım 6: Verilerin üzerine 1 (bir) ile yazma; ve
Adım 7: Verilerin üzerine rastsal bir karakter ile yazma.

VSITR veri silme yöntemi, Kanada Kraliyet Atlı Polisleri Standardı (TSSIT OPS-II) veri silme yöntemiyle aynıdır, ancak VSITR'da daha sonra doğrulama için bir kontrol yapma özelliği yoktur. Federal Bilgi Güvenliği için VSITR yöntemi, bir sabit diskte depolanan verilere uygulanırsa, verilerin yazılım tabanlı veya donanım tabanlı kurtarılması imkânsız görülmektedir.

4.1.1.2. Pfitzner Yöntemi (Pfitzner Method)

Bu veri silme yönteminin orijinali Roy Pfitzner tarafından öne sürülmüştür. Bazı veri silme programları, bir sabit diskteki veya başka bir depolama ortamındaki mevcut bilgilerin üzerine yazmak için Pfitzner yöntemini kullanır. Pfitzner yöntemi yazılım

[3] DGD Deutsche Gesellschaft für Datenschutz GmbH, "Erasure Standards,"

tabanlı bir veri silme standardıdır. Bu veri silme yöntemi genellikle aşağıdaki şekilde uygulanır:

Adım 1'den adım 33'e kadar: Verilerin üzerine rastsal bir karakter ile üzerine yazma işlemi yoluyla gerçekleştirilir. Pfitzner metodu ile bir veri depolama ortamının silinmesi, tüm yazılım ve donanım tabanlı restorasyon metotlarını işlevsiz kılması açısından önemlidir.

4.1.2. Amerika Birleşik Devletleri İmha Standartları

Amerika Birleşik Devletleri (ABD), dünyada en fazla imha standardına sahip ülke konumundadır. ABD'nin bilinen yedi imha standardı bulunmaktadır. Bu yedi standardın özellikleri yukarıda sıralandığı şekliyle verilmiştir.[4]

4.1.2.1.ABD Ordusu Standardı (U.S. Army AR380-19)

ABD Ordusu (AR 380-19) tarafından kullanılan veri silme işlemi tipik olarak veri silme yazılımı ile aşağıdaki şekilde gerçekleştirilir:

Adım 1: Verilerin üzerine rastsal bir karakterle üzerine yazma;

Adım 2: Verilerin üzerine tanımlanmış bir karakter (örneğin 0 veya 1 gibi) ile üzerine yazma;

Adım 3: Verilerin üzerine daha önce yapılan rastsal karakterin tersine bir karakterle yazma ve bu karakterin doğrulanması.

Bu yöntem kullanılarak bir veri silme işlemi gerçekleştirildikten sonra, verinin yazılım veya donanım tabanlı bir restorasyonu geçersiz kılınır. Bu veri silme prosedürü ABD Ordusu tarafından "380-19. Ordu Yönetmeliği" belgesinde yayınlanmıştır. Birleşik Devletler Ordusunun bu standardı güncel olarak kullanıp kullanmadığı bilinmemektedir. Ancak, en azından güvenli bir veri silme işlemi gerçekleştirmek için kullanılabilecek programların bir parçası olması açısından önemlidir.

[4] DGD Deutsche Gesellschaft für Datenschutz GmbH, "Erasure Standards,"

4.1.2.2. ABD Savunma Bakanlığı Standardı (Standard of the American Department of Defense, DoD 5220.22 M ve diğer versiyonları)

Amerikan Savunma Bakanlığı standardı (DoD 5220. 22-M), iyi bilinen birkaç program(Darik's Boot And Nuke, Eraser, Disk Wipe) tarafından güvenli veri silme amacıyla kullanılır. Verilerin üzerine 3 kez yazılmasını önerir. DoD 5220. 22-M veri silme prosedürü şu şekilde gerçekleşir:

Adım 1: Verinin üzerine 0 (sıfır) ile yazmak ve bu karakterin doğruluğunu kontrol etmek;

Adım 2: Verinin üzerine 1 (bir) ile yazmak ve bu karakterin doğruluğunu kontrol etmek;

Adım 3: Rastsal bir karakter ile verinin üzerine yazmak ve bu karakterin doğruluğunu kontrol etmek.

DoD 5220. 22-M'e ait bu yöntem güvenli silme için yaygın olarak kabul görmektedir. DoD standardı ile silinen verilerin yazılım veya donanım tabanlı restorasyonu genellikle hariç tutulur. DoD 5220. 22-M silme standardı, ABD Ulusal Endüstriyel Güvenlik Programı (NISP) tarafından yayınlanmıştır. En sık kullanılan veri silme yöntemlerinden biridir.

NISP tarafından tanımlanan DOD 5220.22-M, ayrıca DOD 5220.2-M olarak da adlandırılır. Savunma Güvenliği Servisi (Defense Security Service, DSS) tarafından güvenli veri temizliği için bir çözüm olarak geliştirilmiştir. Aynı zamanda, 3 doğrulama işleminde ve 7 doğrulama işleminde uygulanan çeşitli doğrulama sıklıklarında uygulanan veri temizliği için kullanılan en gelişmiş, güvenli ve yaygın silme standartlarından biridir.[5] Aşağıda DoD 5220.2-M'nin yaygın olarak kullanılan birkaç versiyonu verilmiştir:[6]

DoD 5220.22-M (ECE) – Veriler üzerine 7 kez yazma kabiliyetine sahiptir.

DoD 5220.22-M (E) - Verilerin üzerine 3 kez yazma kabiliyetine sahiptir.

[5] Stellar Data Recovery Inc., "7 Effective Algorithms to Remove Files and Folders Permanently," 2018, (Çevrimiçi) https://www.stellarinfo.com/article/7-algorithms-to-wipe-files-folders-permanently.php, 23 Şubat 2019.

[6] Stellar Data Recovery Inc., "7 Effective Algorithms to Remove Files and Folders Permanently,"

DoD 5220.28-M -STD - Verilerin üzerine 7 kez yazma kabiliyetine sahiptir.

Bu versiyonlar arasındaki fark, her birinin farklı doğrulama frekanslarında ve geçiş sayısında bir karakter ve karakter doğrulaması kullanmasıdır.

3 kez üzerine yazmada

Adım 1: Verilerin üzerine 0 (sıfır) ile yazar ve bunu doğrular.

Adım 2: Verilerin üzerine 1 (bir) ile yazar (ilk çalıştırma değerinin tamamlayıcısı) ve onaylar.

Adım 3: Sahte değerlerle veriler üzerine yazar ve bunu doğrular.

Şekil 4.1: DoD 5220.22-M (E) :Verilerin Üzerine 3 Kez Yazma Kabiliyeti

(**Kaynak:** Data Destroyers, "Data Carrier Sanitization," (Çevrimiçi) https://www.datadestroyers.eu/technology/data_carrier_sanitize.html, 31 Temmuz 2019.)

7 kez üzerine yazmada

Adım 1-3: DoD 5220.22-M (E) ile verilerin üzerine yazma,

Adım 4: Üzerine sahte rastsal değerlerle üzerine yazma ve

Adım 5: DoD 5220.22-M (E) standart değerlerle verilerin üzerine yazma.

4.1.2.3. Amerika Birleşik Devletleri (ABD) Hava Kuvvetleri Sistem Güvenliği (U.S. Air Force System Security Instructions, AFSSI-5020)

ABD Hava Kuvvetlerinin silme standardı ilk olarak Hava Kuvvetleri Sistem Güvenlik Talimatları AFSSI-5020 altında yayınlanmıştır. Bir sabit sürücü veya başka bir depolama ortamında var olan bilgilerin üzerine yazmak için yazılım tabanlı veri imhası

kullanan sayısız program tarafından yaygın olarak kullanılır. AFSSI-5020 veri silme işlemi aşağıdaki şekilde yapılır:

Adım 1: Verilerin üzerine 0 (sıfır) ile yazma;

Adım 2: Verilerin üzerine 1 (bir) ile yazma; ve

Adım 3: Verinin üzerine rastsal bir karakter ile yazma ve bu karakterin doğruluğunu kontrol etme.

Bir veri saklama ortamı AFSSI-5020 veri silme yöntemiyle silindikten sonra, yazılım tabanlı dosya restorasyonu genellikle hariç tutulur. Ayrıca, bu silme standardının kullanılması, donanım tabanlı bir restorasyonun veya verilerin çıkarılmasını önler.

4.1.2.4. ABD Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology, NIST 800-88)

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından, Eylül 2006'da Amerikan Federal Bilgi Güvenliği Yönetimi Yasası (FISMA) tarafından tanımlanan görevleri yerine getirmek için bir kılavuz yayımlandı. NIST, yeterli bilgi güvenliği için minimum gereklilikleri tanımlamak da dâhil olmak üzere, ABD'deki standartların ve kılavuzların geliştirilmesinden sorumludur.

NIST 800-88'e göre kendi kullanımlarıyla "veri temizleme" işlemi üç aşamada gerçekleşir. Bunlar; boşaltma (clear), temizleme (purge) ve imhadır (destroy). Bunlardan birine karar vermek için verinin sınıflandırılması, kaydedildiği ortamın niteliğinin değerlendirilmesi, gizlilik riskinin düşünülmesi ve ortam için gelecek planlarının belirlenmesinin gerektiği ifade edilmektedir. Seçilen yöntem maliyet, çevresel etki, vb. şartlar şeklinde değerlendirilmelidir. Ayrıca, silinecek verilerin yetkisiz bir şekilde ifşa edilmesi riskini en iyi şekilde azaltan bir kararın verilmiş olması esastır.[7] Söz konusu 3 aşamanın içinde farklı teknikler uygulanabilmektedir. Örneğin boşaltma ve temizleme aşamalarında üzerine yazma işlemi kullanılabilir. Ayrıca temizleme aşamasında

[7] U.S. Department of Commerce, National Institute of Standards and Technology (NIST), **NIST Special Publication 800-88 (Revision 1): Guidelines for Media Sanitization**, Haz. Richard Kissel v.d., Gaithersburg, 2014, s. 24, (Çevrimiçi) http://dx.doi.org/10.6028/NIST.SP.800-88r1, 23 Mart 2018.

etkisizleştirme (degaussing) tekniği de kullanılabilir. Boşaltma ve temizleme aşamaları genellikle verinin fiziksel imhasını içermezken imha aşamasında fiziksel imhadan da söz edilir.

4.1.2.5. ABD Donanma Personeli Dokümanı (Navy Staff Office Publication, NAVSO P-5239-26)

NAVOS 5239-26 veri silme prosedürü aşağıdaki şekilde çalışır:

Adım 1: Tanımlanmış bir karaktere sahip veriler ile üzerine yazma (örneğin 1);

Adım 2: Tanımlanan karakterin zıttı olan veriler ile üzerine yazma (örneğin, 0);

Adım 3: Verinin üzerine rastsal bir karakter ile üzerine yazmak ve bu karakterin doğruluğunu kontrol etmek.

NAVSO P-5239-26 veri silme standardı, sayısız veri imha çözümünde uygulanan standartların bir parçasıdır. Bir sabit disk NAVSO 5239-26 veri silme yöntemiyle silindikten sonra, yazılım tabanlı bir dosya ile geri yüklemesi genellikle mümkün değildir. Donanım tabanlı restorasyon yöntemleri de genellikle verileri kurtarmaz. NAVSO 5239-26 veri silme prosedürü başlangıçta 5239-26 Donanma Personel Ofisi yayın modülünde tanımlanmıştır. Standart ABD Donanmasının silme yöntemi olarak halen kullanılmaktadır.

4.1.2.6. ABD Ulusal Bilgisayar Güvenliği Merkezi Standardı (National Computer Security Center, NCSC-TG-025 Standard)

Ulusal Bilgisayar Güvenlik Merkezi'nin standardı olan NCSC-TG-025, verinin imhasında yaygın olarak kullanılmaktadır. NCSC-TG-025 prosedürü orijinal olarak ABD Ulusal Güvenlik Ajansının (NSA) bir parçası olan Ulusal Bilgisayar Güvenlik Merkezi (NCSC) tarafından Forest Green Book adlı kitapta yayınlanmış ve tanımlanmıştır. Bu yöntem, bir veri ortamında mevcut bilgilerin yazılım tabanlı üç kez üzerine yazılmasına esasına dayanır. NCSC-TG-025'in teknik işlevi aşağıdaki gibidir:

Adım 1: Verinin üzerine 0 (sıfır) ile yazmak ve bu karakterin yazısını doğrulamak;

Adım 2: Verinin üzerine 1 (bir) ile yazmak ve bu karakterin yazısının doğrulamak;

Adım 3: Verinin üzerine rastsal bir karakter ile yazmak ve bu karakterin yazısını doğrulamak.

NCSC-TG-025 silme yöntemi, DoD 5220.22-M ile eş değerdir. Bir sabit diskin NCSC-TG-025 metodu yardımıyla silinmesinden sonra, verilerin yazılım tabanlı restorasyonu genellikle mümkün değildir. Verilerin donanım tabanlı yöntemlerle çıkarılması büyük ölçüde hariç tutulmuştur.

4.1.2.7. Bruce Schneier Algoritması (Bruce Schneier Algorithm)

Algoritmayı geliştiren Bruce Schneier, algoritmayı "Applied Cryptography: Protocols, Algorithms ve Source Code in C" kitabında yayınlamıştır. Bruce Schneier algoritması çok sayıda veri imha programı tarafından kullanılmaktadır. Yazılım, temelinde bir sabit diskte veya başka bir depolama ortamında mevcut verilerin üzerine 7 kez yazılmayı sağlar. Bu algoritma yardımıyla, ilk önce ikili sıfırlarla (00) ve daha sonra ikili birlerle (11) bir sabit diskin üzerine yazılır. Geri kalan beş adımda, verilerin üzerine yazmak için rastsal oluşturulmuş bir bit deseni kullanılır.

Adım 1: Verilerin üzerine 0 (sıfır) ile yazma;

Adım 2: Verilerin üzerine 1 (bir) ile yazma;

Adım 3: Verilerin üzerine rastsal bir karakter ile yazma;

Adım 4: Verilerin üzerine rastsal bir karakter yazma;

Adım 5: Verilerin üzerine rastsal bir karakter ile yazma;

Adım 6: Verilerin üzerine rastsal bir karakter ile yazma;

Adım 7: Verilerin üzerine rastsal bir karakter ile yazma.

Bruce Schneier'in veri silme yönteminin yardımıyla bir veri taşıyıcısını sildikten sonra, yazılım tabanlı dosya kurtarma işlemi genellikle mümkün değildir. Verilerin donanım tabanlı çıkarılması da çoğu durumda başarısız olur.

4.1.3. Avustralya İmha Standartları

Avustralya'da bilinen iki farklı imha standardı bulunmaktadır. Bunlar; ISM 6.2.92 ve Peter Gutmann Algoritmasıdır. Her iki yöntemin teknik özellikleri aşağıda verilmiştir.[8]

4.1.3.1. Avustralya Bilgi Güvenliği Standartları El Kitabı (Australian Information Security Manual Standard, ISM 6.2.92)

Bu veri silme işlemi, yazılımı tarafından aşağıdaki şekilde belirtildiği gibi tek bir adımda gerçekleştirilir:

Adım 1: Verinin üzerine rastsal bir karakterin üzerine yazmak ve bu karakterin yazısını doğrulamak.

ISM 6.2.92, genellikle güvenli bir veri silme işlemi yapan programlarca kullanılır. Standart, bir sabit diskte veya başka bir depolama ortamında mevcut bilgilerin üzerine bir kez yazma işlevi görür. Avustralya hükümeti tarafından yayınlanan, yazılım tabanlı bir veri silme yöntemidir. Bir sabit diskin ISM 6.2.92 veri silme yöntemiyle silinmesinden sonra, genellikle veri kurtarma işlemi başarısız olur. Yönteminin asıl kaynağı, Avustralya Savunma Bakanlığı Bilgi Güvenliği El Kitabında (ISM) yapılmıştır.

4.1.3.2. Avustralya Peter Gutmann Algoritması (Peter Gutmann Algorithm)

Peter Gutmann'ın silme yöntemi kullanıldığında, bir veri taşıyıcıdaki verilerin tanımlanmış değerlerle 35 kez üzerine yazılabilir. Bu silme yöntemi son derece zaman alıcıdır, ancak yine de herhangi bir riske girmeden veri silme için çok güvenli bir yöntem olduğu düşünülmektedir. Gutmann metodu sayısız yazılım çözümünde kullanılır. Bu tür veri imha programları, bir sabit diskteki veya başka bir depolama ortamındaki mevcut verilerin üzerine yazmak için Gutmann algoritmasını kullanır. Gutmann'ın verilerin üzerine 35 kez yazma işlemini hangi verilerle yaptığı aşağıdaki tabloda verilmiştir.

Tablo 4.1: Peter Gutmann Algoritması

Veri Üzerine Yazma

[8] DGD Deutsche Gesellschaft für Datenschutz GmbH, "Erasure Standards,"

Adım No. (Tekrar Sayısı)	Veri Üzerine Yazılan Veri	Hedeflenen Kodlama Şeması		
1	Rastsal (Random)			
2	Rastsal (Random)			
3	Rastsal (Random)			
4	Rastsal (Random)			
5	01010101 01010101 01010101 0x55	(1,7) RLL		MFM
6	10101010 10101010 10101010 0xAA	(1,7) RLL		MFM
7	10010010 01001001 00100100 0x92 0x49 0x24		(2,7) RLL	MFM
8	01001001 00100100 10010010 0x49 0x24 0x92		(2,7) RLL	MFM
9	00100100 10010010 01001001 0x24 0x92 0x49		(2,7) RLL	MFM
10	00000000 00000000 00000000 0x00	(1,7) RLL	(2,7) RLL	
11	00010001 00010001 00010001 0x11	(1,7) RLL		
12	00100010 00100010 00100010 0x22	(1,7) RLL		
13	00110011 00110011 00110011 0x33	(1,7) RLL	(2,7) RLL	
14	01000100 01000100 01000100 0x44	(1,7) RLL		
15	01010101 01010101 01010101 0x55	(1,7) RLL		MFM
16	01100110 01100110 01100110 0x66	(1,7) RLL	(2,7) RLL	
17	01110111 01110111 01110111 0x77	(1,7) RLL		
18	10001000 10001000 10001000 0x88	(1,7) RLL		
19	10011001 10011001 10011001 0x99	(1,7) RLL	(2,7) RLL	
20	10101010 10101010 10101010 0xAA	(1,7) RLL		MFM
21	10111011 10111011 10111011 0xBB	(1,7) RLL		
22	11001100 11001100 11001100 0xCC	(1,7) RLL	(2,7) RLL	
23	11011101 11011101 11011101 0xDD	(1,7) RLL		

24	11101110 11101110 11101110 0xEE	(1,7) RLL		
25	11111111 11111111 11111111 0xFF	(1,7) RLL	(2,7) RLL	
26	10010010 01001001 00100100 0x92 0x49 0x24		(2,7) RLL	MFM
27	01001001 00100100 10010010 0x49 0x24 0x92		(2,7) RLL	MFM
28	00100100 10010010 01001001 0x24 0x92 0x49		(2,7) RLL	MFM
29	01101101 10110110 11011011 0x6D 0xB6 0xDB		(2,7) RLL	
30	10110110 11011011 01101101 0xB6 0xDB 0x6D		(2,7) RLL	
31	11011011 01101101 10110110 0xDB 0x6D 0xB6		(2,7) RLL	
32	Rastsal (Random)			
33	Rastsal (Random)			
34	Rastsal (Random)			
35	Rastsal (Random)			

(**Kaynak:** University of Auckland)

Bir sabit sürücünün Gutmann algoritmasıyla silinmesi, bir yazılımı veya donanım tabanlı kurtarma seçeneklerini hariç tutar.

Orijinal olarak, Gutmann yöntemi daha önce üretilen sabit diskler için geliştirilmiştir. Gutmann, günümüzde, sabit disklerin 35 veri üzerine yazılması yoluyla silinmeleri gerekmediği, modern bir sabit diskin, güvenli veri silmeyi sağlamak için yalnızca birkaç yazma işlemine ihtiyacı olduğuna da inanmaktadır.[9]

4.1.4. İngiltere İmha Standartları

İngiltere'de CESG CPA-Higher Level ve HMG Infosec Standardı olmak üzere iki imha standardı vardır. Bunların özellikleri aşağıda verilmiştir:

[9] Chris Hofman, "You Only Need to Wipe a Disk Once to Securely Erase It," 2016, (Çevrimiçi) https://www.howtogeek.com/115573/htg-explains-why-you-only-have-to-wipe-a-disk-once-to-erase-it/, 14 Eylül 2019.

4.1.4.1. İngiltere Hükümeti Ulusal Teknik Otoritesi Bilgi Güvencesi Standardı (The UK government's National Technical Authority for Information Assurance standard CESG CPA – Higher Level)

3 kez üzerine yazma süreciyle beraber, her bir yazma aşamasında doğrulama yaptıktan sonra diğer aşamaya geçen bir uygulamadır. Uygulama adreslenebilir tüm alanlara üç ayrı yazma işlemi gerçekleştirmektedir. Aşağıda üç ayrı adım açıklanmaktadır:[10]

Adım 1: 8 bitlik tek bir ikili değerle üzerine yazma,

Adım 2: Adım 1'deki değerin tamamlayıcısını kullanan ikinci bir üzerine yazma.

Adım 3: Üçüncü üzerine yazma, rastsal bir bit akışından oluşmaktadır. Ancak üçüncü üzerine yazma işleminin 8 bitlik tek bir rastsal ikili değer kullanmasına izin verilmektedir. Rastsal 8 bitlik bir değer kullanıldığında, birinci veya ikinci üzerine yazma için kullanılanlarla aynı değildir. Üzerine yazılan üç değerin her biri adreslenebilir tüm alanlara yazılmaktadır.

4.1.4.2. İngiliz HMG Infosec Standardı (British HMG Infosec Standard 5)

İngiliz HMG Infosec Standard 5, bazı veri imha programları tarafından kullanılmaktadır. Bir sabit diskte veya başka bir depolama ortamında var olan bilgilerin üzerine yazılmasını sağlar. Yazılım tabanlı bir veri silme yöntemidir. HMG Infosec Standart 5, ABD Savunma Bakanlığı'nın DoD 5220.22-M prosedürüyle neredeyse aynıdır. Aşağıda belirtilen şekilde üzerine yazma işlevini gerçekleştirir:[11]

Adım 1: Verilerin üzerine 0 (sıfır) ile yazma;

Adım 2: Verilerin üzerine 1 (bir) ile yazma;

Adım 3: Verilerin üzerine rastsal bir karakter ile yazma ve bu karakterin yazısını doğrulamak.

[10] United Kingdom National Cyber Security Centre, **CPA Security Characteristic, Overwriting Tools For Magnetic Media, Version 2.1**, 2016, s. 8, (Çevrimiçi) https://www.ncsc.gov.uk/products/4secure-erase-version-10, 8 Eylül 2019.

[11] DGD Deutsche Gesellschaft für Datenschutz GmbH, "Erasure Standards,"

HMG Infosec Standart 5, veri silme yöntemi kullanılarak bir sabit disk silinirse, verilerin yazılım tabanlı bir restorasyonu genellikle imkânsızdır. Ayrıca, verilerin donanım tabanlı bir restorasyonu çoğu durumda hariç tutulmaktadır. Bu yöntemi ilk olarak, Birleşik Krallık Hükümeti'ne ait olan Communications Electronics Security Group (CESG) tarafından HMG Bilgi Güvence Standardı No. 5 olarak tanımlanmıştır.

4.1.5. Kanada İmha Standartları

Kanada'nın bilinen iki imha standardı bulunmaktadır. Bunlar; RCMP TSSIT OPS-II ve CSEC ITSG-06'dır. Yaygın olarak CSEC ITSG-06 kullanılmaktadır. Her ikisine ait özellikler aşağıda verilmiştir:[12]

4.1.5.1. Kanada Kraliyet Atlı Polisleri Standardı (Royal Canadian Mounted Police, TSSIT OPS-II)

Kanadalı Atlı Polis Standardı RCMP TSSIT OPS-II, Kanada hükümeti tarafından daha önce kullanılan veri silme prosedürüdür. Bu silme prosedürü sayesinde, veri taşıyıcısındaki tüm veriler değişen dizilerin üzerine yazılır. Yazılım tabanlı bir veri silme yöntemidir. Bu silme standardının fonksiyonları şunlardır:

Adım 1: Verilerin üzerine 0 (sıfır) ile yazma;

Adım 2: Verilerin üzerine 1 (bir) ile yazma;

Adım 3: Verilerin üzerine 0 (sıfır) ile yazma;

Adım 4: Verilerin üzerine 1 (bir) ile yazma;

Adım 5: Verilerin üzerine 0 (sıfır) ile yazma;

Adım 6: Verilerin üzerine 1 (bir) ile yazma;

Adım 7: Verinin üzerine rastsal bir karakter ile yazmanın yanı sıra bu karakterin yazısını da doğrulama.

TSSIT OPS-II kullanılarak sabit sürücüler silinirse, yazılım kurtarma veya donanım tabanlı restorasyon yöntemleriyle veri kurtarma işlemi gerçekleştirilemez. RCMP TSSIT OPS-II veri silme yöntemi aslen Kanada Kraliyet Polis Teşkilatı OPS-

[12] **A.y.**

II belgesinde (RCMP) "Bilgi Teknolojisi için Teknik Güvenlik Standartlarının Sanitasyonu" belgesinde yayınlanmıştır. Orijinal TSSIT OPS-II yazılımı artık Kanada hükümeti tarafından kullanılmamaktadır. Kanada'daki mevcut veri silme standardı CSEC ITSG-06 standardıdır. Bu standartla ilgili bilgiler sonraki başlıkta verilmiştir.

4.1.5.2. Kanada İletişim Güvenliği Kurumu Standardı (Communication Security Establishment Canada Standard CSEC ITSG-06)

CSEC ITSG-06 bazı veri imha programları tarafından kullanılır. Yazılım temelinde, bir sabit sürücü veya başka bir depolama ortamında var olan bilgilerin üzerine yazılmasını sağlar. Veri silme yöntemi şu şekilde uygulanır:

Adım 1: Verilerin üzerine 0 (sıfır) veya 1 (bir) ile yazma;

Adım 2: Verilerin karşıt işaretiyle üzerine yazılması (ilk geçişte 1 (bir) ile yazılmışsa, ondan sonrası için 0 (sıfır) sıfır kullanılır, ilk geçişte 0 (sıfır) ise, ondan sonrası için 1 (bir) kullanılır);

Adım 3: Verinin üzerine rastsal bir karakter ile üzerine yazma ve bu karakterin yazısını doğrulama.

Bu veri silme yöntemiyle bir sabit sürücünün silinmesi, yazılım tabanlı veya donanım tabanlı dosya kurtarmayı hariç tutmaktadır. CSEC ITSG-06 standardı başlangıçta IT-Güvenlik Rehberi 06'da tanımlanmıştır. Kanada'da, CSEC ITSG-06, RCMP TSSIT OPS-II yerine kullanılmaktadır.

4.1.6. Rusya Federasyonu İmha Standartları

Rusya Federasyonun kullandığı bilinen bir imha standardı bulunmaktadır. GOST R 50739-95'in özellikleri aşağıda verilmiştir:[13]

4.1.6.1. Rus Devlet Standardı (Russian State Standard, GOST R 50739-95 (russ. ГОСТ Р 50739-95))

Veri silme için Rus standardı GOST R 50739-95 (Rusça: ГОСТ Р 50739-95), bazı programlar tarafından güvenli veri silme amacıyla kullanılır. Yazılım aracılığıyla

[13] DGD Deutsche Gesellschaft für Datenschutz GmbH, "Erasure Standards,"

bir sabit diskteki veya başka bir depolama ortamındaki mevcut bilgilerin üzerine yazılmasını mümkün kılar. GOST R 50739-95, sıklıkla GOST p50739-95 olarak adlandırılır. Bu yöntem, genellikle aşağıdaki iki yoldan biriyle uygulanır:

Versiyon 1.

Adım 1: Verilerin üzerine 0 (sıfır) ile yazma;

Adım 2: Verilerin üzerine rastsal bir karakter ile yazma.

Versiyon 2.

Adım 1: Verilerin üzerine rastsal bir karakter ile yazma.

Bir sabit disk GOST R 50739-95 yöntemiyle silindikten sonra, yazılımın veya donanım tabanlı bir veri geri yüklemesi genellikle başarısız olur. GOST standardı başlangıçta bilgiye yetkisiz erişime karşı koruma sağlamak için tasarlanmıştır. ГОСТ, государственный стандарт'ın "Devlet Standardı" olarak çevrilmiş kısaltmasıdır. Güvenli Veri Silme için sayısız program, GOST R 50739-95 standardını da destekler.

4.1.7. Yeni Zelanda İmha Standartları

Yeni Zelanda'da kullanılan imha standardı Yeni Zelanda Bilgi ve İletişim Teknolojileri Standardı (New Zealand Information and Communications Technology Standard NZSIT 402)'dir. Bu standardın özellikleri aşağıda verilmiştir:[14]

Veri silme için Yeni Zelanda standardı (NZSIT 402) birçok veri imha programı tarafından kullanılmaktadır. Bir sabit sürücü veya başka bir depolama ortamında var olan bilgilerin üzerine bir kez yazılır ve bu nedenle veri silme için yazılım tabanlı bir yöntem oluşturur. Söz konusu standart, Yeni Zelanda hükümeti standardı olarak kullanılmaktadır. The NZSIT 402 veri silme süreci genel olarak aşağıdaki şekliyle uygulanır:

Adım 1: Verinin üzerine rastsal bir karakter ile üzerine yazma ve bu karakterin yazısını doğrulama.

Sabit diski NZSIT 402 ile silmek, yazılım tabanlı verilerin restorasyonunu genellikle önler. Donanım tabanlı veri kurtarma da bu standartta başarısız olur. NZSIT

[14] **A.g.m.**

402 veri silme yöntemi ilk önce Yeni Zelanda hükümeti tarafından İletişim Teknolojileri Güvenliği El Kitabındaki İletişim Güvenliği Bürosu tarafından yayınlandı. Güvenli veri silme için birkaç program tarafından desteklenir.

4.1.8. Kullanılan Veri Silme Standartlarının Özellikleri

Yukarıda sıralanan dünyadaki yaygın imha standartlarının özelliklerini tek bir tablo üzerinden göstermek ve imha özelliklerinin anlaşılmasını kolaylaştırmak için tarafımızdan aşağıdaki tablo **(Tablo 4.2)** hazırlanmıştır. Tabloda standardın geliştirildiği ülke ismi, kullandığı yöntem, teknik bilgileri yanı sıra standardın doğrulama yapıp yapmadığı, yazılımsal veya donanımsal tabanlı olarak silinmiş verinin dönüşüne izin verip vermediği gibi sütunsal başlıklarla karşılaştırma yapılmıştır.

Aşğaıda verilen tabloya göre geliştirilen standartların kullandığı yöntemlerin başında üzerine yazma gelmektedir. Üzerine yazma haricinde blok silme, kriptografik silme ve de-manyetize etme yöntemleri kullanılmaktadır. Üzerine yazma tekniklerine baktığımızda asgari 1 kez olmak üzere işlemi 35 kez tekrar edecek standartlar da bulunmaktadır. Üzerine yazma işlemi gerçekleştikten sonra doğrulama yapılıp yapılmadığı standarttan standarda değişişiklik göstermektedir. Bazılarında doğrulama yapıp yapmadığı bilinmezken bazıları birden çok doğrulama da yapabilmektedir. Bu standartlarda önemli olan konu ise imha edilen verinin yazılım veya donanım tabanlı verinin tekrar kurtarılmasıdır. Bazı standartlar yazılım tabanlı kurtarmayı imkansız hale getirirken bazıları da donanım tabanlı kurtarmayı mümkün kılmamaktadır. Bir kısmı ise hem yazılım hem de donanım tabanlı kurtarmayı desteklemez.

Tablo 4.2: Dünyadaki İmha Standartları ve Özellikleri

Standardın, Geliştirildiği Ülke	İsmi	Kullandığı Yöntem	Kullandığı Teknik	Doğrulama Yapıp Yapmadığı	Yazılım Tabanlı Kurtarılma	Donanımsal Tabanlı Kurtarılma
Almanya	VSITR	Üzerine yazma	7 kez yazma	Yapılmaz	Hayır	Hayır
Almanya	Pfitzner	Üzerine yazma	33 kez	Yapılmaz	Hayır	Hayır
ABD	U.S. Army AR380-19	Üzerine yazma	3 kez	Yapılır	Hayır	Hayır
ABD	DoD 5220.22 M (E)	Üzerine yazma	3 kez	Birden fazla doğrulama yapılır	Hariç tutulmakta	Hariç tutulmakta
ABD	DoD 5220.22-M (ECE)	Üzerine yazma	7 kez	Birden fazla doğrulama yapılır	Hariç tutulmakta	Hariç tutulmakta
ABD	DoD 5220.28-M -STD	Üzerine yazma	7 kez	Birden fazla doğrulama yapılır	Hariç tutulmakta	Hariç tutulmakta
ABD	U.S. Air Force AFSSI-5020	Üzerine yazma	3 kez	Yapılır	Hariç tutulmakta	Hayır
ABD	NIST 800-88 (Clear)	Üzerine yazma	Bilinmiyor	Bilinmiyor	İhtimal dahilinde tutulmakta	Bilinmiyor
ABD	NIST 800-88 (Purge)	Üzerine yazma, Blok silme, Kriptografik silme, De-manyetize etme	Herhangi bir yöntemden biri kullanılabilir	Bilinmiyor	Bazı yöntemler için mümkün değil. Demanyetize etme gibi	Bazı yöntemler için mükün değil. De-manyetize etme gibi
ABD	NIST 800-88 (Destroy)	Fiziksel imha	Parçalama, ezme, eritme, yakma, kıyma	Bilinmiyor	Hayır	Hayır
ABD	Navy Staff Office, NAVSO P-5239-26	Üzerine yazma	3 kez	Yapılır	Hayır	Mümkün görülmemekte.
ABD	National Computer Security Center NCSC-TG-025 Standard	Üzerine yazma	3 kez	Yapılır	Hayır	Hariç tutulmakta
ABD	Bruce Schneier Algorithm	Üzerine yazma	7 kez	Yapılmaz	Hayır	Çoğu durumda hayır

Avustralya	Information Security Manual Standard ISM 6.2.92	Üzerine yazma	1 kez veya 3 kez	Yapılır	Genellikle hayır	Genellikle hayır
Avustralya	Peter Gutmann Algorithm	Üzerine yazma	35 kez	Bilinmiyor	Hariç tutulmakta	Hariç tutulmakta
İngiltere	CESG CPA – Higher Level	Üzerine yazma	3 kez	Yapılır	Bilinmiyor	Bilinmiyor
İngiltere	British HMG Infosec Standard 5	Üzerine yazma	3 kez	Yapılır	Genellikle hayır	Hariç tutulmakta
Kanada	Royal Canadian Mounted Police TSSIT OPS-II	Üzerine yazma	7 kez	Yapılır	Hayır	Hayır
Kanada	CSEC ITSG-06	Üzerine yazma	3 kez	Yapılır	Hariç tutulmakta	Hariç tutulmakta
Rusya	GOST R 50739-95	Üzerine yazma	1 kez veya 3 kez	Bilinmiyor	Genellikle hayır	Genellikle hayır
Yeni Zelanda	NZSIT 402	Üzerine yazma	1 kez	Yapılır	Genellikle hayır	Hayır

(**Kaynak:** Yazar tarafından hazırlanmıştır.)

4.2. ELEKTRONİK BELGE YÖNETİMİNE İLİŞKİN ULUSLARARASI STANDARTLARDA VE DÜZENLEMELERDE İMHA UYGULAMA GÖSTERGELERİ

Dünyada belge yönetimi için çeşitli ülkeler tarafından uygulanan farklı standart ve düzenlemeler bulunmaktadır. Standartlardaki farklılıklar, ülkelerin değişen idari yapılarına, gelişen donanım ve yazılım alt yapılarına, belgelerin üretim, depolama, transfer ve erişim noktasındaki farklılaşmalara ve entegrasyon süreçlerine bağlıdır. Söz konusu farklılıklar ve ihtiyaçlar her ülkenin kendine göre standart bir yapı benimsemesine neden olmuştur. Benimsenen standardı sürekli güncelleyerek sürekliliği ve gelişen teknolojik uyumluluğu yakalamak da aynı standardın revizyonuna (5'er yıllık

periyotlarda) gereksinimi zorunlu kılmıştır. Bir kısım ülkede durum bu şekildeyken bazı ülkelerde daha önce ortaya konmuş standartları/düzenlemeleri temel alarak bazı değişikliklerle kendi ihtiyaçlarına göre yeniden düzenlemişlerdir.[15] Bütün bu standartları belirli sınıflara ayırmak mümkündür. Bu standart sınıflamalarını temel standartlar, faaliyete özgü standartlar, analiz standartları, sistem standartları ve format

[15] Özgür Külcü, **Kurumsal Bilgi Sistemleri ve Belge Yönetimi: Organizasyonlarda Bilgi ve Belge Yönetimi Sistemlerinin Temel İlkeleri**, İstanbul, Hiperlink Yayınları, 2018, s. 165.

standartları olmak üzere 5 farklı başlıkta inceleyebiliriz.[16] İncelenen bu standartlar iki farklı açıdan değerlendirilmiştir. Birinci açı, başlıkta da belirtildiği gibi, elektronik belge yönetimine ilişkin özelliklerin bulunmasıdır. İkinci açı ise, elektronik belge yönetimini ilgilendiren bu standartların elektronik belge ve izlerinin imhasıyla ilgili herhangi bir düzenlemeye ilişkin gösterge bulunup bulunmadığıdır. Bu iki açıdan değerlendirilen standartlar liste şeklinde verilmiş olup, elektronik imhaya ilişkin düzenleme göstergeleri içerenler alt başlıklar halinde belirtilmiştir. Bunun bir istisnai noktası da bulunmaktadır. Bu istisna, Türkiye'de hazırlanan elektronik belge yönetim standardının alt başlık şeklinde verilmiş olmasıdır. Söz konusu standartta elektronik belge ve izlerine ilişkin herhangi bir gösterge söz konusu değildir. Türkiye için önemli bir düzenleme olduğundan ayrı bir başlık halinde verilmesinin uygun olacağı düşünülmüştür.

4.2.1. Belge Yönetimine İlişkin Temel Standartlarda İmha

Temel standartlar, belge yönetimine ilişkin diğer standartların, yönergelerin ve rehberlerin hazırlanmasında başvurulan birincil değerdeki kaynaklardır. Bu kaynaklarda, hangi ortamda olursa olsun belgelerin sahip olması gereken özellikleri vurgulanır ve bu konuda rehberlik edilir. Örneğin, ISO 15489 standardı, belge yönetiminde temel gereklilikler ve ilkeler konusunda sınırlar çizmektedir. Yine CAN/CGSB-72.34-2017 standardı, yasal işlemlerde kanıt olarak kabul edilebilirliklerini ve ağırlıklarını desteklemek için elektronik ortamdaki her türlü belgenin üretimi ve yönetimi için ilkeleri, yöntemleri ve uygulamaları ana hatlarıyla belirtir.[17] Temel olarak nitelendirilecek olan belge yönetimine ilişkin standartlar aşağıda listelenmiştir:

- Avustralya Ulusal Belge Yönetim Standardı AS 4390 (AS 4390: 1996 Records Management)
- AS ISO 15489-1 Enfomasyon ve Dokümantasyon - Belge Yönetimi 1. Bölüm: Kavramlar ve İlkeler (ISO 15489-1:2016 – Information and Documentation - Records Management - Part 1: Concepts and Principles)

[16] Archives of Manitoba Government Records Office, **Recordkeeping Fact Sheet, Recordkeeping Standard**, 2019, s. 1-6, (Çevrimiçi) https://www.gov.mb.ca/chc/archives/gro/recordkeeping/docs/recordkeeping_standards_fact_sheet.pdf, 31 Mayıs 2019.

[17] **A.g.s.**, s. 1-3.

- AS ISO 15489-2 Enformasyon ve Dokümantasyon - Belge Yönetimi 2. Bölüm: Rehber (AS ISO 15489.2-2002, Records Management - Part 2: Guidelines)[18]
- CAN/CGSB-72.34-2017 - Belgesel Kanıt Olarak Elektronik Belgeler (Electronic Records as Documentary Evidence)
- ISO 30300 Belgeler İçin Yönetim Sistemleri: Temel Unsurlar ve Sözlük (Information and Documentation - Management Systems for Records - Fundamentals and Vocabulary)
- ISO 30301 Belgeler İçin Yönetim Sistemleri: Gereksinimler (Information and Documentation - Management Systems for Records - Requirements)

4.2.1.1. Avustralya Ulusal Belge Yönetim Standardı AS 4390

Bu standart, 1995 yılında Avustralya'da geliştirilen belge yönetim alanındaki ilk düzenlemedir. AS 4390: 1996 Records Management adıyla 1996 yılında yayınlandı. Avustralya standardının onaylanıp yayınlanmasının ardından, Uluslararası Belge Yöneticileri Derneği-ARMA International (Association of Records Managers and Administrators) tarafından, uluslararası bir standartın geliştirilmesi üzerinde başlangıç noktası olarak bu standart kullanılmış oldu. Yapılan çalışmalar sonucu 2002 yılında yayınlanan ISO 15489: 2002 Enformasyon ve Dokümantasyon - Belge Yönetimi, AS 4390'ın yerini aldı. AS 4390: 1996 belge yönetimi konusunda tanınmış uluslararası en iyi uygulama rehberi olarak da nitelendirilmektedir.[19] AS 4390'a göre hazırlanan ve onun yerini alan 15489'daki bilgiler bu konuda gerekli bilgiyi vermektedir. Söz konusu bilgi sonraki alt başlık altında verilmiştir.

4.2.1.2. ISO 15489-1 Enformasyon ve Dokümantasyon - Belge Yönetimi[20]

Standardın teknik rapor bölümünde elektronik belgelerin imhası ile ilgili bilgiler, fiziksel imha başlığı altında verilmektedir. Buna göre elektronik belgelerin imhasının

[18] ISO tarafından 2017 yılında kullanımdan kaldırıldı.

[19] Territory Records Office, **Records Advice No 23- Australian Standard for Records Management**, (Çevrimiçi) https://www.territoryrecords.act.gov.au/__data/assets/pdf_file/0008/435527/Records-Advice-No-23-Australian-Standard-for-Records-Management-January-2011.pdf, 24 Mayıs 2019.

[20] ISO 15489-1: 2016, ISO 15489-1: 2001'in yerine geçmiş oldu. 2001 sürümünde ayrıca 2. bölüm de yer aldı. Standardın bu ikinci bölümü gözden geçirilmedi ve 2017 yılında geri çekildi, ancak "bölüm 1" tanımı 15489 başlığında kalmış oldu (Archives of Manitoba Government Records Office, **Recordkeeping Fact Sheet, Recordkeeping Standard**, s. 1).

iki şekilde olabileceği ve bunların formatlama ve üzerine yazma işlemleri olduğu belirtilmektedir. Formatlamaya ilişkin yapılan işlemin geri alınamayacak şekilde olması gerektiği de ifade edilmektedir. Yine elektronik belgelerin uygulama programı ve işletim sistemindeki izlerine ilişkin sistemdeki talimatların yetersiz olacağı da vurgulanmaktadır. Ayrıca depolama seçeneklerinin çokluğuna atıfla yedek kopyaların da imha sürecinde göz önünde bulundurulması istenmektedir. Tüm bunların yanında formatlama ve üzerine yazma işlemlerinin yetersiz kaldığı durumların da olabileceği belirtilmektedir. Buna göre WORM diskler gibi veri saklama alanlarının fiziksel olarak imhası da tavsiye edilmiştir.[21] Verilen bilgiler, ISO 15489 standardının elektronik belgeye uygulanan imha işleminin belgenin izlerine de uygulanması bu standardın imha açısından da önemli bir eksiği kapatmaya çalıştığını göstermektedir.

4.2.1.3. CAN/CGSB-72.34-2017 – Belgesel Kanıt Olarak Elektronik Belgeler

Standardın 6.4.6.3 numaralı maddesinde sistem işlem günlüklerinin, denetim izlerinin ve diğer uygun imha ve değişiklik yapılan faaliyet kayıtlarının kalıcı olarak muhafaza edilmesi gerektiği vurgulanmaktadır. Bu vurgudan sonra, özellikle gizlilik mevzuatı veya diğer mevzuata uygun olarak yasal veya idari gereklilikler nedeniyle belirli bir kaydın belge yönetim sisteminden imha edilmesi gerekebileceği durumlar olabileceği ifade edilmiştir. Bunun için de belge yönetim sisteminin düzenlenebilir bir işlem kullanarak belgeleri imha etmesine, değiştirmesine veya düzeltmesine izin vermesinin uygun olacağı belirtilmektedir. İmha edilen belgeler için, sistem prosedürleri hem belgenin hem de konumlandırıcının yok edilmesini sağlamalıdır. Elektronik belgelerin imhası, belgelerin gizliliğini koruyacak ve kişisel bilgiler açıklanmayacak bir şekilde tamamlanması istenmektedir.[22] Anlaşıldığı üzere, imha uygulamlarına ilişkin faaliyetlerin kayıt altına alınması, yapılan işin mevzuata uygun olarak işlemesi gerektiği açıklanmıştır. Bu açıklamadan sonra belge yönetim sistemlerinin imha uygulama fonksiyonunun olması ve bunun belgelerin kendisine ve diğer izlerine de uygulanarak

[21] Türk Standartları Enstitüsü, **TS ISO/TR 15489-2 Enformasyon ve Dokümantasyon – Belge Yönetimi, Bölüm 2: Klavuz**, 2001, s. 23-24.

[22] National Standard of Canada, **CAN/CGSB-72.34-2017 –Electronic Records as Documentary Evidence**, Gatineau-Canada, Canadian General Standards Board, 2017, s. 19, (Çevrimiçi) http://publications.gc.ca/collections/collection_2017/ongc-cgsb/P29-072-034-2017-eng.pdf 24 Mayıs 2019.

tamamen ortadan kaldırılması şeklinde olması gerektiği açıklanmıştır. Ayrıca, yapılan imha uygulamalarının belgelerin gizliliğini ifşa etmeyecek şekilde olması da dikkat edilmesi gereken noktalardandır.

Standardın 7.2.2 nolu "gizlilik" bölümünde, gizliliğin bulut bilişimde önemli bir problem olduğu ifade edilmiştir. Her ne kadar kaydedilen bilgilerin fiziksel olarak aynı ülke sınırları içinde tutulmuş olsa bile, çevrimiçi erişim, herhangi bir yerden erişilebileceği gibi, saldırıya uğramış, tahrif edilmiş ya da farklı bağlamlara dâhil edilebilecek anlamına gelebileceği değerlendirilmektedir. Bunun yanı sıra, imha için planlanan belgelerin aslında fazlalık ve yedeklemeler nedeniyle bulundukları tüm yerlerde imha edileceği garantisinin olmayacağı söylenmektedir. Çoğu durumda, erişim bağlantılarının kaldırıldığı ancak malzemenin imha edilmediği belirtilmektedir.[23] Burada ifade edilen imha uygulamalarına yönelik kaygılar bu çalışmanın da temelini oluşturmaktadır.

4.2.2. Faaliyete Özgü Standartlar

Faaliyete özgü standartlar, belge yönetiminin temel ilkelerinden ziyade belge yönetimi içinde belirli önemli süreçlerin daha iyi takip edilmesi için yapılan düzenlemelerdir. Örneğin belge üretim süreçlerinden biri olan belgelerin dijitalleştirilmesi belge yönetimi içinde belge üretim aşamalarından biridir. Sadece bu aşamaya yönelik yapılan düzenleme faaliyete özgü düzenlemedir. Belgelerin dijitalleştirilmesi yanında belgelerin dönüşümü ve taşınması için hazırlanan standartlar ile belgelerin üstverileri için oluşturulan standartlar da mevcuttur. Aşağıda söz konusu faaliyete özgü standartlar listelenmiştir.

- ISO/TR 13028:2010 – Belgelerin Dijitalleştirilmesi İçin Uygulamalı Rehberler (Information and Documentation - Implementation Guidelines for Digitization of Records)
- ISO 13008:2012 - Dijital Belgelerin Dönüşüm ve Taşınma süreçleri (Information and Documentation - Digital Records Conversion and Migration Process)

[23] **CAN/CGSB-72.34-2017 –Electronic Records as Documentary Evidence**, s. 25.

- ISO 23081-1 - Belgeler İçin Üstveri 1. Bölüm: Prensipler (AS ISO 23081.1-2006, Information and Documentation - Records Management Processes - Metadata for Records – Principles.)
- ISO 23081-2 Belgelerin Üstveri Özelliklerinin Yönetimi 2. Bölüm: Kavramsal ve Uygulama Sorunları (Information and Documentation - Managing Metadata for Records - Part 2: Conceptual and Implementation Issues)
- ISO 23081-3 Belgelerin Üstveri Özelliklerinin Yönetimi 3.Bölüm: Bireysel Değerlendirme Metotları (Information and Documentation - Managing Metadata for Records - Part 3: Self-assessment Method)

4.2.2.1. ISO 23081-1/2/3 Belgeler İçin Üstveri

Bu standart üç bölümden oluşmaktadır. ISO 23081-1, üstverinin ISO 15489 çerçevesinde anlaşılması, uygulanması ve kullanılması için bir rehber niteliğindedir. ISO 23081-2 ve ISO 23081-3 ise daha çok üstverinin uygulanma sorunları üzerinde pratik bilgiler sağlamaktadır. Ayrıca belge yönetimine ilişkin üstverinin bu standarttaki ilkelere uygunluğu değerlendirilmektedir.[24] Standardın 2017 baskısındaki 5.2.3. nolu alt başlık olan belge sağlama sonrası üstveri ve 9.3.1. nolu alt başlık olan belge sağlama açısından kurum kuralları, politikaları ve zorunlulukları hakkındaki üstveri olarak iki kısımda imha ile ilgili bilgiler verilmiştir. Yukarıda ifade edildiği gibi bu standart ISO 15489 çerçevesinde üstveri oluşturmaya yönelik bir kılavuzdur. Bu nedenle ISO 15489'daki imha gereklilikleri üstveri kısmında da yer bulmuştur.

4.2.3. Analiz Standartları

Analiz standartları, bir kurum veya kuruluşun iş gereksinimlerini karşılamak için gereken belge yönetimi gereksinimlerinin nasıl analiz edileceği konusunda rehberlik eder. Standartlar, belgelerin nasıl ve ne kadar süreyle tutulması gerektiğinin yanı sıra,

[24] International Organization for Standardization (ISO), **ISO 23081-1 Information and Documentation- Records Management Processes-Metadata for Records, Part 1: Principles, Second Edition**, 2017, (Çevrimiçi) https://www.sis.se/api/document/preview/922676/, 31 Mayıs 2019.

hangi belgelerin üretilmesi ve sağlanması gerektiğine karar vermek için iş faaliyetlerini değerlendirme sürecine de yardımcı olur.[25] Söz konusu standartların listesi aşağıda verilmiştir.

- ISO/TR 21946:2018 - Belgelerin Yönetiminde Değerlendirme (Information and Documentation - Appraisal for Managing Records)
- ISO/TR 26122: 2008 - Belgelerin İş Süreç Analizleri (Work Process Analysis for Records)
- ISO/TR 18128:2014 - Belge Sistem ve Süreçlerinde Risk Değerlendirmesi (Information and Documentation - Risk Assessment for Records Processes and Systems)

4.2.4. Sistem Standartları

Sistem standartları, elektronik belge yönetimi için işlevsel gereklilikleri ortaya koymaktadır. Bu gereklilikler, iş süreçlerini destekleyen elektronik sistemlerin, belgelerin üretiminin ve yönetiminin bütünlüğünü ve erişilebilirliğini sağlamak için nasıl çalışması gerektiğini belirtirler. Özellikle ISO 16175 ve MoReq2010 bu konuda başlıca standartlardır.[26] Bu iki düzenlemelerin yanı sıra diğer standartlar da aşağıda listelenmiştir:

- DoD 5015. 2-STD Elektronik Belge Yönetimi Yazılım Uygulamalarında Tasarım Kriterleri (Electronic Records Management Software Applications Design Criteria Standard)
- Uluslararası Arşiv Konseyi-ICA Elektronik Ortamdaki Belgeler İçin Temel ve İşlevsel Kriterler (ICA Principles and Functional Requirements for Records in Electronic Office Environments)
- ISO 16175- Elektronik Ortamdaki Belgeler İçin Temel ve İşlevsel Kriterler (Information and Documentation - Principles and Functional Requirements for Records in Electronic Office Environments)

[25] Archives of Manitoba Government Records Office, **Recordkeeping Fact Sheet, Recordkeeping Standard**, s. 3.

[26] **A.g.s.**, s. 4.

- ISO 16175-1: 2010: 1. Bölüm - Genel Açıklamalar (Part 1: Overview and Statement of Principles)
- ISO 16175-2: 2011: 2. Bölüm - Dijital Belge Yönetim Sistemleri İçin Rehberler ve İşlevsel Kriterler (Part 2: Guidelines and Functional Requirements for Digital Records Management Systems)
- ISO 16175-3: 2010: 3. Bölüm - Kurumsal Sistemlerde Belgeler İçin Rehberler ve İşlevsel Kriterler (Part 3: Guidelines and Functional Requirements for Records in Business Systems)
- MoReq2010 - MoReq2010 Belge Sistemleri İçin Modül Gereklilikleri (Modular Requirements for Records Systems, June 2011)
- TNA 2002 - Elektronik Belge Yönetim Sistemleri İçin Kriterler (Requirements for Electronic Records Management Systems
- TNA 2002 Birleşik Krallık Ulusal Arşivi Elektronik Belge Yönetim Sistemleri İçin Gereklilikler – 1: Fonksiyonel Gereklilikler
- TNA 2002 Birleşik Krallık Ulusal Arşivi Elektronik Belge Yönetim Sistemleri İçin Gereklilikler – 2: Üstveri Standardı
- TNA 2002 Birleşik Krallık Ulusal Arşivi Elektronik Belge Yönetim Sistemleri İçin Gereklilikler – 3: Referans Dokümanı
- TNA 2002 Birleşik Krallık Ulusal Arşivi Elektronik Belge Yönetim Sistemleri İçin Gereklilikler – 4: Uygulama Kılavuzu
- TS 13298: 2015- Elektronik Belge ve Arşiv Yönetim Sistemi

4.2.4.1. DoD 5015. 2: 2007 Elektronik Belge Yönetimi Yazılım Uygulamaları Tasarım Kriterleri

Amerika Savunma Bakanlığı belge yönetim uygulama standardı olan DoD 5015.2-STD, 2002 yılındaki versiyonunda belgelerin imhası bölümünde madde C2.2.6.6.3'te "belge yönetim uygulamaları, imha edilmesi onaylanan elektronik belgeleri, belgelerin fiziksel olarak yeniden yapılandırılamayacak şekilde sileceğinden" bahseder. Aynı standardın 2007 versiyonunda madde C2.2.7.6.3'te ise "imha için onaylanan elektronik belgelerin, yaygın olarak bulunan dosya geri yükleme yardımcı programlarını kullanarak fiziksel yeniden yapılandırmalarını engelleyecek şekilde si-

linmesi" şeklinde ifade edilmiştir. Bu kriterin yasal dayanağı da Code of Federal Regulations (Federal Düzenlemeler Kodu) CFR1228.34 nolu maddeye bağlanmaktadır. DoD kriterlerindeki bu değişiklik zamanla yazılım ve donanım eksikliğinin yine yazılım ve donanım araçlarıyla ortaya çıkarılması veya sorunun giderilmesinin sağlandığını göstermektedir. Bu değişiklik olmasa bile silinen belgelerin hiçbir şekilde geri getirilmesi mümkün olmayacak duruma getirilmesi ilkesi varlığını korumaktadır. Bilgi teknolojileri ürünleri çeşitlerinin gün geçtikçe artması, söz konusu ilke için imha uygulamaları açısından tehdit oluştursa bile buna yönelik tedbirler de aynı ivmeyle ortaya çıkmaktadır. Önemli olan bu gelişmeleri takip edip mevcut elektronik belge yönetim sistemlerinde bu düzenlemeleri uygulamak olacaktır.

4.2.4.2. ICA Elektronik Ortamdaki Belgeler İçin Temel ve İşlevsel Kriterler

Uluslararası Arşiv Konseyine göre elektronik belge yönetim sistemlerindeki silme işlemi kalıcı olarak imha etmeyi kast eder. Ancak yedeklemeler, kişisel sabit sürücüler vb. nedenlerle ve dijital adli bilişim aracılığıyla malzemeye (silinmesine rağmen) erişilebilir, bulunabilir veya kurtarılabilir. Bu teknik konuların politika veya teknik düzeyde ele alınması gerektiği ifade edilir. Buna ilişkin alınacak yasal veya güvenlik gereksinimlerinin "her şeyden önemli" olduğu vurgusu yapılır.[27] ICA'nın 2006-2008 yılları arasında hazırlamış olduğu bu kriterleri, ISO tarafından 2010 yılında kabul görmüş ve ISO 16175 nolu standart olarak yayınlanmıştır.[28] Bu nedenle buradaki imha göstergeleri ISO 16175 standardının da göstergelerini yansıtmaktadır.

4.2.4.3. (MoReq1- MoReq2-) MoReq2010 – MoReq2010 Belge Sistemleri İçin Modül Gereklilikleri

Avrupa Birliği tarafından hazırlanan modül gerekliliklerinin birinci versiyonu olan MoReq (birinci sürüm)'de 5.3.13 nolu kriterde, elektronik belge yönetim sistem-

[27] International Council on Archives (ICA), **Principles and Functional Requirements for Records in Electronic Office Environments – Module 2: Guidelines and Functional Requirements for Electronic Records Management Systems**, 2008, s. 41-42, (Çevrimiçi) www.ica.org, 31 Mayıs 2019.

[28] ICA, **Principles And Functional Requirements For Records In Electronic Office Environments: Overview of Implementation Guidance and Training Products**, 2013, s. 4, (Çevrimiçi) https://www.ica.org/sites/default/files/1%20Overview.pdf, 14 Eylül 2019.

lerinin yeniden yazılabilir medyada depolanan belge sınıflarının ve bireysel belge dosyalarının, tamamen veri kaybına uğratılarak, uzman veri kurtarma olanaklarıyla geri yüklenemeyecekleri şekilde tamamen imha edilmesinin sağlanması gerektiği ifade edilmektedir. Söz konusu kriterin devamında bazı ortamlarda, verilerin üzerine yazma işlemini belirli standartlara göre uygulanması istenmektedir. Bu işlem yapılırken yedekleme ünitelerindeki kopyaların da göz önünde bulundurulması gerektiği ayrıca belirtilmektedir. Ayrıca üzerine yazma işleminin MoReq (birinci sürüm) kapsamında olmadığı, bu işlem için ayrı düzenlenmiş prosedürler gerektiği belirtilmektedir. Yeniden yazılabilir medya için imha uygulamaları bu şekilde iken üzerine bir kez yazılabilen ortamlar için ise 5.3.14 nolu kriterde açıklama yapılmıştır. Bu kriterde, üzerine bir kez yazılan ortamın imhası için "normal kullanımı veya standart işletim sistemi yardımcı programları tarafından geri alınamayacak şekilde bunlara erişimi engellemek için olanaklar sağlamalıdır" şeklinde açıklama yapılmaktadır. Bu yolla verilerin konumlarını üzerine bir kez yazılan ortamda depolanan index verilerin (yeniden yazılabilir medyada tutulan) imha edilmesi anlamına geldiği de ifade edilmiştir.[29] MoReq2 (ikinci sürüm)'nin 5.3.18 nolu kriterinde "elektronik belge yönetim sisteminin imha için işaretlenmiş bir belgeyi imha ettiğinde, belgeye ait tüm yorumlamaların da imha edilmesini sağlamalıdır" şeklindeki ifadeye yer verilmiştir.

4.2.4.4. TNA 2002 Birleşik Krallık Ulusal Arşivi Elektronik Belge Yönetim Sistemleri İçin Gereklilikler

TNA 2002'deki gerekliliklerin 1 nolu dokümanı olan fonksiyonel gerekliliklerde imhaya ilişkin A.4.67 nolu sistem kriterinde belgelerin yeniden yazılabilir ortamdaki depolandığı yerlerde, elektronik belge yönetim sisteminin, işletim sistemi özellikleri veya uzman kişiler tarafından verilerin geri yüklenemeyecek şekilde, programlanmış ve onaylanmış belgelerin, parçaların, klasörlerin ve klasör gruplarının tamamen yok edilmesinin sağlanması gerektiği belirtilmektedir.[30] Bu istek zorunlu olan kriterler içinde yer almaktadır. Hatta aynı dokümanın A.4.74 nolu kriterde EBYS içinde bir

[29] European Communities, **MoReq Specification-Model Requirements for the Management of Electronic Records**, Bruxelles- Luxembourg, CECA-CEE-CEEA, 2001, s. 38, (Çevrimiçi) https://ec.europa.eu/idabc/servlets/Doc1faf.pdf?id=16847, 31 Ekim 2018.

[30] The National Archives of United Kingdom (TNA), **Requirements for Electronic Records Management Systems-1: Functional Requirements**, **2002 Revision: Final Version**, 2002, Surrey-United Kingdom, s. 29.

belge imha sürecine dâhil olduğunda, söz konusu belgenin sunuşlarına ilişkin tüm bilginin de imha edilmesinin sağlanması gerektiği ifade edilmektedir.[31]

4.2.4.5. TS 13298: 2015- Elektronik Belge ve Arşiv Yönetim Sistemi

TS 13298: 2015, Türk Standartları Enstitüsünün Bilişim İhtisas Kurulu'na bağlı TK01 Bilişim Teknolojileri Teknik Komitesi'nce TS 13298: 2009'in revizyonu olarak hazırlanmış ve TSE Teknik Kurulu'nun 23 Ekim 2015 tarihli toplantısında kabul edilerek yayımına karar verilmiş ulusal bir standarttır.[32] Türkiye'de kamu kurumlarının elektronik belge yönetim sistemi temininde söz konusu standarda uygunluk şartı aranan belge yönetim alanındaki önemli bir düzenlemedir. Standardın hazırlanmasında uluslararası standart ve düzenlemelerden de yararlanılmıştır. Bunlardan bazıları yukarıda açıklanan ISO 15489-1,2, DoD 5015.2 STD, TNA 2002 ve MoReq2 (ikinci sürüm) gibi düzenlemelerdir. Bu düzenlemelerde elektronik belgenin imhasının nasıl olacağı ifade edilmiştir. MoReq2 (ikinci sürüm)'de imha uygulamalarında üzerine yazma ve diğer güvenlik ölçütlerin olabileceği ancak MoReq2 (ikinci sürüm) kapsamında olamayacağı ifade edilmişti. Genel itibariyle elektronik belgelerin imhasının geride iz bırakmayacak şekilde uygulanması, üzerine yazma işlemi veya elektronik belgelerin bulunduğu ortamın fiziksel imhası gibi ifadeler kullanılırken TS 13298 standardında bu şekilde ibarelerle karşılaşılmamıştır. İmha uygulamalarının nasıl olacağına dair kriterler hiçbir şekilde standartta yer bulmamıştır. Kurumlar imhaya ilişkin kriterleri, satın almak istedikleri yazılımın sistem isterlerinde olup olmadığı sorgulamak gerektiğini bilmelidirler. Hazırlanan EBYS yazılımları hazırlanırken belge yöneticisi ve arşivci katılımlı olmak üzere imha isterlerini de sistem isteri olarak isteyebilirler. Hazır EBYS yazılım paketlerinde bunların olmasının oranı düşük olduğundan kurumların, EBYS yazılımları satın alırken bu yazılımların kendi sistem isterlerine uygun olup olmadığını raporlaması sorunun çözümü olarak görülebilir.

4.2.5. Format Standartları

Format standartları, tezin bir önceki bölümünde açıklanan format izleri kısmındaki format çeşitlilikleri düşünüldüğünde, elektronik belge yönetimi için belgelerin

[31] TNA, **Functional Requirements**, s. 30.
[32] Türk Standartları Enstitüsü (TSE), **TS 13298 Elektronik Belge Yönetimi**, 2015.

birçok formatta bulunabileceği anlaşılmaktadır. Çok fazla çeşitliliğin olması belgelerin uzun süreli kullanımında problemlere yol açabilmektedir. Bu nedenle ISO tarafından hazırlanan format standartları, elektronik belge yönetiminde kullanılacak yaygın bir format için önemlidir. ISO'nun 2005 yılında hazırladığı ve 2011 yılında da revize ettiği format standardı aşağıda verilmiştir.

- PDF/A - ISO 19005 - Elektronik Belgelerin Uzun Süreli Korunmasına İlişkin Elektronik Dosya Formatı (Document Management - Electronic Document File Format For Long-Term Preservation).

ISO 19005-1: 2005: 1. Bölüm – PDF 1.4'ün Kullanımı (Document Management – Electronic Document File Format for Long-Term Preservation - Part 1: Use of PDF 1.4 (PDF/A-1))

- ISO 19005-2: 2011: 2. Bölüm - PDF 1.7'nin Kullanımı (Document Management - Electronic Document File Format for Long-Term Preservation - Part 2: Use of ISO 32000-1 (PDF 1.7) (PDF/A-2))

Yukarıda açıklanan elektronik belgelerin yönetiminde kullanılan farklı kategorilerdeki standartlar açıklanmıştır. Bu kategorilerden temel standartlar, faaliyete özgü standartlar ve sistem standartlarında bu tez kapsamında değerlendirilen elektronik belge ve izlerinin imha edilmesi gerektiği pek çok gösterge belirtilmiştir.

4.3. İMHA UYGULAMALARI İÇİN GELİŞTİRİLEN ULUSLARARASI YAZILIMLAR

Veri temizleme yazılımı, disk temizleme yazılımı veya sabit disk silme yazılımı olarak adlandırılan veri imha yazılımı, verileri bir sabit sürücüden tamamen silmeye yönelik yazılım tabanlı bir yöntemdir. Bilgisayarlarda silme işlemi, bilgileri gerçekten silmez, yalnızca işletim sisteminin bulamaması için bazı referansları siler. Referansların silinmesi verilerin varlığına zarar vermemekte ve tüm veriler olduğu gibi sistemde durmaktadır ve bunların üzerine herhangi bir veriyle yazılmadığı sürece, dosya kurtarma yazılımı kullanılarak kolayca kurtarılabilir. Bununla birlikte, veri imha yazılımı verileri gerçekten silebilir. Her veri imha programı, sürücüdeki bilgilerin üzerine kalıcı olarak yazabilecek bir veya daha fazla veri temizleme yöntemini kullanır. Herhangi

bir virüsün tüm izlerini silmek gerekirse veya sabit sürücü veya bilgisayar geri dönüştürülmek veya atılmak isteniyorsa, sabit sürücüyü veri imha yazılımı kullanarak silmek içindeki bilgileri korumanın en iyi yoludur. Aşağıdaki tabloda verilen elektronik veri için hazırlanmış yazılımlar ve bu yazılımların hangi imha standardına göre yöntem geliştirdiği açıklanmıştır.[33] Bu yazılımlar ücretsiz olarak kullanılabilir. Ancak kurum ve birey ihtiyaçları göz önünde bulundurulduğunda bu ücretsiz yazılımlar tam ihtiyacı karşılamayabilir. Söz konusu yazılımların ticari versiyonlarında veya burada ifade edilmeyen diğer birçok yazılımda daha geniş özelliklerle imha işlemi yapılabilmektedir.

Tablo 4.3: İmha Yazılımlarının Kullandıkları Yöntem ve Teknikler

Yazılım Adları		**İmha Standartlarına Bağlı Olarak Geliştirilmiş Yöntemler**	**Silinen Verinin Yazılım ve Donanımsal Geri Getirilme Durumu**	**Desteklenen İşletim Sistemleri**	**Neyi Desteklemez?**
1.	Darik's Boot And Nuke (DBAN)	DoD 5220.22-M, RCMP TSSIT OPS-II, Gutmann, Random Data, Write Zero		Tüm işletim sistemleri Windows, macOS vd.	SSD'ler
2.	CBL Data Shredder	DoD 5220.22-M, Gutmann, RMCP DSX, Schneier, VSITR		Windows XP'den Windows 10 kadar tüm versiyonlar	Bilgi yok
3.	MHDD	Secure Erase		Bilgi yok	Bilgi yok
4.	PCDiskEraser	DoD 5220.22-M		Bilgi yok	Bilgi yok
5.	KillDisk	Write Zero			
6.	Macrorit Data Wiper	DoD 5220.22-M, DoD 5220.28-STD, Random Data, Write Zero.			
7.	Eraser	DoD 5220.22-M, AFSSI-5020, AR 380-19, RCMP TSSIT OPSII, HMG IS5, VSITR,			

[33] Tim Fisher, "40 Free Data Destruction Software Programs: Completely Free Disk Wipe And Hard Drive Eraser Software Utilities," 2019, (Çevrimiçi) https://www.lifewire.com/free-data-destruction-software-programs-2626174?print, 8 Mart 2019.

		GOST R 50739-95, Gutmann, Schneier, Random Data			
8.	Freeraser	DoD 5220.22-M, Gutmann, Random Data			
9.	Disk Wipe	DoD 5220.22-M, GOST R 50739-95, Gutmann, HMG IS5, Random Data, Write Zero			
10.	Hardwipe	DoD 5220.22-M, GOST R 50739-95, Gutmann, Random Data, Schneier, VSITR, Write Zero			
11.	Secure Eraser	DoD 5220.22-M, Gutmann, Random Data, VSITR			
12.	PrivaZer	AFSSI-5020, AR 380-19, DoD 5220.22-M, IREC (IRIG) 106, NAVSO P-5239-26, NISPOMSUP Chapter 8 Section 8-501, NSA Manual 130-2, Write Zero			
13.	PC Shredder	DoD 5220.22-M, Gutmann, Random Data			
14.	AOMEI Partition Assistant Standard Edition	Write Zero			
15.	Remo Drive Wipe	DoD 5220.22-M, Random Data, Write Zero			
16.	CCleaner	DoD 5220.22-M, Gutmann, Schneier, Write Zero			

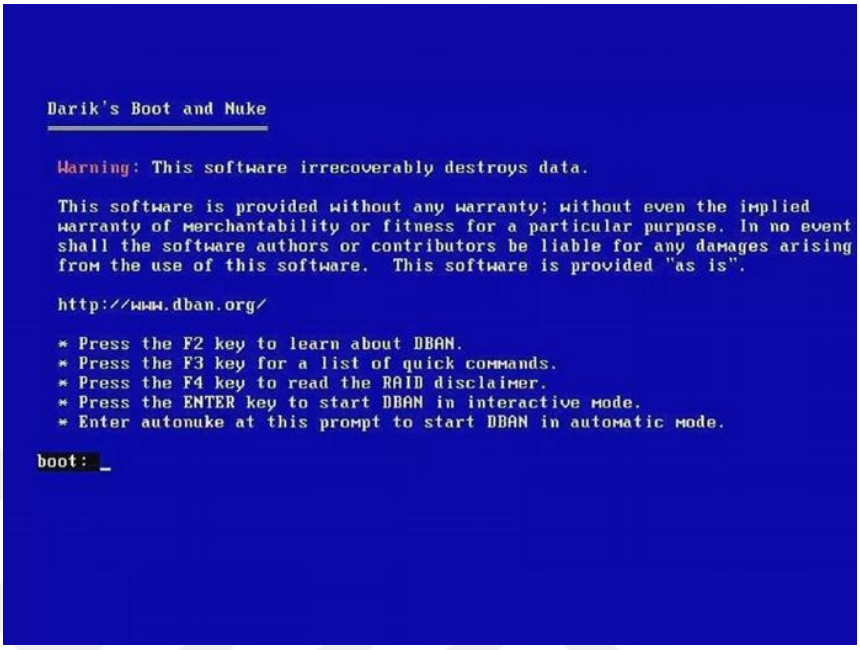
17.	File Shredder	DoD 5220.22-M, Gutmann, Random Data, Write Zero			
18.	Hard Drive Eraser	AR 380-19, DoD 5220.22-M, Gutmann, Write Zero			
19.	Super File Shredder	DoD 5220.22-M, Gutmann, Random Data, Write Zero			
20.	TweakNow SecureDelete	DoD 5220.22-M, Gutmann, Random Data			
21.	MiniTool Drive Wipe	DoD 5220.22-M, DoD 5220.28-STD, Write Zero			
22.	XT File Shredder Lizard	DoD 5220.22-M, Random Data, Write Zero			
23.	Free File Shredder	DoD 5220.22-M, Gutmann, Random Data			
24.	WipeDisk	Bit Toggle, DoD 5220.22-M, Gutmann, MS Cipher, Random Data, Write Zero			
25.	Free EASIS Data Eraser	DoD 5220.22-M, Gutmann, Random Data, Schneier, VSITR, Write Zero			
26.	Puran Wipe Disk	DoD 5220.22-M, Schneier, Write Zero			
27.	BitKiller	DoD 5220.22-M, Gutmann, Random Data, Write Zero			
28.	Simple File Shredder	DoD 5220.22-M, Gutmann, Random Data			
29.	Ashampoo WinOptimizer Free	DoD 5220.22-M, Gutmann,			

		Write Zero			
30.	AbsoluteShield File Shredder	Schneier, Write Zero			
31.	DP Secure WIPER (DPWipe)	DoD 5220.22-M, Gutmann, Write Zero			
32.	DeleteOnClick	DoD 5220.22-M			
33.	CopyWipe	Gutmann, Random Data, Secure Erase, Write Zero			
34.	SDelete	DoD 5220.22-M			
35.	Wise Care 365	Random Data			
36.	ProtectStar Data Shredder	Random Data			
37.	Baidu Antivirus	Write Zero			
38.	Hdparm: Data Sanitization Methods:	Secure Erase			
39.	HDShredder Free Edition	Write Zero			
40.	MilShield,				
41.	BitRaser				
42.	Blancco				
43.	File Eraser				
44.	WipeDrive Home				

(Kaynak: Tablo yazar tarafından hazırlanmıştır.)

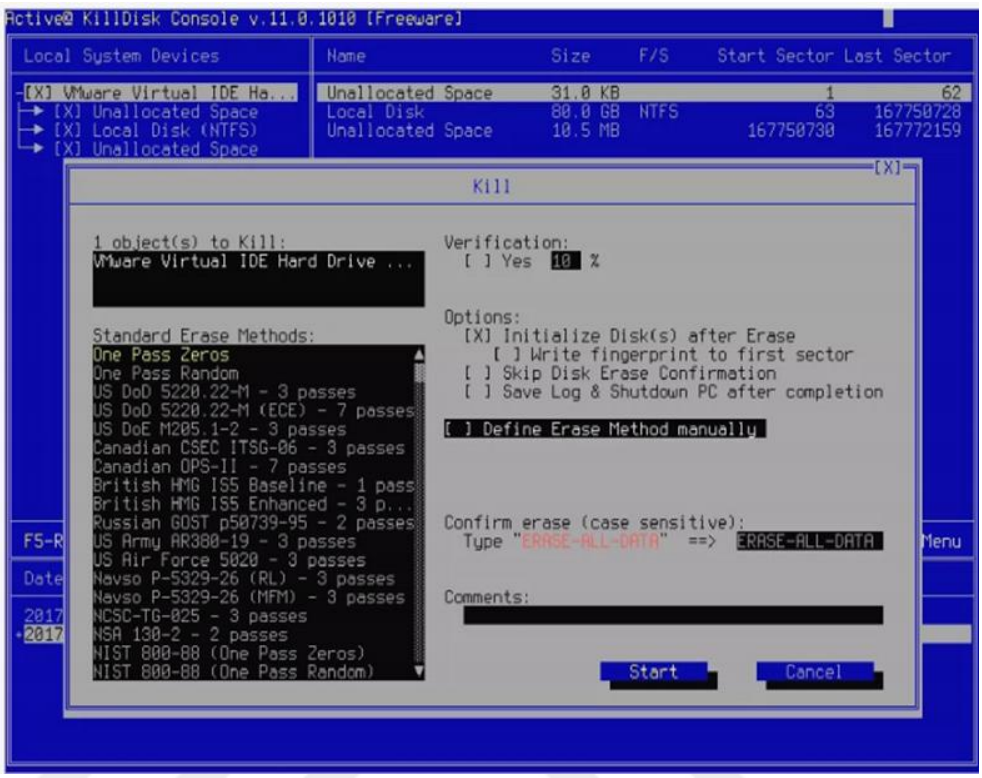
Tabloda verilen imha yazılımlarının kullandıkları yöntem ve teknikler, tezin bu bölümündeki ilk başlıkta açıklanan imha standartlarındaki teknik özelliklere göre hazırlanmıştır. Bazı yazılımlar sadece bir yöntem sunarken bazıları imha standartlarındaki tüm yöntemleri sunabilmektedir. Ancak bazı yazılımlar ticari amaçlarla yazılımın bazı özelliklerini ücretsiz kullandırırken tam işlevli çalışabilen versiyonlar için ücret talebinde bulunabilirler. Yazılımlara ilişkin ekran görüntüleri aşağıda verilmiştir.

Şekil 4.2: Darik's Boot And Nuke (DBAN) Ekran Görüntüsü



(**Kaynak:** Tim Fisher, "40 Free Data Destruction Software Programs: Completely Free Disk Wipe And Hard Drive Eraser Software Utilities," 2019, (Çevrimiçi) https://www.lifewire.com/free-data-destruction-software-programs-2626174?print, 8 Mart 2019)

Şekil 4.3: Killdisk Ekran Görüntüsü



(**Kaynak:** Fisher, "40 Free Data Destruction Software Programs…,".)

4.4. TÜRKİYE'DEKİ DÜZENLEMELER

Türkiye sahip olduğu zengin arşiv malzemesi dolayısıyla dünyadaki arşiv ilke ve uygulamalarına ilişkin gelişmeleri geç de olsa takip etmeye çalışmaktadır. Osmanlı döneminden kalan arşiv malzemesi günümüzde saklanılmakta, düzenleme ve tanımlama işlemlerinden sonra araştırmacıların erişimine açılmaktadır. Türkiye için arşiv malzemesi olan Osmanlı döneminden kalan belgeler, bulundukları dönemlere göre farklı uygulamalara tabi tutulmuştur. Bu uygulamalar, mevcut araştırmanın kapsamı dâhilinde değerlendirildiğinde ifade edilmesi gereken önemli bir uygulama olan evrak imhasının burada da açıklanması anlamlıdır. Özellikle evrak imha ve muhafazasına dair yayımlanan ilk nizamname olarak bilinen Islahat-ı Maliye Komisyonunca hazırlanan altı maddelik nizamname layihası (1334/1917), arşivcilik düşüncesiyle ortaya

konması bakımından değerlidir. Layihaya göre[34] imhası uygun görülen evrakın, yakılarak veya satılmak suretiyle imhâsına karar verilirken evrakın ilgisiz insanların eline geçmemesi için tedbirlerin alınması gerektiği de ifade edilmiştir. Bu hassasiyetin nasıl sağlanacağına dair layihanın altıncı maddesine göre evrak ya okunamayacak bir şekilde kestirilerek satılacak ya da yakılarak imhâ edilecekti. Bütün bakanlıklardan bu hassasiyetin gözetilmesi ve kuralların tatbiki istenmiştir.[35] Her ne kadar ilk düzenleme olarak ifade edilse de layihanın yayınlandığı tarihten önce de imha uygulamalarıyla karşılaşılmaktadır. Bunların arşiv imha uygulamaları ve teorisi bakımından bir anlam ihtiva etmesi söz konusu değildir. Ancak Osmanlı Dönemi'ndeki ilga edilen bir kurumun üretmiş olduğu belgelerin imha edildiği bilinmektedir. Örneğin, 1826 yılında ilga edilen yeniçeri ocağının sahip olduğu evraklar, 1845 yılında dönemin Maliye Bakanı olan Safveti Paşa'nın gerekçeli mazbatasında fırınlarda yakılmak suretiyle imha edilmesi istenmişti.[36] Bu da arşivciliği kapsayan hukuki bir dayanağa ihtiyaç duyulmadan evrakın imhasının gerçekleşmiş olduğunu göstermektedir.

Türkiye Cumhuriyeti'nin kurulmasıyla yeni üretilen belgelerin imhasıyla ilgili hangi düzenlemelerin olduğu da kısaca ifade edilmesinde yarar görülmektedir.

Bu konuda bilinen ilk düzenleme "Resmi Evrak ve Defterlerden Lüzumsuz Olanlarının Yok Edilme Tarzı Hakkında Nizamname (19 Eylül 1934 tarihli ve 2/1282 sayılı Bakanlar Kurulu Kararı)"dir. Bu tüzüğün uygulanması, 21.05.1937 tarihli ve 2/6651 sayılı Bakanlar Kurulu Kararı ile bu konuda yeni bir proje hazırlanana kadar resmi evrak ve defterlerin hiçbir şekilde yok edilmemesi kararlaştırılarak durdurulmuştur.[37]

---

[34] Geniş bilgi için bkz. Bilgin Aydın, "Osmanlı Devleti'nde Evrak İmha ve Muhafazasına Dair Neşredilen İlk Nizamname Layihası," **Arşiv Araştırmaları Dergisi**, , S. 1, 1999, s. 47-53; Fatih Rukancı ve Hakan Anameriç, "Evrak-ı Atikanın Suret-i Tasfiyesine Dair Rapor," **Belgeler**, C. 27, S. 31 2006, s. 96-110.

[35] Bilgin Aydın, "Osmanlı Devleti'nde Evrak İmha ve Muhafazasına Dair Neşredilen İlk Nizamname Layihası," **Arşiv Araştırmaları Dergisi**, , S. 1, 1999, s. 47-53.

[36] İshak Keskin, "Osmanlı Bürokrasisinde Evrak İmha Uygulamalarına Dair Gözlemler," **Türk Devlet Yönetimi Geleneği**, Ed. Cengiz Buyar, Mehmet Kıldıroğlu, Murat Kocobekov, Bişkek, 2016, s. 317.

[37] Fahrettin Özdemirci,"Cumhuriyet Dönemi Milli Arşivimizin Örgütsel Yapılanma Gereksinimleri,", **Bildiriler: Müzeler, Kütüphaneler, Yayınevleri, Telif Hakları**, Ed. Zeki Dilek, Mustafa Akbulut, Zeynep Bağlan Özer, Reşide Gürses, Banu Karababa Taşkın, Ankara, Atatürk Kültür, Dil ve Tarih Yüksek Kurumu Başkanlığı, 2009, s. 196.

Ülkemizde, arşivlerdeki ayıklama ve imha işlemlerini düzenlemek üzere diğer bir düzenleme ise 26 Mart 1956 tarihinde kabul edilen 6696 sayılı "Muhafazasına Lüzum Kalmayan Evrak ve Vesaikin İmha Edilmesi Hakkında Kanun" dur. Kanuna bağlı olarak 13 Eylül 1957 tarihli ve 4/9438 sayılı "Muhafazasına Lüzum Kalmayan Evrak ve Vesaikin İmha Edilmesi Hakkındaki Nizamnameyi Mer'iyete Koyan İcra Vekilleri Heyeti Kararı" çıkarılmıştır.

"Hukuken mer'iyyette olan bu Kanun, uygulamada maalesef geçerlilik kazanamamıştır. Ayrıca, uygulama yönünden olduğu kadar şümulü yönünden de günün ihtiyaçlarına cevap veremez hale gelmiştir.

Bu arada, 1959 yılı ve onu takip eden yılların bütçe kanunlarına, «Muhafazasına Lüzum Kalmayan Evrak ve Vesaikin İmha Edilmesi Hakkındaki 6696 sayılı Kanun hükümleri…. malî yılında uygulanmaz.» şeklinde bir fıkra eklenmiş ve bugüne kadar gelinmiştir.

Ancak, bazı kurum ve kuruluşlar, 1968 yılından sonra bütçe kanunlarına konan bu hükümden yararlanarak ve kendilerine istisna ve özel yetkiler sağlayarak, bu Kanun hükümlerine tabi olmaksızın hazırladıkları yönetmelik esasları içerisinde evrak ve vesaik imha etme yetkisi elde etmişlerdir. Bu arada, esasları bilinmeden, gelişigüzel yapılan ayıklama ve imha işlemi ile de, çok önemli arşiv malzemesinin yok edilmiş olduğu şüphesizdir."[38]

Şeklindeki gerekçe, 4 Ekim 1988 yılında Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun Hükmünde Kararname ve İçişleri Komisyonu Raporu'nda (1/418) ifade edilerek Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun Hükmünde Kararname metni teklif edilmiştir.

3473 sayılı ve 28.09.1988 tarihli Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanun'da imha ile ilgili dikkat çekici bilgi mükellefiyet başlığı altında madde 3'te verilmiştir. Buna göre;

"Bu Kanun kapsamına giren ve elinde arşiv malzemesi ve arşivlik malzeme bulunduran kurum ve kuruluşlar, ellerinde bulundurdukları arşiv malzemesi ile arşivlik malzemeyi her türlü zararlı tesir ve unsurlardan korumak, aslî düzenlerine göre tasnif edip saklamak, yönetmelikte belirtilecek bekletme ve saklama süreleri sonunda Devlet

[38] "Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun Hükmünde Kararname ve İçişleri Komisyonu Raporu," Esas No: 1/418, Tarih: 04.04.1988, (Çevrimiçi) https://www.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d18/c014/tbmm18014005ss0073.pdf, 14 Haziran 2019.

Arşivleri Genel Müdürlüğüne teslim etmek ve muhafazasına lüzum kalmayan evrak ve malzemeyi yok etmekle mükelleftirler."[39]

Şeklindeki açıklama kurumların gereksiz olan evrakı yok etme sorumluluğunu taşıdığını göstermektedir.

- Devlet Arşiv Hizmetleri Hakkında Yönetmelik (19816 sayılı 16 Mayıs 1988 tarihli Resmi Gazete)

Bu yönetmeliğin ilk yayınlanma tarihinde imhanın nasıl yapılacağına dair Madde 39'da bilgiler verilmektedir.[40]

a) Kâğıt ham maddesi olarak kullanılmak üzere Türkiye Selüloz ve Kâğıt Fabrikaları Genel Müdürlüğüne (SEKA) gönderilmesi veya SEKA'nın yetkili mahallî kuruluşlarına teslim edilmesi suretiyle yerine getirilir.

Gizli evrak ve malzeme ile başkaları tarafından görülüp okunması mahzurlu olan malzemenin SEKA'ya verilmesi gerektiği takdirde, gönderilmeden önce özel makinelerle okunamayacak şekilde kıyılması şarttır. Mükellefler, bu hususun yerine getirilmesi için, kurum arşivleri emrine teknik teçhizat sağlarlar.

b) SEKA'ya gönderilmesi veya mahallinde özel makinelerle kıyılması mümkün olmayan yahut ekonomik görülmeyen malzeme, 2886 sayılı ihale Kanunu veya mükelleflerin kendi özel mevzuatlarına göre, sorumluluk taraflarına ait olmak üzere, kıyılmak kaydı ile özel şahıslara ihale edilebilir.

Yönetmelikte imha edilecek malzemenin öncelikle imha için yetkilendirilmiş kuruluşlara teslim edilmesi istenmektedir. Gizli olan malzemenin özel makinelerce okunmayacak şekilde kıyılması ve bu işlem için kurumlara gerekli teçhizatın sağlanması da belirtilmektedir. Söz konusu düzenleme imha işleminin kendi sorumluluğunda özel şahıslara ihale edilebileceğine de yer vermektedir. 1988 yılında hazırlanan bu yönetmelik, imhanın ne şekilde yapılacağına dair zorunlulukları dile getirmesi açısından imha teorisi için önemlidir.

Aynı yönetmeliğin 24487 sayılı 08.08.2001 tarihli değişiklik yapılmasına dair yönetmelikte yukarıda açıklanan Madde 39 değiştirilmiştir. Değişikliğe göre;[41]

---

[39] "3473 sayılı tarihli Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanun," **Resmi Gazete**, Sayı: 19949, Tarih: 04.10.1988 http://www.resmigazete.gov.tr/arsiv/19949.pdf, 14 Haziran 2019.

[40] "Devlet Arşiv Hizmetleri Hakkında Yönetmelik," **Resmi Gazete**, Sayı: 19816, Tarih: 16.05.1988, Madde 39, (Çevrimiçi) http://www.resmigazete.gov.tr/arsiv/19816.pdf, 13 Haziran 2019.

[41] "Devlet Arşiv Hizmetleri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik," **Resmi Gazete**, Sayı: 24487, Tarih: 08.08.2001, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2001/08/20010808.htm#6, 13 Haziran 2019.

"İmha edilecek malzeme, başkaları tarafından görülüp okunması mümkün olmayacak şekilde özel makinelerle kıyılarak, kağıt hammaddesi olarak kullanılmak üzere değerlendirilir. Özelliği gereği imha şekli kendi mevzuatında belirlenmiş malzemenin imhası hakkında ilgili mevzuat hükümleri uygulanır."

şeklindeki ifadeler yer almaktadır. Ayrıca elektronik ortamlarda kaydedilen arşiv malzemesi için ek madde konulmuştur. Bu ek maddeye göre;[42]

"Ek Madde 1 — Elektronik ortamlarda teşekkül eden bilgi ve belgelerden arşiv malzemesi özelliği taşıyanların kaybını önlemek ve devamlılığını sağlamak amacıyla bir kopyası cd, disket veya benzeri kayıt ortamlarına aktarılmak suretiyle muhafaza edilir. Bu tür malzemelerin muhafaza, tasnif, devir vb. arşiv işlemlerinde diğer tür malzemeler için uygulanan hükümler uygulanır."

Yönetmeliğin 25735 sayılı ve 22.02.2005 tarihli değişiklik düzenlemesinde kurumların kendi arşiv yönergelerini hazırlama hakkı verilmiştir. Hazırlanacak olan yönergelerin yönetmeliğe aykırı olmaması şartı aranmıştır.[43]

- Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi (Kararname Sayısı: 11, Resmi Gazete Tarih ve Sayısı: 16/7/2018-30480)

Söz konusu Cumhurbaşkanlığı Kararnamesi, Türkiye Büyük Millet Meclisi ve Milli İstihbarat Teşkilatı hariç olmak üzere devlet tüzel kişiliği ve kamu tüzel kişiliği olan tüm kurum ve kuruluşları vergi muafiyeti tanınan vakıfları ve kamu yararına çalışan dernekleri kapsamaktadır. Düzenlemede, Devlet Arşivleri Genel Müdürlüğü Cumhurbaşkanlığına bağlanmış ve ismi de Devlet Arşivleri Başkanlığı şeklinde değiştirilmiştir. Düzenlemenin Madde 5-g bendinde *"Kâğıt ve elektronik ortamda oluşturulan arşiv belgelerinin her türlü güvenliğine ilişkin önlemlerin alınmasını sağlayacak usul ve esasları belirlemek."* şeklinde Devlet Arşivleri Başkanlığının görevleri arasında elektronik ortamda oluşturulan arşiv belgelerinin güvenliği de gösterilmektedir. Madde 11'de ise Devlet Arşivleri Başkanlığı hizmet birimi olarak oluşturulmuş Bilgi

[42] "Devlet Arşiv Hizmetleri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik,".

[43] "Devlet Arşiv Hizmetleri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik," **Resmi Gazete**, Sayı: 25735, Tarih: 22.02.2005, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2005/02/20050222-8.htm, 13 Haziran 2019.

İşlem ve Elektronik Arşiv Dairesi Başkanlığının görevleri sıralanmaktadır. Bu görevler arasında;[44]

- Bilgi güvenliği politikası oluşturması,
- Bilişim teknolojisinin gelişimini izlemesi, bilgi işlem donanım ve yazılımlarının kullanılmasında diğer kamu kurum ve kuruluşlarıyla işbirliği yapması,
- Başkanlığa devredilecek elektronik ortamdaki arşiv belgelerinin devri hususunda usul ve esasları belirlemesi,
- Elektronik belge yönetimi ve arşivleme sistemleri uygulamalarında bulunması gerekli belge yönetimi ve temel arşivcilik fonksiyonlarını belirlemesi ve tanımlaması şeklinde birçok görevi sıralanmıştır.

Söz konusu görevler arasında imhanın açıkça ne şekilde olması gerektiği veya imha için gerekli yazılımları sağlaması noktasında vurgu yoktur. Ancak bilgi güvenliği politikasının oluşturulmasının istenmesi, teknolojik gelişmelerin takip edilmesi ve belge yönetimi ile arşivleme sistemlerindeki gerekli temel fonksiyonların belirlenmesinin istemesi, Bilgi İşlem ve Elektronik Arşiv Daire Başkanlığı'nın imhaya yönelik gelişmeleri takip etmesi, imha teorisinin teknolojik gelişmeler ışığında temel arşivcilik prensibi olarak belirlemesi ve bunu yasal düzenlemelere yansıtması beklenmektedir. Yine Madde 18'de Yükümlülük kısmında, kamu kurum ve kuruluşlarının saklanmasına gerek kalmayan belgeleri yok etmekle yükümlü olmalarının belirtilmesi, tüm kamu kurum ve kuruluşlar için elektronik belgenin nasıl yok edilmesi gerektiği tartışmasını da ortaya koymaktadır.

Bilgi İşlem ve Elektronik Arşiv Daire Başkanlığı'nın, 18 Ekim 2019 tarihinde yayımlanan Devlet Arşiv Hizmetleri Hakkında Yönetmelik'te de imhaya ilişkin alması gereken direktifler yer almamaktadır. İmhaya ilişkin yer alan kısımların da anlaşılmadığı görülmektedir. Nitekim Yönetmelik'te 17. maddenin dördüncü fıkrasında "*e-Ar-*

[44] "Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi-Kararname Sayısı 11," **Resmi Gazete**, Sayı: 30480, Tarih: 16.07.2018, Madde 11, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2018/07/20180716-1.pdf, 13 Haziran 2019.

şivlerde saklanan belgelerin tasfiye işlemleri, saklama planlarına bağlı olarak, bu Yönetmelik hükümleri kapsamında sistem üzerinden yapılır."[45] Şeklindeki hüküm ile 22. maddenin üçüncü fıkrasında "*e-Arşivlerde tutulan belgelerin imhası, görülüp okunması ve kullanılması mümkün olmayacak şekilde sistemden çıkarılarak tasfiye edilir."*[46] Şeklinde hüküm açıklanmıştır. Her iki fıkra karşılaştırıldığında tasfiye kavramı dikkat çekmektedir. Yönetmelik'teki tanımlar kısmında bu kavramın tanımı yapılmamıştır. Söz konusu yukarıdaki iki hüküm içinde ne anlama geldiği tam olarak anlaşılmamaktadır. Ayrıca, 17. maddede tasfiye (eğer maksat ayıklama ve imha ise) işlemlerinin sistem üzerinden yapılması gerektiği, 22. maddede ise imha şeklinin belgelerin sistemden çıkrılarak tasfiye (eğer maksat imha ise) edilmesi istenmektedir. Bu karmaşıklıkla beraber elektronik belgelerin veya elektronik arşivlerdeki imha yöntem ve teknikleri adına herhangi bir direktif yer almamaktadır. Kurumların hazırlayacakları yönergelerinde bunlara açık bir şekilde yer vermesi gerektiği de ifade edilmemiştir.

4.4.1. Kişisel Verileri Koruma Kurumunun (KVKK) Belge İmhasına Yönelik Düzenlemeleri

6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazetede yayımlanmasıyla Kanunda belirtilen görevleri yerine getirmek üzere, idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz Kişisel Verileri Koruma Kurumu kurulmuştur. Kişisel verilerin korunması için kanun çıkarılması ve kanunla beraber ilgili bir kurumun kurulmuş olması arşivcilik açısından da önemlidir. Özellikle bu tezin kapsamında değerlendirildiğinde kişisel verilerin arşivcilik imha teorisiyle düşünülmesi gerekir. Bu nedenle Kanundaki düzenlemeler ve ikincil mevzuatın bu açıdan değerlendirilmesi yerinde olacaktır. Kişisel Verileri Koruma Kanunu Madde 7'de kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi başlığı altında bilgiler verilmiştir. Bu bilgilere göre; mevzuata uygun olarak işlenmiş verinin, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler kendi-

[45] "Devlet Arşiv Hizmetleri HakkındaYönetmelik," Madde 17, **Resmi Gazete**, Sayı: 30922, Tarih: 18.10.2019, (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2019/10/20191018-9.pdf, 25 Ekim 2019.

[46] "Devlet Arşiv Hizmetleri HakkındaYönetmelik," Madde 22.

liğinden veya ilgili kişinin talebi üzerine sorumlu kişiler tarafından silinmesi, yok edilmesi veya anonim hâle getirilmesi istenmektedir. Ayrıca kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklı kalmak suretiyle uygulamaya ilişkin usul ve esasların yönetmelikle düzenlenmesi Kanunda yer almaktadır.

Kanunun 9 uncu maddesinde kişisel verilerin yurt dışına aktarılması için gerekli şartların sıralanması özellikle bulut teknolojisini kullanan gerçek ve tüzel kişilikleri yakından ilgilendirmektedir. 11 inci maddede ilgili kişinin hakları başlığı altında kişilerin, Kanunun 7 inci maddesi çerçevesinde kişisel verilerinin silinmesini veya yok edilmesini isteme hakları olduğunu ifade etmektedir. Kanunun 17 nci maddesinde Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenlerin 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılacağı beyan edilmektedir. Kişisel verilerle ilgili bu Kanundan önce yapılan işlemler için de Kanunun yayım tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilmesi, Kanun hükümlerine aykırı olduğu tespit edilen kişisel verilerin de derhâl silinmesi, yok edilmesi veya anonim hâle getirilmesinin istenmesi önemlidir.

30224 sayılı ve 28.10.2017 tarihli Resmi Gazete tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik, veriden sorumlu kişilerin öncelikle kişisel veri saklama imha politikası hazırlamaları noktasında yükümlü kılmıştır.[47] Kişisel veri saklama imha politikası kapsamında "*kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirler"* ibaresi de koyulmuştur. Yönetmeliğin 7 inci maddesinde veri sorumlusunun kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi işlemiyle ilgili uyguladığı yöntemleri ilgili politika ve prosedürlerinde açıklamakla yükümlü olduğu da açıklanmıştır. Yönetmeliğin 8 inci, 9 uncu ve 10 uncu maddelerine göre veri üç yöntemle imha edilmektedir. Bu yöntemler; verilerin silinmesi, verilerin yok edilmesi ve verilerin anonim hale getirilmesidir. Bu yöntemler aşağıda açıklanmıştır:

[47] "Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik," Madde 5, **Resmi Gazete**, Sayı: 30224, Tarih: 28.10.2017, (Çevrimiçi) Haziran 2019 tarihinde http://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm, 13 Haziran 2019.

Verilerin silinmesi: Bu yöntem kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Bu işlem için gerekli her türlü gerekli teknik ve idari tedbir alınmak zorundadır.

Verilerin yok edilmesi: Bu yöntem kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Bu işlem için de gerekli her türlü teknik ve idari tedbir alınmak zorundadır.

Verilerin anonim hale getirilmesi: Bu yöntem kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu ve diğer paydaşlar tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir. Yönetmeliğin 13 üncü maddesinde;

"*Bu Yönetmeliğin uygulanması sırasında doğacak tereddütleri ve uygulamaya ilişkin aksaklıkları gidermeye ve uygulamayı yönlendirmeye, ilke ve standartları belirlemeye ve uygulama birliğini sağlayacak gerekli düzenlemeleri yapmaya, bu hususta gerekli her türlü bilgi ve belgeyi istemeye, bu Yönetmelikte yer almayan konularda ilgili mevzuat hükümleri çerçevesinde karar vermeye Kurul yetkilidir."*[48]

Burada Kuruldan kasıt Kişisel Verileri Koruma Kuruludur. Aksakları gidermeye yönelik ilke ve standartları belirleme ve uygulama yetkisine sahip olan Kurul, kişisel elektronik belgelerin yazılımsal ve donanımsal olarak iz bırakmadan silinmesi için çeşitli standartları uygulama zorunluluğunu yerine getirme yetkisine sahip olması imha teorisi açısıdan anlamlıdır. Çünkü verinin geri getirilemez, tekrar kullanılamaz olması silinmiş veriye ait izlerin de yok edilmesini gerektirir. Bu konuda aksaklıkların ortaya çıkması haliyle Kurulun müdahalesini gerektirir. Bu müdahale yazılımsal ve donanımsal olarak imha edilmiş verinin tekrar erişimine engel olacak yazılımların sağlanmasıyla yapılabilir.

[48] "Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik," Tereddütlerin Giderilmesi, Madde 13.

Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmeliğe dayanılarak

söz konusu işlemlerin nasıl yapılacağı hakkında uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturması bakımından çeşitli konu başlıklarına dikkat çekmek amacıyla Kurul tarafından Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi ("Rehber") hazırlanmış ve kamuoyuna sunulmuştur.[49]

Rehberde kişisel verilerin silinme süreci şu şekilde ifade edilmiştir:[50]

- Silinmesi gerekli olan verinin belirlenmesi.
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi.
- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi.
- İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması.

Yukarıda da ifade edildiği gibi Kişisel Verileri Koruma Kanununda verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi olmak üzere üç yöntemden bahsedilmişti. Bunların Kişisel Verileri Koruma Kurumu tarafından hazırlanan rehber ile şekil bulduğu görülmektedir. Rehbere göre;

Verilerin silinmesi yönteminde verilerin sistem ve depolama alanlarından silinmesi için silme komutunun kullanılması gerektiği ifade edilmektedir.[51]

Verilerin yok edilmesi yönteminde belirlenen üç teknik bulunmaktadır. Bunlar; de-manyetize etme, üzerine yazma ve verinin bulunduğu ortamın fiziksel imhasıdır.[52]

Verilerin anonim hale getirilmesi yöntemi ise üçe ayrılmakta ve her üç yöntemin uyguladığı farklı teknikler bulunmaktadır. Bu üç yöntem ve uygulanan farklı teknikler şu şekildedir: [53]

[49] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Rehberi**, Ankara, 2018, s. 2.

[50] **A.g.r**., s. 6.

[51] **A.g.r**., s. 7-9.

[52] **A.g.r**., s. 9-13.

[53] Yöntem ve tekniklerin ayrıntılı açıklamaları için bkz. **A.g.r.**, s. 16-33.

Tablo 4.4: Verilerin Anonim Hale Getirilmesi Yöntemi

Değer düzensizliği sağlamayan yöntem	• Değişkenleri Çıkartma • Kayıtları Çıkartma • Bölgesel Gizleme • Genelleştirme • Alt ve Üst Sınır Kodlama • Global Kodlama • Örnekleme
Değer düzensizliği sağlayan yöntem	• Mikro Birleştirme • Veri Değiş Tokuşu • Gürültü Ekleme
Anonim hale getirmeyi kuvvetlendirici istatistiksel yöntem	• K-Anonimlik • L-Çeşitlilik • T-Yakınlık

(**Kaynak:** Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Rehberi, Ankara, 2018)

Kişisel Verileri Koruma Kurumunun Facebook nezdinde gerçekleşen veri ihlalinin değerlendirilmesi konusunda 11.04.2019 tarih ve 2019/104 sayılı Kararı da kurumun veri ihlali ile ilgili verdiği güncel bir bilgi olmasından dolayı burada ifade edilmesi önemlidir. Karar, Facebook API uygulamasının belirli tarihler arasında kullanıcı fotoğraflarına üçüncü taraflarca erişim izni veren sistem hatasının Kişisel Verileri Koruma Kuruluna bildirilmediği, sistem hatasının Facebook Mühendislik Direktörü Tomer Bar tarafından 14.12.2018 tarihinde yaptığı duyuruya dayanılarak mevzuatın ilgili maddeleri gereği 1.650.000 TL ceza kesilmiştir. Bu cezanın 1.100.000 TL veri ihlali, 550.000 TL ise kuruma bilgi verilmediği içindir.[54]

4.4.2. Kamu Kurum ve Kuruluşlarında Saklama Planları ve Belge İmhasına Yönelik Uygulamalar

Kamu kurum ve kuruluşlarında mevzuat gereği bilgi ve belgeler saklama planlarına tabi tutulur. Modern arşivcilik literatüründe, belgenin imha veya muhafazasına dair uygulamaları belirten tablolara /yönetmeliklere "saklama planı" denmektedir.[55]

[54] Kişisel Verileri Koruma Kurumu, "Facebook Nezdinde Gerçekleşen Veri İhlalinin Değerlendirilmesi ile ilgili Kişisel Verileri Koruma Kurulunun 11.04.2019 tarih ve 2019/104 Sayılı Kararı Özeti," (Çevrimiçi) https://www.kvkk.gov.tr/Icerik/5450/2019-104, 15 Haziran 2019.

[55] İshak Keskin,"Osmanlı Bürokrasisinde Evrak İmha Uygulamalarına Dair Gözlemler," s. 315.

Saklama planı, Uluslararası Arşiv Konseyi (International Council on Archives / ICA) tarafından hazırlanan ve pek çok dile çevrilen Arşivcilik Terimleri Sözlüğünde;[56]

"*bir kurumun evrakları içinde arşivsel değere sahip olmaları sebebiyle saklanması gerekenleri niteleyen ve saklanmayacak olanların belirli saklama sürelerinin geçmesi veya belirli olay yahut da eylemlerin gerçekleşmesinden sonra imhasına, sürekli bir esas çerçevesinde izin veren belge*"

şeklinde açıklanmaktadır. Saklama planları, arşivsel değerlendirmenin yapılabilmesi için arşivcilere ve belge yöneticilerine kolaylık sağlar. Bu kolaylık hangi belgenin süresiz olarak saklanacağını ve hangi belgenin imha edileceğini sağlamasıyla görülür. Saklama planları olmadan arşiv imha teorisinin uygulanması herhangi bir değer atfetmez. Kamu kurum ve kuruluşlarında saklama planlarının dolayısıyla arşiv imha teorisinin yer bulması yapılmış ve yapılacak hukuki düzenlemelere ihtiyaç duyar. Türkiye'de bu saklama planlarının bütün kamuda standart hale gelmesi için pek çok düzenleme bulunmaktadır. Bunlar;

- 3473 sayılı Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanun (Resmi Gazete, Sayı: 19949, Tarih: 04.10.1988, tekrar yürürlüğe giriş tarihi 09.07.2018)
- 4982 Sayılı Bilgi Edinme Hakkı Kanunu (Resmi Gazete, Sayı: 25269, Tarih: 24.10.2003)
- 5070 sayılı Elektronik İmza Kanunu (Resmi Gazete, Sayı: 25355, Tarih: 23.01.2004)
- 6698 sayılı Kişisel Verilerin Korunması Kanunu (Resmi Gazete, Sayı: 29677, Tarih: 07.04.2016)
- 6098 sayılı Türk Borçlar Kanunu (Resmi Gazete, Sayı: 27836, Tarih: 04.02.2011)
- 4734 sayılı Kamu İhale Kanunu (Resmi Gazete, Sayı: 24648, Tarih: 22.01.2002)

[56] **Arşivcilik Terimleri Sözlüğü**, Çev. ve Gnş. Bekir Kemal Ataman, İstanbul, Librairie de Péra, 1995, s. 94.

- 657 sayılı Devlet Memurları Kanunu (Resmi Gazete, Sayı: 12056, Tarih: 23.07.1965)
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu (Resmi Gazete, Sayı: 26200, Tarih: 16.06.2006)
- 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu (Resmi Gazete, Sayı: 25326, Tarih: 24.12.2003)
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu (Resmi Gazete, Sayı: 28339, Tarih: 30.06.2012)
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun (Resmi Gazete, Sayı: 18571, Tarih: 10.11.1984)
- 4857 sayılı İş Kanunu (Resmi Gazete, Sayı: 25134, Tarih: 10.06.2003)
- 2547 sayılı Yükseköğretim Kanunu (Resmi Gazete, Sayı: 17506, Tarih: 06.11.1981)
- 5434 sayılı Türkiye Cumhuriyeti Emekli Sandığı Kanunu (Resmi Gazete, Sayı: 7235, Tarih: 17.06.1949)
- 2828 sayılı Sosyal Hizmetler Kanunu (Resmi Gazete, Sayı: 18059, Tarih: 27.05.1983)
- Devlet Arşiv Hizmetleri Hakkında Yönetmelik (Resmi Gazete, Sayı: 30922, Tarih: 18.10.2019)
- Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik (Resmi Gazete, Sayı: 25692, Tarih: 06.01.2005)
- Bilgi Edinme Hakkı Kanununun Uygulanmasına İlişkin Esas Ve Usuller Hakkında Yönetmelik (Resmi Gazete, Sayı: 25445, Tarih: 27.04.2004)
- Tapu ve Kadastro Verilerinin Paylaşımı Hakkında Yönetmelik (Resmi Gazete, Sayı: 29288, Tarih: 07.03.2015)
- Kamu Hizmetlerinin Sunumunda Uyulacak Usul ve Esaslara İlişkin Yönetmelik (Resmi Gazete, Sayı: 15169, 27305, Tarih: 21.08.2009)
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkinYönetmelik (Resmi Gazete, Sayı: 28710, Tarih: 17.08.2013)
-

- Kayıtlı Elektronik Posta (KEP) Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik (Resmi Gazete, Sayı: 28036, Tarih: 25.09.2011)
- Kayıtlı Elektronik Posta (KEP) Sistemi İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (Resmi Gazete, Sayı: 28036, Tarih: 25.09.2011)
- Standart Dosya Planı (SDP) Genelgesi (Genelge Sayısı: 2005/7, Resmi Gazete, Sayı: 25766, Tarih: 25.03.2005)
- Elektronik Belge Standartları Genelgesi (Genelge Sayısı: 2008/16, Resmi Gazete, Sayı: 26938, Tarih: 16.08.2008)
- Kamu Bilgi Sistemlerinde Birlikte Çalışabilirlik Esasları Genelgesi (Genelge Sayısı: 2009/4, Resmi Gazete, Sayı: 27155, Tarih: 28.02.2009)

Yasal düzenlemeler tüm kamu kurum ve kuruluşlarına kendi arşiv yönergelerini hazırlamaları konusunda gerekli hukuki alt yapıyı sağlamıştır. Ayrıca 6698 sayılı Kişisel Verileri Koruma Kanunu da yine tüm kurum ve kuruluşlara kendi kişisel verileri saklama ve imha politikası hazırlamalarının zeminini oluşturmuştur. Bu yasal düzenlemelere rağmen birçok kurumun bu konularda tam işlevsellik sağlayamadıkları görülmektedir. Bu konunun izahı için verinin imhası için bir politikaya sahip olan kurumları açıklamak yerinde olacaktır.

4.4.2.1. Kişisel Verileri Koruma Kurumu

Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmeliğinin ikinci bölümü olan "kişisel veri saklama ve imha politikası"na ilişkin 5 inci ve 6 ıncı maddelerde veri sorumlularının kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamaları hükmü yer almaktadır. Hükme göre politikanın kapsamı şu şekilde ifade edilmektedir:

- Kişisel veri saklama ve imha politikasının hazırlanma amacına,
- Kişisel veri saklama ve imha politikası ile düzenlenen kayıt ortamlarına,
- Kişisel veri saklama ve imha politikasında yer verilen hukuki ve teknik terimlerin tanımlarının yapılmasına,
- Kişisel verilerin saklanmasını ve imhasını gerektiren hukuki, teknik ya da diğer sebeplere ilişkin açıklamaya,

- Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirlere,
- Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirlere,
- Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimlerine ve görev tanımlarına,
- Saklama ve imha sürelerini gösteren tabloya,
- Periyodik imha sürelerine,
- Mevcut kişisel veri saklama ve imha politikasında güncelleme yapılmış ise söz konusu değişikliğe ilişkin bilgileri kapsar.

Kişisel verileri koruma kanunun 16 ıncı maddesi gereği hazırlanacak kapsamı sıralanan imha politikası, veri sorumlulukları siciline kayıtlı tüm yükümlüler tarafından hazırlanmak zorundadır. Veri sorumluları siciline kayıtlı olmayan yükümlülerin imha politikası hazırlamasa da ilgili kanun ve yönetmeliğe uygun olarak kişisel verileri saklama, silme, yok etme veya anonim hale getirme yükümlülükleri devam eder.

Kişisel Verileri Koruma Kurumu da yasal zorunluluk gereği kendisi için kişisel verileri saklama ve imha politikası düzenlemiştir. Bu politikada kişisel verilerin saklandığı elektronik ve elektronik olmayan ortamlar tanımlanmıştır. Buna göre;[57]

Tablo 4.5: KVKK Kişisel Verilerin Saklandığı Elektronik ve Elektronik Olmayan Ortamlar

Elektronik Ortamlar	**Elektronik Olmayan Ortamlar**
1. Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) 2. Yazılımlar (ofis yazılımları, portal, EBYS, VERBİS.) 3. Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) 4. Kişisel bilgisayarlar (Masaüstü, dizüstü) 5. Mobil cihazlar (telefon, tablet vb.) 6. Optik diskler (CD, DVD vb.) 7. Çıkartılabilir bellekler (USB, HafızaKart vb.) 8. Yazıcı, tarayıcı, fotokopi makinesi	1. Kâğıt 2. Manuel veri kayıt sistemleri (anketformları, ziyaretçi giriş defteri) 3. Yazılı, basılı, görsel ortamlar

[57] Kişisel Verileri Koruma Kurumu, **Kişisel Veri Saklama ve İmha Politikası**, s. 8, (Çevrimiçi) https://www.kvkk.gov.tr/Icerik/5386/KVKK-KISISEL-VERI-SAKLAMA-ve-IMHA-POLITIKASI, 15 Haziran 2019.

(**Kaynak:** Kişisel Verileri Koruma Kurumu, Kişisel Veri Saklama ve İmha Politikası, s. 8, (Çevrimiçi) https://www.kvkk.gov.tr/Icerik/5386/KVKK-KISISEL-VERI-SAKLAMA-ve-IMHA-POLITIKASI, 15 Haziran 2019)

Şeklinde listelenmiştir. Bu verilerin silinmesi, yok edilmesi aşağıda ifade edilen imha teknikleriyle yapılmaktadır.[58]

Kişisel Verilerin Silinmesi,

Tablo 4.6: KVKK Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek / boyanarak / silinerek karartma işlemi de uygulanır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

(**Kaynak:** Kişisel Verileri Koruma Kurumu, Kişisel Veri Saklama ve İmha Politikası, s. 12-13)

Kişisel Verilerin Yok Edilmesi,

Tablo 4.7: KVKK Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi

[58] Kişisel Verileri Koruma Kurumu, **Kişisel Veri Saklama ve İmha Politikası**, s. 12-13.

	uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

(**Kaynak:** Kişisel Verileri Koruma Kurumu, Kişisel Veri Saklama ve İmha Politikası, s. 12-13)

4.4.2.2. Bağcılar Belediyesi

Bağcılar Belediyesinin kişisel veri saklama ve imha politikasında, verilerin bulunduğu elektronik ve fiziksel ortamları şu şekilde ifade edilmektedir:[59] Elektronik ortamlar için, exchange server, file server, beyaz MIS, AD DC, Yordam kütüphane sunucusu, ERBEN PDKS sunucusu, Antizan, EBYS-Oracle, Logsign, fortigate firewall, 3B internet sunucusu, BBLibrary kütüphane sunucusu, kariyer merkezi sunucusu olmak üzere 13 farklı ortam ifade edilmektedir.

Fiziksel ortamlar için de birim dolapları, insan kaynakları arşivi ve kurum arşivi olmak üzere 3 farklı yer gösterilmektedir. Bağcılar Belediyesinin bu farklı ortamlarda bulunan kişisel verilerin silinmesi ve yok edilmesi aşağıdaki yöntem ve tekniklerle ifade edilmiştir:[60]

Verilerin silinmesi,

Tablo 4.8: Bağcılar Belediyesi Kişisel Verilerin Silinmesi

	Veri Kayıt Ortamı	İmha Yöntemi	İmha Tekniği
Elektronik Ortamdaki Veriler	Exchange server, File server, Beyaz MIS, AD DC, Yordam kütüphane sunucusu, ERBEN PDKS sunucusu, Antizan, EBYS-Oracle, Logsign, fortigate firewall, 3B internet sunucusu, BBLibrary kütüphane sunucusu, kariyer merkezi sunucusu	Yazılımdan güvenli olarak silme	Erişime kapatma
	Exchange server, File server, Beyaz MIS, AD DC, Yordam kütüphane sunucusu, ERBEN PDKS sunucusu, Antizan, EBYS-	Uzman tarafından güvenli olarak silme	İlgili kullanıcıların erişimine kapatma

[59] Bağcılar Belediyesi, **Kişisel Veri Saklama ve İmha Politikası**, 2018, (Çevrimiçi) http://www.bagcilar.bel.tr/Files/Dokuman/kvk_2018/KVKVeriSaklamaveimhapolitikasi.pdf, 13 Kasım 2018.

[60] Bağcılar Belediyesi, **Kişisel Veri Saklama ve İmha Politikası**, s. 10-11.

	Oracle, Logsign, for-tigate firewall, 3B internet sunucusu, BBLibrary kütüphane sunucusu, kari-yer merkezi sunucusu		
Elektronik Olmayan Ortamdaki veriler	Birim dolapları, insan kaynakları arşivi, kurum arşivi	Verilerin karartılması	Fiziksel kesme, sabit mürekkep kullanılarak kapatılması

(**Kaynak:** Bağcılar Belediyesi, Kişisel Veri Saklama ve İmha Politikası, 2018, (Çevrimiçi) http://www.bagcilar.bel.tr/Files/Dokuman/kvk_2018/KVKVeriSaklamaveimhapolitikasi.pdf, 13 Kasım 2018)

Not: Başka herhangi bir kurum, kuruluş veyahut kişinin erişimine kapalı olması, kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması koşullarının sağlanması durumunda veriler silinmiş olarak kabul edilecek.

Verilerin yok edilmesi,

Tablo 4.9: Bağcılar Belediyesi Kişisel Verilerin Yok Edilmesi

	Veri Kayıt Ortamı	**İmha Yöntemi**	**İmha Tekniği**
Elektronik ortamdaki veriler	Manyetik	De-manyetize etme (de-manyetize olmazsa fiziksel imha yoluna gidilir)	Degausser araçları (Belirtilmemiş)
	Depolama aygıtları, flash diskler, hard diskler, floppy diskler	Fiziksel imha	Kıyılma, toz haline getirme
	Depolama aygıtları, flash diskler, hard diskler, floppy diskler	Üzerine yazma	Özel yazılımlar aracılığı ile manyetik medya ve yeniden yazılabilir optik medya üzerinden en az yedi kez 0 ve 1'lerden oluşan rastsal veriler yazılarak yok etme

Elektronik olmayan ortamdaki veriler	Kağıt, mikrofiş	Fiziksel imha	Belirtilmemiş

(**Kaynak:** Bağcılar Belediyesi, Kişisel Veri Saklama ve İmha Politikası, s. 10-11)

Kişisel Verileri Koruma Kurumu ve Bağcılar Belediyesinin veri saklama ve imha politikaları ayrıntılı olarak yukarıda verilmiştir. Bu kurumlar haricinde Doğuş Üniversitesi kişisel veri saklama ve imha politikası[61], Dudullu Organize Sanayi Bölgesi Boğaziçi Üniversitesi Teknopark A.Ş. kişisel verilerin korunması politikası[62] İstanbul Teknik Üniversitesi Arı Teknokent Proje Geliştirme Planlama A.Ş kişisel verilerin korunması politikası[63] gibi kamu tüzel kişiliğine ve özel hukuk tüzel kişiliğe sahip birçok kurumun kişisel verileri saklama ve imha politikası bulunmaktadır. Bu politikalarda geçen imha yöntem ve teknikler, Kişisel Verileri Koruma Kurumunun hazırladığı kişisel veri güvenliği rehberi[64] ve kişisel verileri saklama ve imha politikasında ifade edildiği şekliyle hazırlanmıştır.

4.4.3. Kayıtlı Elektronik Posta (KEP) Uygulamaları ve İmha

Kayıtlı Elektronik Posta (KEP), "*elektronik iletilerin, gönderimi ve teslimatı da dâhil olmak üzere kullanımına ilişkin olarak hukukî delil sağlayan, elektronik postanın nitelikli şeklini*" [65] olarak ifade edilmektedir. KEP ile ilgili yönetmelikte imhayı ilgilendiren durumlar şu maddelerde belirtilmektedir:

[61] Doğuş Üniversitesi, **Kişisel Veri Saklama ve İmha Politikası**, (Çevrimiçi) https://www.dogus.edu.tr/docs/default-source/dokumanlar/ki%C5%9Fisel-verileri-saklama-ve-imha-politikas%C4%B1.pdf?sfvrsn=79ec4bf8_0, 21 Haziran 2019.

[62] Dudullu OSB Boğaziçi Üniversitesi Teknopark A.Ş., **Kişisel Verilerin Korunması Politikası,** (Çevrimiçi) http://www.budotek.com.tr/wp-content/uploads/2019/02/kisisel.pdf, 21 Haziran 2019

[63]İstanbul Teknik Üniversitesi Arı Teknokent Proje Geliştirme Planlama A.Ş., **Kişisel Verilerin Korunması Politikası**, (Çevrimiçi) http://www.ariteknokent.com.tr/tr/hakkinda/kisisel-verilerin-korunmasi-kanunu, 21 Haziran 2019.

[64] Kişisel Verileri Koruma Kurumu, **Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)**, Ankara, 2018, (Çevrimiçi) 21 https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf, 21 Haziran 2019.

[65] "Kayıtlı Elektronik Posta (KEP) Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik," **Resmi Gazete**, Sayı: 28036, Tarih: 25.08.2011, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2011/08/20110825-7.htm, 21 Haziran 2019.

13 üncü maddenin 6. kısmında kullanıma kapatılan KEP hesaplarına ilişkin bütün bilgi, belge ve diğer delillerin saklama süreleri boyunca güvenliği ve bütünlüğünün sağlanması istenmektedir. Saklama süreleri imha teorisinin varlığını da gösterdiğinden saklama süreleri sonunda elde tutulan verinin ne kadar süre ile saklanacağı, yine yönetmeliğin 16 ıncı maddesinin (ı) bendinde ifade edildiği üzere 20 yıl olarak belirlenmiştir. 20 yılın sonunda verinin imha edilmesiyle ilgili herhangi bir ifade yer almazken, KEP hizmetini sağlayan Kayıtlı Elektronik Posta Hizmet Sağlayıcılarının (KEPHS) faaliyetlerine son vermesi durumunda verinin nasıl bir işleme tabi tutulacağı belirtilmektedir. Buna göre faaliyetine son veren KEPHS elindeki tüm verileri, varsa devir yapılan başka bir KEPHS firmasına teslim eder. Böyle bir durumda devreden KEPSH elindeki tüm veriyi erişime kapatıp imha etmekle mükelleftir. Devir yapılacak KEPHS yoksa mevcut KEPHS elindeki verinin tamamını imha eder ve KEP süreç ve işleyişleriyle ilgili kayıtları 20 yıl süreyle saklar. Burada geçen verinin imhası yedek veriyi de kapsayacak şekilde uygulanması şeklinde beyan edilmiştir. Yine verinin bulunduğu ana ve yedek sistemlerin Türkiye sınırları içerisinde bulundurma zorunluluğu da vardır.

KEP ile ilgili hazırlanan Kayıtlı Elektronik Posta Sistemi İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğin 5 inci maddesinde KEPHS'lerin, işleyişinin bütün aşamalarında Avrupa Telekomünikasyon Standartları Enstitüsünün (European Telecommunications Standards Institute- ETSI TS 102 640) standardına uymaları hükmü söz konusudur. Bu tezi ilgilendiren kısmıyla söz konusu standartta imha ile ilgili bilgi güvenliği gerekliliklerinin 12 inci maddesine ilişkin notta Güvenli silme ile, en son teknolojiye dayalı olarak, silinen verilerin kurtarılamayacağını garanti eden bir prosedür amaçlanmaktadır.[66] şeklinde açıklama yer almaktadır.

[66] European Telecommunications Standards Institute, **ETSI TS 102 640-4 V2.1.1 (2010-01)**: **Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Part 4: REM-MD Conformance Profiles**, s. 11, (Çevrimiçi) https://www.etsi.org/deliver/etsi_ts/102600_102699/10264004/02.01.01_60/ts_10264004v020101p.pdf, 20 Haziran 2019.

4.4.4. Kamu Kurum ve Kuruluşlarının Arşiv Yönetmeliklerinde Veya Yönergelerinde İmhaya İlişkin Yaklaşımlar

Kamu kurum ve kuruluşları arşiv yönetmeliklerini, 16 Mayıs 1988 tarihli ve 19816 sayılı Devlet Arşiv Hizmetleri* yönetmeliğinde geçen 45 inci maddede ifade edilen

"*Mükellefler, Genel Müdürlüğe teslim etmedikleri arşiv malzemesi ile arşivlik malzeme hakkında, kuruluşlarının ve ellerindeki bu tür malzemenin özelliklerini gözönünde bulundurarak, arşiv hizmet ve faaliyetlerini düzenlemek ve yürütmek, tasnif usul ve esaslarını göstermek üzere, Başbakanlığın görüşünü almak suretiyle 6 ay içerisinde kendi yönetmeliklerini yayımlarlar.*"[67] hükmüne göre kendileri hazırlamaktadırlar.

Kamu kurumları yönetmelik maddesine dayanarak 2005 yılına kadar kendi yönetmeliklerini hazırlayabiliyorlardı. Aynı yönetmelikte, yukarıda ifade edilen 45 inci madde başlığıyla beraber değiştirildi.[68] Değişikliğe göre mükelleflerden kendi arşiv yönetmeliği yerine yönerge hazırlamaları ve bunu 3 ay içinde yapmaları istendi. Mart 2005'ten itibaren kamu kurum ve kuruşları kendi arşiv yönergelerini 2018 yılına kadar hazırlamış oldular. Belirli bir tarihe kadar yönetmelik daha sonraları ise yönerge hazırlama zorunluğu kurumlara getirilmiş oldu. Marmara Üniversitesi Kurumsal Belge Yönetimi Yönergesi'nin[69] 26 ıncı maddesinde " *EBSY'de dokümanlar üzerinde silme işlemi, ilgili veya yetkili kişi tarafından yapılabilir. Paraf ve/veya imza sürecinden geçmiş belgelerde silme işlemi yapılamaz. Bu belgeler iptal edilir.*" Elektronik belge yönetim sisteminde belgelerin silinmeyeceği ifade edilmektedir. EBYS için uygulanan TS 13298 standardının 2015 yılındaki versiyonunda belge yönetim sürecine arşiv modülü de eklenmiştir. Söz konusu standart 23 Ekim 2015 tarihinde karara bağlandığı

---

* Bu yönetmelik 18 Ekim 2019 tarihinde yayımlanan Devlet Arşiv Hizmetleri Hakkında Yönetmelik ile yürürlükten kaldırılmıştır. Yeni yönetmeliğe göre, kurumların kendi arşiv yönergelerini ve yönetmeliklerini 6 ay içerisinde kaldırmak suretiyle kendi arşiv yönerglerini hazırlamalrı istenmiştir ("Devlet Arşiv Hizmetleri HakkındaYönetmelik," **Resmi Gazete**, Madde: 32-33, Sayı: 30922, Tarih: 18.10.2019, (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2019/10/20191018-9.pdf, 25 Ekim 2019).

[67] "Devlet Arşiv Hizmetleri Hakkında Yönetmelik," Madde 45, **Resmi Gazete**, Sayı: 19816, Tarih: 16.05.1988, (Çevrimiçi) http://www.resmigazete.gov.tr/arsiv/19816.pdf, 13 Haziran 2019.

[68] "Devlet Arşiv Hizmetleri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik," **Resmi Gazete**, Sayı: 25735, Tarih: 22.02.2005, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2005/02/20050222-8.htm, 21 Haziran 2019.

[69] "Marmara Üniversitesi Kurumsal Belge Yönetimi Yönergesi," Sayı: 337-3-C, Tarih: 28.07.2015, (Çevrimiçi) http://dosya.marmara.edu.tr/www/mevzuat/yeni4/mu_kurumsal_belge_yonetimi_yonergesi_senato_web_versiyonu.pdf, 21 Haziran 2019.

için bu yönergenin yayınlanmasından sonra son şeklini bulmuştur. Bu yönerge muhtemelen standardın 2009 versiyonuna göre hazırlandığı için arşiv modülü üzerinde düşünülmemiştir.

Ankara Üniversitesi ve Türksat Uydu Haberleşme Kablo Tv ve İşletme A.Ş. arasında yapılan protokolle yapılan e-BEYAS (Elektronik Belge Yönetimi ve Arşivleme Sistemi) projesinin arşiv imha teorisi açısından değerlendirilmesi örnek projelerden olması sebebiyle önemlidir. Ankara Üniversitesinin yapacağı tüm yazışmalar 16 Eylül 2013 tarihinde e-BEYAS uygulaması üzerinden yapılmaya başlanmıştır.[70] Yaklaşık olarak 6 yıldır uygulanmaktadır. İlk faz olarak 2007-2009 yılları arası TÜBİTAK destekli bir proje olarak başlatılmış, daha sonra 2011-2012 yılları arası yine TÜBİTAK destekli bir diğer projeyle gelişim evresini tamamlamıştır. Son olarak da TÜRKSAT A.Ş. ile yapılan 2 yıllık işbirliği çerçevesinde 2013 yılında fiilen uygulanmaya başlamıştır. Söz konusu projenin arşiv yönergesi erişime kapalı olduğundan elektronik imhayla ilgili değerlendirme yapılamamıştır.

4.5. KURUMLARIN ARŞİVSEL İMHAYA YÖNELİK ALGISI

Kamu kurumlarında üretilen belgeler, hukuki, mali ve kültürel değerlere sahiptir. Belgelerin bu üç özelliğini taşımayanlar, saklama sürelerini doldurmuşlarsa arşivsel değerlendirmeye tabi tutulabilirler. Bu değerlendirme sonucunda imha edilecek belgelere uygulanan işlemler kayıt altına alınır. Arşivciler ve belge yöneticileri bu arşivsel değerlendirmeyi arşivcilik ilkeleri doğrultusunda yaparlar.

Kamu kurumlarında belge üretim sorumluluğu verilen kişiler, belge üretimi sonrası bu belgelerin muhafaza edilmesi, arşiv malzemesinin ve arşivlik malzemenin devredilmesi gibi süreçlere ilişkin bilgiye sahip olmayabilir. Devredilen malzemeler dışında muhafazasına gerek kalmayan belgenin hangi işlemlere tabi tutulacağı konusu da aynı şekilde belirsiz olabilir veya kişiler bu konuyla ilgili bilgi sahibi olmayabilir. Özellikle konu arşiv imha teorisi ise bu belge üretim sorumluluğuna sahip kişiler biraz daha çekimser davranabilir. Belgelerin yok edilmesi, belge üretim sorumluluğundaki

[70] Ankara Üniversitesi, "e-BEYAS Uygulama Kuralları," (Çevrimiçi) http://beyas.ankara.edu.tr/uygulama-kurallari/, 22 Haziran 2019.

kişilerce imha teorisi çerçevesinde tanımlanmamışsa belge imhasının önemi anlaşılamaz. Bir diğer ifadeyle yok etmenin olumsuz anlamı hissedilir ve belgenin imhası söz konusu olduğunda bu olumsuz anlam kendini daha fazla gösterir. Böyle bir durumda imhanın gerekçesi veya dayandığı yasal düzenlemeler de o anda düşünülmez. Hatta bu konuyla ilgili yasal düzenlemelerin hazırlık aşamasında dahi imha etmenin olumsuz düşüncesi varlığını korur. Bütün bunlar nedeniyle imha teorisine ilişkin düzenlemeler daha yumuşak bir yaklaşımla değerlendirilir.

Kamuda yapılan faaliyetler yasalara dayalı olma ve aykırı olmama ilkeleriyle yapılır. Kamu kurumlarındaki belge üretim sorumluluğundaki kişilerin imhaya bakışı, imhaya ilişkin mevzuatın varlığını bilmemesinden dolayı olumsuz olabilir. İmha mevzuatı tanımlanmadan sorumlu kişilerce imha edilmesi gereken malzemeye dokunulmazlık kimliği verilir. Kâğıt ortamdaki belgelere karşı algı bu şekilde olabilir. Kâğıt malzeme yanında elektronik ortamdaki belgeler de sorumlu kişilerce farklı algılanabilir.

Gelişen bilgi teknolojilerinin elektronik belge yönetim sistemlerindeki belge üretimi dokunulmaz kimliği düşüncesini kâğıt ortama göre biraz daha değiştirmiştir. Hata sonucu oluşan belgenin sebep olduğu tekrar oluşturma güçlüğü, elektronik ortamdaki belgelerle birlikte ortadan kalkmıştır. Elektronik belgenin belge üretim sorumluluğundaki kişilere bu katkısı yanında arşiv imha teorisi açısından olumsuz bir etkisi de söz konusudur. Çünkü elektronik ortamdaki belge üretim sorumluğu kâğıt ortamdaki gibi belgeyle muhatap olmayı, belgeye dokunmayı, ilgili dosyaya koymayı fiziksel anlamda gerektirmemektedir. Ancak bu rahatlık belge üretimini daha da tetiklemektedir. Dolayısıyla imha edilmesi gereken belgenin sayısını artırmaktadır.

Belge üretim sorumluluğu olan kişilerin arşiv imha teorisini hem hukuki dayanak hem de pratikteki kolaylığı açısından, yapılacak bilinçlendirme programlarıyla gereksiz olanın imha edilmesi hazzını yaşatmak açısından önemlidir. Ayrıca elektronik belgenin üretimini artırmamak için elektronik ortamdaki belgelerin imha edilmesinin kâğıt ortamda olduğu gibi rahat olmayacağını anlatmak, belge üretimindeki hata sonucu oluşan fazla belgelerin varlığını azaltabilir. İmhaya ilişkin pratik uygulama alışkanlıklarının ve yeteneklerin geliştirilmesi belge üretim sorumluluğundaki kişilerce kazanılabilir. Bu noktada kurumları ve kişileri bağlayıcı yasal düzenlemelerin varlığı

konusunun tartışılması önemlidir. Yukarıda ifade edildiği üzere kamu faaliyetlerinin yürütülmesi yasalara dayalı olma ve aykırı olmama ilkelerine bağlıdır. Türkiye'de arşivsel iş ve işlemler, ilgili bazı kanun maddelerine ve ikincil düzenlemelerle sağlanmaya çalışılmaktadır. Hem kurumları hem de kişileri bağlayıcı bir "*arşiv kanunun olmayışı, belgelerin üretiminden düzenlenmesine, devrinden korunmasına ve erişimine kadar arşivcilikle ilgili olan bütün uygulama alanlarında olumsuzlukların yaşanmasına yol açabilmektedir*."[71] Belge üretim sorumluluğundaki kurum ve kişilerin algısında arşiv kanunun olmayışı da büyük etki yapmaktadır. Bu etki imha teorisinin uygulamasını da olumsuz etkilemektedir.

[71] İshak Keskin, **Arşiv Kanunlarının Anatomisi**. İstanbul, Yeditepe Yayınevi, 2016, s. 19-20.

BEŞİNCİ BÖLÜM

ELEKTRONİK BELGENİN (SANAL NESNENİN) İMHASINA YÖNELİK YÖNTEM VE TEKNİKLER

5.1. ELEKTRONİK BELGELER VE İMHA

Kullanım dışı kalmış/güncelliğini yitirmiş belgelerin imha edilmesi, güvenilir ve etkili bir belge yönetim sisteminin sürdürülmesinde önemli bir adımdır. Güncel olmayan belgelerin tutulması sadece kafa karışıklığı yaratır ve personelin hangi belgelerin idari olarak önemli olduğunu ve hangi belgelerin iş için gerekli olduğunu bilmelerini zorlaştırır. Bu nedenle kullanım dışı kalmış/güncelliğini yitirmiş belgelerin imha edilmesi gereklidir. Söz konusu belgelerin imha edilmesinin gerekçesini ve önemini şu şekilde ifade edebiliriz:[1]

- Resmi belge yönetim sistemlerinin güvenilir ve verimli olmasını sağlamak,
- Bakım ve depolama maliyetlerini azaltmak,
- İmha kararlarının uygulanmasında hesap verilebilirliği ve tutarlılığı göstermek,
- İstenmeyen belgeleri imha ederek, kâğıt ve elektronik belge yönetim sistemlerinin verimliliğini artırmak ve
- Hassas veya kişisel bilgilerin yanlış ellere geçme riskini azaltmaktır.

Belgelerin imha edilmesinin önemi yanında imhanın hangi temel ilkelere dayanması gerektiğini de ifade etmek gerekir. Bu ilkeler aşağıdaki başlık altında verilmiştir.

5.1.1. İmhanın Temel İlkeleri

Belge imhası, basit, sıradan ve işlemsel bir uygulama olarak görülmemelidir. İmhanın kendine has özellikleri vardır. Bu özellikler, imhanın temel ilkeleri olarak da görülebilir. Bu ilkeler dört şekilde karşımıza çıkar. Bunlar;[2]

[1] United Nations Archives and Records Management Section, **Records and Information Management Guidance**, [t.y.], (Çevrimiçi) https://archives.un.org/sites/archives.un.org/files/5-guidance_destroying_records.pdf, 13 Ekim 2016.

[2] New South Wales Government, "State Archives and Records," (Çevrimiçi) https://www.records.nsw.gov.au/recordkeeping/advice/retention-and-disposal/destruction-of-records, 07.12.2017;

- İmhanın yetkili kişilerce yapılıyor olması,
- Yapılan imhanın mevzuata veya prosedüre uygun olması,
- İmhanın uygulamasının güvenli ve gizli olarak yapılması,
- İmha işleminin, saklama planlarına bağlı olarak belirli bir zaman içinde ve geciktirilmeden yapılması ve
- İmha edilen malzemelerin veya varlıkların imha kayıtlarının belgelenmiş olmalarıdır.

Bu ilkelerden yetkili, uygun ve güvenli/gizli olanları, yapılması planlanan imha uygulamasının sağlıklı bir şekilde gerçekleştirildiğini gösterir. Resmi olarak saklama süresi dolmuşsa ve özellikle hassas bilgileri içeriyorsa imhanın mümkün olan en kısa süre içinde gerçekleştirilmesi tavsiye edilmektedir.[3] Söz konusu ilkeler -imha edilecek belgelerin bulunduğu ortama bakılmaksızın- hem kâğıt ortam için hem de elektronik ortam için geçerlidir. Özellikle elektronik ortamda, bilgi kalitesini koruyabilmek için düzenli ve sistemli olarak veriyi imha etmek kaçınılmaz bir zorunluluktur. Geleneksel olarak, kullanım ömrü dolmuş bilginin sistemli bir şekilde ayıklanıp imha edilmesinden sorumlu arşivcilerin ve belge yöneticilerinin, gelecekte bu türden imha etme görevlerini de üstlenmeleri hiç uzak bir ihtimal gibi görünmemektedir.[4] Nitekim günümüzde elektronik belge yönetim sistemlerinin yaygınlaşması ve buna bağlı olarak elektronik belgelerin çoğalması, güvenilir ve doğru bilginin doğru kişilerce yönetilmesi, arşivcilerin ve belge yöneticilerinin elektronik ortamdaki imhaya yönelik çalışmaları ortaya koymalarını zorunlu kılmıştır. Çünkü elektronik ortamdaki bilgilerin ve belgelerin silinmesi nihayetinde elektronik kaydın tamamen imha edilmesi anlamına gelmelidir (ve bu durum fiziksel kayıtların güvenli bir şekilde elden çıkarılmanın elektronik eş değeridir). Bu uygulama, aynı zamanda adli veri kurtarma tekniklerini kullanarak bile belgelerin kurtarılamaz hale getirildiği anlamına da gelmektedir.

Queensland Police Service, **Records Retention and Disposal Handbook,V.2.1**, 2004, s. 20, (Çevrimiçi) https://www.police.qld.gov.au/rti/published/policies/Documents/QPS%20Records%20Retention%20and%20Disposal%20Handbook%20v21.pdf, 7 Aralık 2017.

[3] U.K. Centre for the Protection of National Infrastructure (CPNI Standard), **Secure Destruction Of Sensitive Items**, 2014, s. 11, (Çevrimiçi) https://www.cpni.gov.uk/system/files/documents/c5/e1/2017_01_20_CPNI_Secure_Destruction_Standard.pdf, 7 Mart 2019.

[4] Bekir Kemal Ataman, "Enformasyon Bilimlerine Fütüristik Bir Yaklaşım," **Bilgi Dünyası**, C. 9, S. 1, 2008, s. 81.

Uygulamada, çoğu teknik ortamda bir elektronik kaydın bir örneğinin silinmesi, yalnızca bir işletim sistemini veya nesneye uygulama bağlantısını kaldırır ve aynı depolama ortamı alanı birkaç kez yeniden kullanıldığında gerçekte silinen veri kaldırılmamış olur. Bilgilerin normal yöntemlerle alınamayacağından emin olmak için tedbir amaçlı adımlar atılmalıdır. Bu adımlar, yedekleme sistemlerinin de imha kararlarına dâhil edilmesiyle beraber elektronik belge yönetimi sistemi içindeki her iki işlevselliği (işletim sisteminden silinme ve nesneye uygulama bağlantısınının silinmesi) de içeren her türlü etkili kopya kontrolünü kapsamalıdır. Sistemde saklanılan veya orada belgelerin saklanılmasını haklı çıkarmak için çok geçici olan bilgilerin, hızlı oluşturulmuş istemci, kişisel veya ağ sürücüsünden silinmesini sağlamak için bunlara yönelik prosedürlerin var olmasını sağlamak gerekir. Buna yönelik, ABD Savunma Bakanlığı (DoD) elektronik belge yönetim sistemi (ERMS) gereksiniminde imha edilmesi gereken içeriğin üzerine beş defa yazılmasını ön görmektedir. Hatta bu üzerine yazma işleminin yedi defa olmasını da tavsiye etmektedir. ABD'deki bu duruma rağmen İngiltere'de, ERMS gereklilikleri 2002 revizyonunda üzerine yazma işleminden bahsedilmemektedir. Çünkü İngiltere hükümeti üzerine yazma işlemini yüksek güvenlikli bir ortamdaki veriler için gerekli görmektedir. Bunun yanında güvenlik standartları açısından üzerine yazma işlemine sıcak bakılmaktadır.[5]

Üzerine yazma işleminin nasıl yapılması gerektiği ve hangi araçların kullanılacağı bundan sonraki başlıkta ayrıntısıyla yer bulmaktadır. Bundan sonraki iki başlık elektronik ortama bağlı olarak şekillenmiştir. Çünkü teknoloji gün geçtikçe gelişmekte, geride kalan teknolojik ürünler için de eskime gerçekleşmektedir. Bu sebeple teknolojiyi elektronik belgeye yönelik imha yöntemleri güncel ortamda bulunan ve güncelliğini yitirmiş ortamda bulunan elektronik belgeler olmak üzere iki şekilde düşünülmüştür.

[5] The National Archives of United Kingdom (TNA), **Disposal Scheduling**, 2012, s. 20-21, (Çevrimiçi) http://www.nationalarchives.gov.uk/documents/information-management/sched_disposal.pdf, 11 Mayıs 2016.

5.1.2. Güncel Ortamda Bulunan Elektronik Belgeye Yönelik İmha Yöntemleri ve Teknikleri

Modern elektronik veri depolama cihazları son derece dirençlidir. Buna bağlı olarak veri kurtarma teknikleri ve teknolojisi de oldukça ileri düzeydedir. Veri kurtarma teknikleri rutin olarak yakılmış, ezilmiş, suya batırılmış veya yüksekten düşmekle etkilenmiş ortamlardan veri elde edebilmektedir. Bu nedenle verilerden kalıcı olarak kurtulmak oldukça zordur. Verilerin kalıcı ve geri dönüşü olmayacak şekilde imha edilmesi, kurum ve kişilere ait belgelerin gizliliğini ve güvenliğini korumanın temel gerekliliğidir. Veri imhası, her iki ortam (elektronik ve kâğıt) dâhil olmak üzere çok çeşitlidir. İmha metodolojisi seçimi, imha edilen verilerin hassasiyeti ve yetkisiz ifşa edilmenin olası etkisine bağlı olarak ortaya çıkacak riske dayanmalıdır.[6] Uygun imha yönteminin seçilmesi olası risklerin azaltılmasına yardımcı olacaktır.

Dosyalar silindiğinde bilgilerin imha edildiği yaygın bir inançtır, ancak normalde silinenlerin tümü bilginin mantıksal işaretçileridir. Dosyaları silmek hatta sabit sürücüleri biçimlendirmek, yaygın olarak kullanılan uygulamaları kullanarak bu bilgilerin gelecekte kurtarılmasını ve kullanılmasını engellemez. Elektronik ortama yönelik temizleme işlemi, verilerin bilgi teknolojisi ekipmanından ve depolama ortamından çıkarıldığı ve kurtarılamaz hale getirildiği işlemdir. Genel olarak, laboratuvar teknikleri temizlenmiş verileri kurtaramaz. Aşağıdaki *5.1.2.1. Güncel Ortamın İmhası İçin Kullanılan Yöntem ve Teknikler* bölümü, verileri depolama ortamından çıkarmak için kabul edilebilir yöntemleri özetlemektedir. Bir bilgisayar kullanılmıyorsa veya bir birim içindeki yeni bir kullanıcıya veriliyorsa, bilgilerin sabit sürücüden kurtarılamayacağına dair güvence verecek şekilde kaldırılmasını sağlamak için temizlik yapılmalıdır. Temizlik işlemine başlamadan önce, ağ işletim sistemine veya ağdaki diğer dosyalara yanlışlıkla zarar vermemek için bilgisayarın herhangi bir ağla bağlantısının kesilmesi gereklidir.[7]

---

[6] U.S. Department of Education, Privacy Technical Assistance Center, **Best Practices for Data Destruction**, 2019, s. 8, (Çevrimiçi) https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282019-3-26%29.pdf, 22 Eylül 2019.

[7] Kentucky Department for Libraries and Archives Public Records Division, **Destruction of Public Records: A Procedural Guide**, 2007, s. 12, (Çevrimiçi) https://kdla.ky.gov/records/Documents/Destruction%20Guidelines.pdf, 28 Aralık 2017.

Bir kamu kurum ve kuruluşuna ait belgelerin imhası, kurumsal belge yönetim sistemindeki üstverilerde açıkça belgelenmeli ve tutulmalıdır. Ayrıca, bu tür bir imha bildiriminin, hangi belgelere yönelik olduğunun yetkili idareye (örneğin Devlet Arşivleri Başkanlığına) iletilmesi gerekir. Basılı kopyaların imha edilmesi nispeten kolay olsa da, elektronik belgelerin imha edilmesi de benzer şekilde garanti edilmelidir. İmha edilecek elektronik bir belge yazılım ve donanım üzerinde bulunan tüm kopyalarıyla beraber düşünülmelidir. Kurum ve kuruluşların yedekleme uygulamalarının bir parçası olarak tutulan kopyalar da silinmelidir. Çünkü bu kopyalar, silinmiş belgelerin daha sonra ibraz edilmesine neden olabilir.[8]

Elektronik belgelerin imhası kâğıt ortama göre çok daha karmaşıktır. Bu belgelerin bir bilgisayar dizininden silinmesi, söz konusu belgelerin imhası için yeterli değildir. Elektronik belgelerle ilgili bileşenleri ve üstverileri tanımlamak ve bunları imha etmek de gerekli olabilir. Bu tahribatın gerçekleştirilmesi için teknik uzmanlık yanında imha sürecinin denetim izini sürdürmek de gereklidir. Farklı organizasyonlarda mevcut olan teknoloji değişmekle birlikte, imhanın genel ilkesi aynı kalır: Verilerin makul çabalarla geri kazanılmaması için her türlü çaba gösterilmelidir. Bilginin güvenliği veya hassasiyeti, neyin "makul" olduğunu belirlemek için kullanılmalıdır. İmha edilen belgelerin ve imha edilme araçlarının bir tanımını içeren belgeler, imha etme eyleminin kanıtı olarak saklanmalıdır.[9]

Elektronik belgelerin imhasını, arşivcilik ve belge yönetimi literatürüne göre değerlendirdiğimizde imha kavramı belgelerin geri dönüşü olmayacak şekilde imha edilmesi anlamına gelmektedir.[10] Bu açıdan silinmiş belgeler, geri dönüşü olmayacak şekilde silinmeli veya yok edilmelidir. Elektronik ortamı, silinme ve yok etme açısından değerlendirdiğimizde, ortam silinebilir ve yeniden kullanılabilir bir özelliğe sahiptir. Elektronik ortamın silinmesi, bu ortamın tekrar kullanılmasının yolunu açmaktadır.

---

[8] Northern Territory Government of Australia, Department of Corporate and Information Services, **Standard 5- Disposal**, [t.y.], s. 2, (Çevrimiçi) http://www.nt.gov.au/dcis/info_tech/records_policy_standards/records_management_standards/standard5_disposal.shtml, 7 Aralık 2017.

[9] International Records Management Trust, **Modul-3: Managing the Creation, Use and Disposal Of Electronic Records**, Ed. Laura Millar, London, 2009, s. 47.

[10] United Kingdom National Offender Management Services, **Archiving, Retention and Disposal Policy**, 2014, s. 6, (Çevrimiçi) https://www.justice.gov.uk/downloads/offenders/probation-instructions/pi-28-2014-archiving-retention-disposal.doc, 11 Mayıs 2016.

Tekrar kullanılması, önceden silindiği varsayılan bilgi ve belgelerin halen var olması durumunda bir takım problemlere yol açabilir. Bu problemlere sebebiyet vermemek adına tekrar kullanılacak ortamın güvenli imha yöntemleriyle silinmesi gerekir.[11]

Muhtemel tekrar kullanım açısından durum yukarıda anlatılan şekilde düşünülmelidir. Bu durum haricinde, manyetik ortamı yakma, eritme, deforme etme veya parçalama yoluyla da yok edebiliriz. Her iki durumda da silinmesi istenen belgelerin varlığı tekrar kullanım veya fiziksel imha haricinde söz konusu olabilir. Çünkü tek bir dosyanın kopyaları, bazıları kurum ve kuruluşun sistem yöneticisi tarafından bile erişilemeyen sayısız yerde bulunabilir. Bu açıdan düşünüldüğünde elektronik ortamlardaki elektronik dosya ve belgelerin silinmesi için hazırlanması gereken yönergelerin veya süreçlerin olması önemlidir. Bu düzenlemelere bir örnek olarak bazı kuruluşların, birkaç aydan daha eski olan tüm e-postaları, sunucularından aylık olarak sildiklerini örnek vermek yerinde olur. Silme işleminden bir hafta önce, sistem yöneticisi, personele ihtiyaç duydukları dosyaları ayrı bir yere kaydetmeleri konusunda tavsiyede bulunur. Bu uygulama kurum ve kuruluşlar tarafından saklanılan gereksiz dosya miktarını azaltır. Sayısız kopyaların varlığını bir ölçüde engeller.[12]

Elektronik ortamın tekrar kullanılması için yapılan silme işlemi ve ortamın fiziksel olarak imha edilmesinde yaygın olan yöntem ve teknikler vardır. Tüm dünyada, gizli, özel ve hassas verileri, sabit sürücüler, SSD'ler, SD kartlar, Flash sürücüler vb. gibi bellek aygıtlarından - kurtarma kapsamı dışında tamamen yok etmek için kullanılan birçok veri silme algoritması vardır. Bu silme algoritmalarından bazıları, ABD Savunma Bakanlığı, diğer ülke hükümetleri ve dünyadaki özel kuruluşlar gibi dünyanın en ünlü askeri kuruluşları da dâhil olan kurumlar tarafından tasarlanmıştır. Bu algoritmalar, gizli ve özel dosyalarının / verilerinin yetkisiz bir kuruluş veya düşman eline

[11] Geof Huth, **Retention and Disposition of Records: How Long to Keep Records and How to Destroy Them, Archives Technical Information Series 41**, 2002, s. 18, (Çevrimiçi) http://www.archives.nysed.gov/common/archives/files/mr_pub41.pdf, 11 Mayıs 2016.

[12] **A.y.**

sızmamasını veya içine sızmamasını ve ticari olarak temin edilebilir herhangi bir işlemle kurtarılamamasını sağlamak için tasarlanmıştır.[13] Algoritmalara ilişkin farklı ülkelerde çeşitli standartlar daha önceki bölümlerde açıklanmıştı. Bunlar aşağıda listelenmiş, daha sonra da bağımsız olarak herbiri değerlendirilmiştir.

5.1.2.1. Güncel Ortamın İmhası İçin Kullanılan Yöntem ve Teknikler

Bilgisayar sistemlerinde birincil depolama alanı, disk sürücülerle sağlanır. Depolama alanlarının öncelikli görevi kullanıcı verilerini yanlışlıkla silinmeye karşı korumaktır. İşletim sistemleri, kullanıcı verilerinin yanlışlıkla silinmesini önlemek ve dosya kurtarma komutlarına sahip olmak için disk dosyalarını geri dönüşüm veya çöp klasörlerine siler. Dosya silme, yalnızca dosya bloğunu gösteren işaretleyicileri ve dosya sisteminin bir dosyayı yeniden birleştirmesine izin veren bağlantıları siler. Bu tür bir silme işlemi en hızlı olmakla beraber verilerin diskte kalması nedeniyle dosyaların daha sonra geri yüklemesini de kolaylaştırır. Ancak bu işlem güvenli değildir. Hem işaretçilerin hem de dosya verilerinin silinmesi güvenli temizleme olarak görülmektedir. Bilgisayar kasetleri için güvenli silme tipik olarak kasetin fiziksel imhası, veri şifreleme veya manyetik bozma yöntemlerini gerektirir. Ancak bu yöntemler uygulanmadan da veriler sık sık kaybolabilir. Bu nedenle güvenli silme yöntemlerinin niçin var olduğunu iyi anlamakta yarar vardır. Kullanıcı verilerini korumak ve uygun, hızlı kullanıcı verisine erişim ve kurtarmaya izin vermek için alınan tipik önlemler verileri yetkisiz kişilerin kurtarmasına karşı savunmasız bırakabilir. Bu yüzden kullanılmayan hard disk sürücülerine ve kasetlere uygun görülmüş ve güvenilebilir veri temizleme yöntemlerinin uygulanması hem güvenlik hem de gizlilik sebebiyle önemlidir.[14]

ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST 800-88), veri temizleme yöntemlerinin kapsayan veri temizleme (data sanitization) kavramını tercih etmektedir. Söz konusu veri temizleme yöntemleri dört başlık altında tanımlanmaktadır. Bun-

[13] Stellar Data Recovery Inc., "7 Effective Algorithms to Remove Files and Folders Permanently," 2018, (Çevrimiçi) https://www.stellarinfo.com/article/7-algorithms-to-wipe-files-folders-permanently.php, 23 Şubat 2019.

[14] Gordon F. Hughes, Daniel M.Commins ve Tom Coughlin, "Disposal of Disk and Tape Data by Secure Sanitization," **IEEE Security and Privacy**, C. 7, No: 4, July/August 2009, s. 29.

lar; tasfiye (disposal), arındırma (clearing), temizleme (purging) ve imha etme (destroying)'dir. Bunlar arasında verilerin güvenlik seviyesi açısından birbirleriyle farklılık arz eder. Ayrıca, işlemi gerçekleştirme süresi açısından da büyük farklılık vardır. Aşağıdaki tabloda bu gibi farklılıklar belirtilmiştir.

Tablo 5.1: Veri Temizleme Metotlarının Karşılaştırılması

Temizleme Yöntemleri	**100 GB İçin Ortalama Süre**	**Güvenlik Seviyesi**	**Açıklamalar**
İşletim sistemi (OS) dosya silme işlemi	Birkaç dakika içinde	Düşük	Gerçek veriyi değil sadece dosya işaretleyiciyi siler; Ortak ticari veri kurtarma yazılımı ile veri kurtarma mümkündür.
Üzerine yazma (DoD5220)	Ortalama yarım gün	Orta	Güncelliğini yitirmiş; üç kez üzerine yazma ve bir tane doğrulama gerektirir; yeniden atanmış blokları silmeyebilir; Birden fazla döngü başka güvenlik açıkları bırakır.
NIST 800-88 güvenli silme (SE)	30 dakikadan 3 saate kadar	Yüksek	Kullanıcının erişebileceği tüm blokların sürücüden silinmesini gerçekleştirir.
Gelişmiş SE	Milisaniye	Yüksek	Sürücü içi şifreleme anahtarının güvenli bir şekilde silinmesini sağlar.
Fiziksel veya manyetik imha	Saniyeler içinde	En yüksek	Çok gizli veriler ve daha fazlası için gereklidir.

(Kaynak: Gordon F. Hughes, Daniel M.Commins ve Tom Coughlin, "Disposal of Disk and Tape Data by Secure Sanitization," **IEEE Security and Privacy**, C. 7, No: 4, July/August 2009, s. 30)

5.1.2.1.1. Tasfiye Etme (Disposal)

Tasfiye etme, depolama ortamını başka bir temizleme işlemine gerek kalmadan veya Windows ve Linux gibi kamuya açık işletim sistemlerinde kullanıcı dosya dizinlerini silerek atmak anlamına gelir.

5.1.2.1.2. Boşaltma (Clearing)

Boşaltma işlemi, bilgileri ortamdan çıkarma işlemidir. Ortamın duyarlılığını veya sınıflandırmasını otomatik olarak değiştirmez. Ayrıca ortamın imhasını da içermez.[15] Bu işlem bilgisayar ekipmanları olan yönlendiriciler, anahtarlar, ağ arayüz kart-

[15] Tasmanian Archive and Heritage Office, **Approved Destruction Methods for State Records, State Records Guideline No 21**, s. 8, (Çevrimiçi) 7 Aralık 2017 https://www.informationstrategy.tas.gov.au/Records-ManagementPrinciples/Document%20Library%20%20Tools/Guideline%2021%20Approved%20destruction%20methods%20for%20State%20records.pdf, 7 Aralık 2017.

ları ve güvenlik duvarları ve ağ cihazının çalışmasında kullanılan bellek gibi malzemelerde uygulanır. Bu işlemin uygulanmasında, birimlerin cihazı sıfırlamaları ve cihazın hafızasını kullanmak için sahte bir yapılandırma (veya eş değeri) yüklemeleri ve sıfırlamanın başarılı olduğunu doğrulamak için bir geri okuma sağlamaları yoluyla olabilir. Mikrofiş, mikrofilm, optik diskler, yazıcı şeritleri ve baskı plakasına bakan darbe yüzeyi, programlanabilir salt okunur hafıza, sadece hafıza okuma, başarıyla sterilize edilemeyen arızalı veya diğer tür ortamlarda boşaltma işlemi uygulanmaz.[16] Boşaltmanın mümkün olduğu bir ortamda bile, teknolojik sorunlar ve bilgisayar korsanlarının ve saldırı yöntemlerinin karmaşıklığındaki ilerlemeler nedeniyle, ortamın kendisinin (ek) imhası, böyle bir ortamın daha hassas veya yüksek kişisel veri hacmine sahip olduğu durumlarda gerekli olabilir.[17] Boşaltma işlemi bir tür üzerine yazma işlemi veya üzerine yazılma mümkün olmayan ortamlarda cihazın sıfırlanması/fabrika ayarlarına dönülmesi anlamında kullanılır.

5.1.2.1.3. Üzerine Yazma (Overwriting)

Elektronik ortamdaki belgelerin güvenli olarak kaldırılması işlemi için kabul edilebilir ve yaygın olan iki imha yöntemi vardır. Bunlar; Üzerine yazma ve fiziksel imhadır. Fiziksel imhaya diğer başlıklarda yer verileceğinden bu kısımda ele alınmayacaktır. Üzerine yazma işlemi olarak imha etme bu kısımda ele alınmıştır. Üzerine yazma iki seviyeli bir işlemdir. Bu seviyeler düşük seviyeli üzerine yazma ve yüksek seviyeli üzerine yazmadır.

Düşük seviyeli üzerine yazma işlemi, temizlenmiş verileri kurtarmak için özel bir yardımcı yazılım veya teknik kullanılmadığı sürece, bilgileri depolama ortamından okunamaz hale getirecek şekilde kaldıran özel bir program kullanarak dosyaları silme işlemidir. ABD'de çok çeşitli fiyat yapılarına sahip çok sayıda ürün mevcuttur ve yapılan seçimin Amerika Savunma Bakanlığı (Department of Defense document, DoD 5220) standardına uyması zorunluluğu söz konusudur. Ancak, sabit disk teknolojisin-

[16] **A.g.r.**, s. 6-7.

[17] Singapore Personel Data Protection Commission, **Guide to Disposal of Personal Data On Physical Medium**, 2016, s. 8, (Çevrimiçi) https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-to-disposal-of-personal-data-on-physical-medium-(200117).pdf, 7 Aralık 2017.

deki ilerleme DoD 5220'yi işlevsiz hale getirmiştir. Günümüzde tüm sürücüler, kullanıcı verilerini kaydetmeden önce randomize eden bir teknoloji olan kısmi yanıt kayıt kanallarını kullanmaktadır. Bu nedenle DoD 5220'nin ilk iki aşaması artık amaçlandığı gibi çalışmamaktadır. Günümüzde ABD Savunma Güvenliği Servisi, üzerine yazma hizmetlerini kullanan federal kurumların yetkili bir DoD laboratuvarına sahip olmalarını ve uygun işlevsellik için değerlendirme yapmalarını gerektirir. NIST 800-88, disk sterilizasyonu için DoD 5220'nin yerini almıştır.[18] Standarda (NIST 800-88) uyması yanında her boyuttaki sabit sürücüyü desteklemesi, işletim sistemlerini, program dosyalarını ve verileri kalıcı olarak silmesi, tüm verileri fiziksel sabit sürücüden silmesi ve tüm bölüm tablolarını ve sürücü biçimlerini de silmesi gerekmektedir. Bu işlem üzerine yazma anlamında değerlendirildiğinde düşük seviyeli üzerine yazma tekniği olarak nitelendirilebilir. Bu teknik, birimlerde kullanılmaya devam edilen bilgisayarlardan verilerin silinmesinde en iyi yöntemdir. Yine, verilerin teknik yollarla kurtarılmasını engellemediğinden, yeniden satılacak veya atılacak sabit disk depolama ortamını temizlemenin kabul edilebilir bir yöntemi değildir.[19]

Yüksek seviyeli üzerine yazma (yeniden biçimlendirme), bir sürücüde veya diskte önceden depolanan verilerin önceden belirlenmiş bir anlamsız bilgi düzeneğiyle değiştirilmesi anlamına gelir. Bu etkili bir şekilde veriyi kurtarılamaz hale getirir. Bu teknik için kullanılan yazılım ürünleri ve uygulamaları aşağıdaki spesifikasyonları karşılamasının beklendiği ifade edilmektedir:[20]

- Verilerin bir modelle uygun şekilde üzerine yazılması gerektiği,
- Üç defa üzerine yazma işlemi tamamlanmadan ve bir doğrulama girişi bitmeden temizleme işleminin bitmeyeceği,
- Yazılım, tüm sabit disk sürücüsünün üzerine yazma yeteneğine sahip olması ve böylece anlamlı verilerin kurtarılmasını imkânsız hale getirmesi gerektiği,

[18] Hughes, Commins ve Coughlin, "Disposal of Disk and Tape Data by Secure Sanitization," s. 30.

[19] Kentucky Department for Libraries and Archives Public Records Division, **Destruction of Public Records: A Procedural Guide**, s. 12-13.

[20] **A.g.r.**, s. 13-14.

- Yazılımın, tüm bölümlerde, bloklarda, izlerde ve tüm sabit disk ortamındaki kullanılmayan disk alanlarında en az üç döngü veri modeli kullanarak üzerine yazma yeteneğine sahip olması gerektiği,
- Yazılımın, tüm verilerin kaldırıldığını doğrulamak için bir yönteme sahip olması gerektiği ve
- Üzerine yazılmayan bölümlerin tanımlanması gerektiği ifade edilmektedir.

Yüksek seviyeli üzerine yazma işleminin veriyi kurtaramaz hale getirdiği Florida Eyalet Kütüphane ve Bilgi Hizmetleri Birimine ait elektronik belge ve elektronik belge yönetim uygulamaları dokümanında da ifade edilmiştir.[21]

Dosya sistemindeki bir dosya bir kullanıcı tarafından silindiğinde, veriler neredeyse hiçbir zaman hemen imha edilmez. Silme işlemi gerçekleştiğinde, işletim sistemin dosyanın belleğini kaldırır. Silinen dosyaların varlığına henüz son verilmiş değildir. İşletim sistemi dosyayı içeren ikili verilerin depolandığı fiziksel disk alanının üzerine yazma için izin vermiş olmaktadır. Silinen kayıtlarda hassas bilgiler varsa, kendi kendine yazılım veya gelişmiş adli veri kurtarma teknikleri kullanılarak silinmiş veri yeniden oluşturulabilir. Bu nedenle, verinin tamamen imha edilmesi dosyanın üzerine yeniden yazma işlemini gerektirir. Dosyanın üzerine yazma işlemi, orijinal dosyanın yerine, rastsal oluşturulmuş "gürültü" verisini veya her ikisini de bir seri 0'lar sonra 1'ler yazan özel bir yazılım gerektirir. Dosyaların durumu bu şekildedir. Bu dosyalara ait üstverilerin durumuna baktığımızda, bir dosyanın meta dataları dosyada saklanır, bu nedenle önceki işlem üstverileri de imha eder. Ancak, bu durumu bilmek ve gözlemlemek mümkündür. Çünkü yok edilen dosyalar hakkındaki meta dataları içeren "sepet" dosyasının varlığı söz konusudur. Bu sepet dosyaları genellikle kullanıcı tarafından oluşturulur ve belge yönetim sorumlusu tarafından bilinmelidir. Bu durumda, dosyalarda aynı parçalama işlemlerini yapmanız burdaki verinin silinmesi için yeterlidir. Bununla birlikte, bazı "sidecars"ların durumu pek belirgin değildir. Bazen işletim sistemi onları kendi iç ihtiyaçları için üretebilir. Yukarıda ifade edilen "sepet" örneği

[21] Florida Department of State Division of Library and Information Services, **Electronic Records and Records Management Practices**, 2010, s. 13-14, (Çevrimiçi) https://dos.myflorida.com/media/31109/electronicrecordsmanagementpractices.pdf, 14 Ekim 2016.

için, Windows ortamında en yaygın kullanıcı tarafından oluşturulan sepet dosyası bir küçük resim önbelleğidir. Vista ve üstü Windows sürümleri, bir dizindeki dosyaların referans görüntülerini içeren bir thumbcache.db dosyasını otomatik olarak oluşturur. İçinde çok fazla bilgi yoktur, ancak klasördeki dosya türlerine bağlı olarak hassas bilgileri tutabilirler ve belgeler yok edildiğinde bu thumbcache.db dosyasının da imha edilmesi gerekir. Örneğin, bir klasör W2 görüntülerini içeriyorsa, küçük resim önbelleği bilgi almak için yeterli çözünürlüğe sahip bir görüntüye sahip olabilir.[22]

Üzerine yazma yordamıyla silinen verilerin kurtarılıp kurtarılamayacağı tartışmalı bir konudur; çünkü üzerine yazma işlemi uygulanan saklama ortamlarının manyetik enerjilerinin çeşitli yöntemler kullanılarak tekrar veriye erişim imkânı verebildiği görülmüştür. Manyetik enerjinin ortadan kaldırılması ise saklama araçlarının da kullanılamaz hale getirmek anlamına geldiğinden bu tekniğin daha çok güncelliğini yitirmiş ortamlar için kullanılması anlam kazanmaktadır. Bu zorluklarla beraber, yazılım ve donanım bileşenlerinin tanımlanması ve bunların imha süreçlerine dâhil edilmesi önemlidir. Verinin üzerine yazıldıktan sonra kurtarılamacağı kanısı yapılan çalışmalarla kanıtlanmaya çalışılmıştır. Mükemmel silme tartışması adı altında sürdürülen çalışmada silinen bir sürücüden gigabayt veya terabaytlık bilgi almak için bir aracın geliştirilebileceği inancının yanlış olacağı vurgulanmaktadır. Çalışmada kurtarılan veri üzerinde örnekler verilerek, kurtarılan verinin aslında anlamsız karakter yığını haline dönüştürüldüğü de gösterilmektedir.[23]

5.1.2.1.4. Temizleme (Purging)

Purging, en gelişmiş laboratuar tekniklerini kullanarak hedef verileri kurtarmayı olanaksız kılan fiziksel veya mantıksal teknikler uygulayarak temizleme yapan bir yöntemdir.[24] Purging, NIST 800-88 tarafından onaylanmış yüksek seviyeli bir veri imha yöntemidir. Onaylanan purging yöntemleri arasında indrive secure erase (SE) komutu ve disk sürücülerinin veya teyp makaralarının manyetiksizleştirmesi vardır.

[22] State Archives of North Carolina, **Destruction of Electronic Records- The G.S. 132 Files**, s. 2, (Çevrimiçi) https://ncrecords.wordpress.com/2014/09/26/destruction-of-electronic-records/, 15 Şubat 2019.

[23] Craig Wright, Dave Kleiman, ve Shyaam Sundhar R.S., "Overwriting Hard Drive Data: The Great Wiping Controversy," Ed. R. Sekar and A.K. Pujari, **ICISS 2008, LNCS 5352**, Berlin Heidelberg, Springer-Verlag, 2008, ss. 243-257.

[24] **NIST 800-88**, s. 43.

Purging, manyetik ortam için manyetiksizleştirme (degaussing) işlemini gerçekleştirmektedir.

5.1.2.1.5. Güvenli Silme (Secure Erase, SE)

Güvenli silme, yukarıda ifade edilen üzerine yazma işlemine benzer bir yapıdadır. Farkı, diğer üzerine yazma programlarından daha hızlı olmasıdır. Çünkü güvenli silme, diğer üzerine yazma programları gibi harici bir veriyle yapılmaz. Burada, yazma düzeninde ana bilgisayardan sürücüye veri aktarımı olmayan tek geçişli bir yazma işlemi uygulanır. Güvenli silme için yazma düzeni önceden tanımlanır ve veri sürücünün içinden alınır. Bu yöntem, 2001 sonrası üretilen ATA (All Advanced Technology Attachment) disk ara yüzlerinde kullanılmaktadır.[25]

5.1.2.1.6. Gelişmiş Güvenli Silme (Enhanced Secure Erase)

Bu silme komutu verilerin tamamen yok edildiğinden emin olmak için önceden belirlenmiş farklı bit desenleriyle birkaç kez verilerin üzerine yazar. Ayrıca artık kullanılmayan sektörler üzerine de yazar. Çünkü buradaki iç hataların verinin erişimine izin verme durumunu ortadan kaldırırarak tüm kullanıcı veri alanlarına (üretici tarafından ayarlanan) üzerine yazma işlemi gerçekleştirir.[26]

5.1.2.1.7. Manyetiksizleştirme (Degaussing)

Etkisizleştirme, medya yüzeyinin manyetik özelliklerini değiştirerek manyetik ortamda depolanan verileri okunaksız hale getiren bir işlemdir. Güçlü bir alternatif manyetik alanın uygulanmasına maruz kalması, verilerin kaybına neden olur ve ortamı manyetik olarak nötr bir hale getirir. Bu teknik, sabit sürücüler, yedekleme ve dijital bantlar gibi belirli çıkarılabilir elektronik ortam türleri için uygundur.[27]

---

[25] Hughes, Commins ve Coughlin, "Disposal of Disk and Tape Data by Secure Sanitization," s. 30.

[26] MediaClone, "Secure Erase Protocols and Methods," (Çevrimiçi) https://www.mediaclone.net/v/vspfiles/downloads/SecureErase.pdf, 19 Eylül 2019.

[27] Joint Technology Committee, "Developing an Electronic Records Preservation and Disposition Plan", Version 1.0, s. 20.

5.1.2.1.8. İmha Etme (Destroying)

Yok etme, NIST 800-88 uyarınca en üst seviyede temizleme seviyesi olarak görülmektedir. Bu seviye, parçalama (disintegration), yakma (incineration), ezme (pulverizing), ufalama (shredding), kimyasal işlem uygulama (chemical attack) veya erime (melting) yoluyla medyanın fiziksel imhası anlamına gelir.[28] Bu yöntemler, ayrıntılı olarak obsolete ortamda bulunan elektronik belgeye yönelik imha yöntemleri ve teknikleri kısmında değerlendirilmiştir.

5.1.2.1.9. Hızlı Silme (Soft Deletion)

Hızlı silme, kamu yararı için açık erişimi veya iş amacıyla saklanması gerekmeyen bilgilere, bağlantıların silinmesi veya silinecek kaydın işaretlenmesi yoluyla erişilemez hale getirilmesi işlemidir. Bu işlem, bilgileri geçici olarak erişilemez hale getirmektedir. Bir kaydın tamamen silinmesi, hızlı silme işleminin ardından belirli bir süre için programlanabilir; bunun ardından kayıt kalıcı olarak silinir. Bu silme işleminin avantajı, normal saklama sürelerini geçen belgelerde sonradan farkına varılan hataların düzeltilmesi için kayıtlara erişilmesi gerektiğinde kısa süreliğine koruma sağlamasıdır.[29] Hızlı silme işlemi özellikle ABD'de yargı organlarınca yaygın olarak kullanılmaktadır. Mahkeme kayıtlarının özel şirketler tarafından kullanılması ve dağıtılması ve mahkeme bilgilerinin internette yayınlanması, yanlış veya eski bilgilerden kaynaklanabilecek olası zararları artırmaktadır. Kamu Kayıtlarının Adil Raporlama Kredisi Kanunu kapsamında ticari amaçlarla kullanımına getirilen kısıtlamalara rağmen, belirli bir dizi için normal saklama süresini aşan süreler boyunca bilgiler yayınlanmış kalabilir. Bu nedenle birçok mahkeme, normalde yok olacak olan dava bilgilerini, daha sonra bilgi doğruluğu konusundaki ihtilaflara karşı sigorta mahiyetinde saklama süresinin ötesinde korumaya devam etmektedirler.[30]

[28] Hughes, Commins ve Coughlin, "Disposal of Disk and Tape Data by Secure Sanitization," s. 30.

[29] Joint Technology Committee, "Developing an Electronic Records Preservation and Disposition Plan", Version 1.0, s. 20.

[30] **A.g.p.**, s. 20.

5.1.2.1.10. Expunging

Bir mahkeme kararıyla, bir kaydın tamamını veya bir kısmını kalıcı olarak kaldırma veya yok etme sürecidir. Bazı durumlarda, bu kaldırma süreci bir belgeyi kapatma veya söz konusu belgeye erişimi kısıtlama işlemini ifade eder.[31] ABD'de yükümlülerin suçları sabitleştiğinde, verilen hapis cezası sonunda, cezasını çektiği varsayımından, yükümlüye ait yargılama sürecindeki mahkeme kayıtları erişime kapatılmaktadır. Bu uygulamayla, yükümlünün sosyal hayatına zarar verebilecek sicil kaydı erişime kapatılır. Yükümlü, iş başvurularında sicil kaydı yokmuş gibi tavır sergileyebilmekte hatta kendisine sorulduğunda sicil kaydının olmadığını ifade etme hakkı da yükümlüye tanınmaktadır. Ancak cinayet, adam kaçırma, cinsel suçlar, terörizm, çocuk tehlikesi ve ihanet gibi birçok ciddi suç ile ilişkisi olan kişilerin belgeleri bu uygulamaya dâhil edilmez. Amerika'nın tümünde standart bir yapısı olmaksızın bölgeden bölgeye değişebilecek uygulamalar söz konusudur.[32] Türkiye'de özellikle bankalarda kredi talebindeki kişilerin kendileri hakkında oluşturulmuş sicil notlarına bağlı olarak kredi verilip verilmeyeceği değerlendirilmektedir. Expunging uygulamasının bankalarca uygulanabilirliği, bankalar açısından müşteri kitlesini artırma yönelik tartışmaya değer bir konu olarak görülebilir. Örneğin bankaya kredi borcu olan birinin çeşitli nedenlerle ödemelerini yapamamış olması, geç ödemiş olması gibi durumlarda, mevcut kişinin yeni bir kredi başvurusunda -eğer borcunu kapatmış ise siciline yönelik bilgilerin yeni başvuru için engel teşkil etmemesi adına- söz konusu expunging yöntemi kullanılabilir.

5.1.2.1.11. Kripto Silme (Crypto Erase)

Şifreleme, bir şifreleme / şifre çözme anahtarı olarak adlandırılan, özel bilgiye sahip olanlar dışında herkes için okunamaz hale getirmek için şifreli bir algoritma (şifre olarak adlandırılır) kullanarak bilgiyi dönüştürme işlemidir. "Tek yönlü" şifre-

[31] Kentucky Department for Libraries and Archives, **Public Records Division, Destruction of Public Records: A Procedural Guide**, s. 2.

[32] Kele Onyejekwe, "Erasing the Past: How to Expunge a Client's Criminal Record," 2016, (Çevrimiçi) https://www.americanbar.org/groups/young_lawyers/publications/tyl/topics/client-development/erasing past-how-expunge-clients-criminal-record/, 11 Nisan 2019.

leme, ilk önce verileri şifreleyerek ve ardından verileri şifrelemek için kullanılan anahtarı imha ederek verileri kullanılamaz hale getirmek için şifreleme tekniklerini kullanan bir veri imha tekniğidir.[33]

Dijital bilgi, ortamın yeni bilgilerle şifrelenmesiyle erişilemez duruma getirilebilir. Bu teknikler gizli olan bilgi ve belgelere uygun olmayabilir, ancak fiziksel ortamın hala iyi ve tekrar kullanılabilir olduğu durumlar için yeterli olabilir.[34] Bu yöntem, şifreleme anahtarını silen bir şifreleme silmesini çağırmak için yerel komutu kullanır. Bu yöntem, üretici tarafından tanımlanan yerel komutları kullandığından, yalnızca silinen sürücü tarafından destekleniyorsa kullanılabilir.[35]

5.1.2.2. İmha İçin Kontrol Listesi

Elektronik belgelerin imhasının saklama planları çerçevesinde yapılacağı ifade edilmişti. Ayrıca belgelerin hangi yöntem ve teknikle imha edilmesi gerektiği genel yasallara ve kurumsal iç düzenlemelere bağlıdır. Tüm bunlardan sonra belge imha kararı verilmeden aşağıda sıralanan kontrol listesinin[36] de gözden geçirilmesi yararlı olacaktır.

- Kurum ve kuruluşa ait imha edilecek belgeler, söz konusu kurum ve kuruluşun bağlı olduğu üst idare tarafından yetkilendirilmiş midir?
- Kurum ve kuruluş için artık gerekmeyen ve saklanılmasında yasal bir zorunluluk olmayan belgelere mi uygulanmaktadır?
- İmha edilecek belgeler güncel veya bekleyen bir soruşturmaya dâhil midir veya erişimi gerekli midir?
- İmha edilecek belgeler için kurum yetkilileri uygun bir veri imha şirketiyle iletişime geçmiş midir?

---

[33] U.S. Department of Education, Privacy Technical Assistance Center, **Best Practices for Data Destruction**, s. 10.

[34] Joint Technology Committee, "Developing an Electronic Records Preservation and Disposition Plan", Version 1.0, s. 20.

[35] Katie Moss Jefcoat, "A Comprehensive List of Data Wiping and Erasure Standards, Cryptographic Erasure (Crypto Erase)," 2017, (Çevrimiçi) https://www.blancco.com/blog-comprehensive-list-data-wiping-erasure-standards/, 24 Şubat 2019.

[36] New Zealand University of Otago, **Records Destruction Guidelines**, 2012, s. 4. (Çevrimiçi) https://www.otago.ac.nz/administration/corporaterecords/otago015244.pdf, 7 Aralık 2017.

- Belgelerin imha edilmesini sağlayacak şirketin yetkili imha sertifikası var mıdır?
- İmha edilecek belgelerin listesi tutulmuş mudur?

5.1.3. Obsolete Ortamda Bulunan Elektronik Belgeye Yönelik İmha Yöntemleri ve Teknikleri

Bilgi teknolojilerindeki hızlı değişim, ortaya konan donanımsal araçların da değişimini sağlamaktadır. Özellikle depolama alanlarına yönelik ürünler gün geçtikçe değişmektedir. Disketler, CD'ler, harici bellekler, sürücü diskler, NAS sistemler, SAN sistemler vb. çeşitlilik teknolojik değişimin bir yansıması olarak karşımıza çıkmaktadır. Yeni ürünler veya araçlar kullanılırken daha önce kullanılan ürünlerin yeni ürünlerle uyum sağlaması gerekmektedir. Bu uyum, eski depolama alanlarının yeni depolama alanlarına verinin geçişi ile mümkün olabilmektedir. Eskiden yeniye geçiş yapılırken, eski depolama araçlarının da imha edilmesi gündeme gelmektedir. Güncelliğini yitirmiş ortam diye ifade edebileceğimiz eski depolama araçlarının imhası özellikle barındırdığı bilgi ve belgenin niteliğine göre belirlenmesi gerekirken, tam olarak ne barındırdığını bilmiyorsak imhanın ne denli önemli olduğunu anlamak gayet açıktır.

Özellikle belge yönetimi ve arşivcilik açısından olaya bakıldığında imha işlemi daha da anlam kazanmaktadır. Bu nedenle, güncelliğini yitirmiş ortamın imhası ne şekilde yapılmalı, hangi yöntem ve teknikler kullanılmalı gibi soruların cevapları bu kısımda verilmeye çalışılmaktadır. Aşağıda verilen tabloda bazı araçlar ve bu araçlar için uygun olan ve olmayan imha yöntemleri verilmeye çalışılmıştır.

Tablo 5.2: İmha Yöntemleri ve Uygulanabilecek Alanlar

		İmha Yöntemleri				
	Nesne Türleri	**Çekiçli Değirmen**	**Parçalayıcı**	**Öğütücü/Zımpara**	**Kesme**	**Etkisizleştirme**
NESNE	Elektrostatik hafıza cihazlar	Evet	Evet	Evet	Hayır	Hayır
	Manyetik disketler	Evet	Evet	Hayır	Evet	Evet
	Manyetik sabit diskler	Evet	Evet	Evet	Hayır	Evet
	Manyetik bantlar (ses ve video kasetleri)	Evet	Evet	Hayır	Evet	Evet

	Optik diskler	Evet	Evet	Evet	Evet	Hayır
	Yarı iletken bellek	Evet	Evet	Hayır	Hayır	Hayır

(**Kaynak:** Tasmanian Archive and Heritage Office, Approved Destruction Methods for State Records, State Records Guideline No 21, s. 7.)

(Aşağıda Sıralanan Ürünlerin Tam Listesi İçin Electronic Records Management Guidelines Version 4, March 2004 Kaynağa Bakılabilir.)

Tablo 5.3: Güncelliğini Yitirmiş Ortama İlişkin Medya Çeşitliliği

Dijital hafıza ürünleri (bir bölümü obsole hale gelmiş olmasına rağmen kullanımdadır):	**Dijital bellek çeşitleri:**	**Disketler, Hard Diskler**	**Manyetik bant çeşitleri:**	**Mikroform çeşitleri:**	**Optik disk çeşitleri:**	**SIM veya akıllı kartlar**
Bilgisayarlar	Dinamik rastsal erişim belleği (Dynamic Random Access Memory, DRAM)	Aşağıdakileri içeren alt formatlara sahip Sabit Disk Sürücüsü (HDD):	Kompakt Kaset (C60 ve C90 alt formatlarında)	Diyafram kartları	Blu-Ray	Cep telefonları
Faxs makineleri	Alan-programlanabilir kapı dizisi (Field-Programmable Gate Array, FPGA)	Dijital bellek içeren Hibrit Sabit Sürücü (HHD)	Dijital Ses Bandı (DAT)	Mikrofilm	Kompakt Disk (CD)	Mobil geniş bant cihazlar
Grafik kartları	Flash bellek (Flash memory)	Paralel AT Eklentisi (PATA) olarak da bilinen Tümleşik Sürücü Elektroniği (IDE)	Dijital Video (DV) kaseti	Mikrofişler.	Dijital Çok Yönlü Disk (DVD).	Banka kartları
Hibrid sabit sürücüler (HHDs)	Sadece hafıza okuyabilir (Read-Only Memory, ROM)	Seri AT Eki (SATA)	Doğrusal Bant Açma (LTO)			Kimlik kartları.
Cep telefonları		Küçük Bilgisayar Sistem Arabirimi (SCSI)	Video Ev Sistemi (VHS) kaseti.			
Yönlendiriciler		ZIP diski				
Güvenli dijital (SD) kartlar						
Kişisel dijital asistanlar (PDAs)						
Yazıcılar						
Katı Hal Sürücüsü (SSDs)						

Telefonlar						
USB'ler						

(**Kaynak:** Electronic Records Management Guidelines Version 4, March 2004)

Dijital hafıza ürünleri:[37] genellikle bir baskılı devre kartı (PCB) bileşen kartına veya ana kartına monte edilmiş ve aşağıdakileri içeren elektronik cihazlarda kullanılan bir dizi yonga[38] olarak yapılandırılan katı hal veya programlanabilir bellektir.

Disketler: Kişisel bilgisayarlarda kullanılan ve çeşitli elektronik dosya türlerini depolamak için bir disket sürücü (FDD) tarafından işletilen yeniden yazılabilir manyetik ortam. Disketler, polyester kaplı, kare veya dikdörtgen plastik bir gövdeye kapatılmış ince ve esnek bir manyetik disk olarak yapılmış 3.5', 5.25' veya 8' formatlarında mevcuttur.[39]

Hard diskler: Veriyi manyetik olarak okumak ve yazmak için kullanılan yeniden yazılabilir, uçucu olmayan rastsal erişim belleği. Genellikle bir iç bilgisayar bileşeni, taşınabilir depolama aygıtı veya sunucularda veya RAID (yedek bağımsız disk dizisi) dizilerinde bulunur. Tipik olarak bir veya daha fazla sert döner plaka, bir motor tahrik mili ve sert mahfaza olarak imal edilmiştir.

Manyetik bantlar: Ses, video ve veri kaydetmek için kullanılan manyetik medya. Tipik olarak uzun ve dar bir plastik olarak yapılır. Sert kaset, kutu veya kartuş içinde bulunan bir makara üzerinde mıknatıslanabilir bir malzemeyle kaplanmış şerit.

Mikroformlar: Depolama, aktarma, okuma veya yazdırma amacıyla belgelerin mikro çoğaltılması için kullanılır. Tipik olarak bir makara üzerinde, genellikle bir kasette ya da düz plastik bir karta monte edilmiş bir film şeklindedir.

[37] U.K. Centre for the Protection of National Infrastructure (CPNI Standard), **Secure Destruction Of Sensitive Items**, s. 16.

[38] Yonga: Milimetrik yüzeyler üzerinde on binlerce devre elemanından oluşan ve son derece karmaşık elektronik devrelerin yerleştirildiği, genellikle silikon benzeri yarı iletken malzeme, çip (Türk Dil Kurumu, "Yonga," (Çevrimiçi) https://sozluk.gov.tr/, 26 Eylül 2019).

[39] U.K. Centre for the Protection of National Infrastructure (CPNI Standard), **Secure Destruction Of Sensitive Items**, s. 16.

Optik diskler: Ses, video ve veri kaydetmek için kullanılan optik medya. Genellikle yeniden yazılabilir. Çeşitli elektronik dosya türlerini saklamak için kişisel bilgisayarlarla birlikte kullanılır. Tipik olarak, plastik bir substrat içinde bulunan bir kayıt katmanına sahip düz, dairesel bir disk.

SIM veya akıllı kartlar: Yeniden yazılabilir medya, tanımlama, doğrulama, veri saklama ve uygulama işleme için kullanılır. Tipik olarak gömülü devre ve plastik kontaklı bir bellek yongası (çip) veya veri iletimi için bir tel halkası içeren plastik bir kart.

5.1.3.1. Güncelliğini Yitirmiş Ortamın İmhası İçin Kullanılan Yöntem ve Teknikler

Güncelliğini yitirmiş ortamdaki belgelerin imhası, güncel ortamdaki belgelerin imhasında kullanılan yöntem ve tekniklerle benzerlik gösterir. Aralarındaki fark güncelliğini yitirmiş ortamdaki belgelerin imhasıyla beraber ortamın da imha edilmesi gerektiğidir. Bu durum kurum ve kuruluşların hassasiyetlerine göre şekillenir. Kurumsal bilgilerin yeni ortamlara dönüşümü sağlanırken geride kalan ortamda hassas bilgi ve belgeler yer alıyorsa, eski ortamın fiziksel imhası kaçınılmazdır. Eğer gizlilik değeri düşük ama yine de başkalarının eline geçilmesi istenmiyorsa, buna göre kullanılan yöntemler de farklılık gösterir. Örneğin kullanılan teknolojik ortamların imhası gerektiğinde ortamın içeriği temizlenerek ortamın kendisi teknolojik bir gösterge olması açısından gelecek nesiller için saklanıp sergilenmesi arşivcilik açısından da anlam taşımaktadır. Aşağıda sıralanan yöntemler, ortamın fiziksel olarak imhasını gerektiren durumlarda başvurulur. Ortam fiziksel olarak imha edilmek istenmiyorsa ancak ortamın içindeki bilgi ve belgeler imha edilmek isteniyorsa yukarıda güncel ortamın imhası için sıralanan yöntemlere başvurulur.

5.1.3.1.1. Erişime Kapatma (Deaccessioning)

Erişime kapatma, bir koleksiyonun veya malzemenin arşiv hizmetinin envanterinden / arşiv kurumu sahipliğinden resmi olarak çıkarılması işlemidir.[40] Çıkarılma işlemi, koleksiyon, seri veya belge grubu içinde olabilmektedir. Bunlar satılma yoluyla

[40] The National Archives of United Kingdom (TNA), **Deaccessioning and Disposal Guidance For Archive Services**, 2015, s. 31, (Çevrimiçi) http://www.nationalarchives.gov.uk/documents/Deaccessioning-and-disposal-guide.pdf, 11.05.2016.

başka kurum ve kuruluşlara devri şeklinde olmaktadır. Yasal ve kurumsal düzenlemelerdeki durumuna göre değerlendirilir. Bazı kurumlar maliyeti azaltmak ve geriye kalan koleksiyonlarını daha zenginleştirmek adına erişime kapatma sürecini işletirler. Süreçte belgelerin tasviyesi adına dört seçenek vardır. Bunlar; transfer, iade (bağışlayan kişiye geri verme), satma ve imhadır.[41] Bu seçeneklerden imhanın nasıl olacağı tezin konusunu ilgilendirmektedir. Böyle bir durumda başvurulması gereken imha yöntem ve teknikleri bu çalışmanın ilgili başlıklarında açıklanmıştır.

5.1.3.1.2. Geri Dönüşüme Uygun Hale Getirme

Bu teknik kâğıt vb. ortamdaki belgelerin imhasında kullanılır. Bu tür malzeme bir şekilde öğütüldükten sonra plastik olan kısmı, metal olan değerli kısımları ayrı ayrı geri dönüşüm için değerlendirilmek üzere işlemden geçirilir. Bu işlemde kâğıt, hamurlaştırma makinesine atılır. Makine malzemeyi doğrayarak çalkalar. Su ve etken kimyasallar malzemeyi lifli sıvı çamur kıvamına getirir. Lifli çamur daha sonra tüm yazı karakterlerinin baskılı yüzeyden çıkarılmasını sağlamak için bir mürekkep çıkarma işlemine tabi tutulur.[42] Geriye kalan malzeme de geri dönüşüm için ham madde olarak kullanılır.

5.1.3.1.3. Taşlama veya Fırçalama (Grinding or Scrubbing)

Bu teknik**,** disklerin imha edilmesi için kullanılır. Diskin kayıt yüzeyindeki katmanı tamamen çıkıncaya kadar aşındırıcı bir yüzeye (zımpara çarkı, taşlama veya zımparalama aygıtı gibi) karşı döndürülür. Kayıt katmanının doğrudan aşındırıcı yüzeye maruz kalmasına dikkat edilmelidir.[43]

5.1.3.1.4. Çekiçli Değirmenle İmha Etme (Hammer-Milling)

Çekiçli değirmenle öğütme, değirmenin haznesinde yüksek hızda dönen çekiçler (tipik olarak sertleştirilmiş çelik bloklar) ile donatılmış döner bir tambur ile yapılır. Haznedeki malzeme, çekiçlerle parçalanırken bir taraftan da hazne duvarı ve diğer

[41] Society of American Archivists (SAA), **Guidelines for Reappraisal and Deaccessioning**, Draft, 2011, s. 13-16, (Çevrimiçi) https://www2.archivists.org/sites/all/files/GuidelinesForReappraisalAndDeaccessioningDRAFT.pdf, 20 Eylül 2019.

[42] U.K. Centre for the Protection of National Infrastructure (CPNI Standard), **Secure Destruction Of Sensitive Items**, s. 20.

[43] **A.g.s.**, s. 19.

malzemelerle sürterek aşınmaya ve ısıya maruz kalır. Böylelikle ortam küçük parçacıklara ayrılırken bilgi kayıt yüzeyleri de imha edilmiş olur. Çekiçli değirmenlerin çoğu, akıllı ekranlarla donatılmış olup, malzeme istenen parça boyutlarına ulaşmadan işlem tamamlanmaz. Akıllı ekran ile beraber, parçalanan malzemelerin hazneden çıkmasını sağlayan yer çekimi sayesinde alt eleklerden geçer. Malzeme istenen parçaya indirgenmeden elekten düşmez veya bir vakup pompası kullanılarak elekten düşebilecek malzemeler çekilir.[44]

5.1.3.1.5. Parçalama (Disintegration)

Parçalama tekniğinde, malzeme hazne içine sabitlenmiş ikinci bir bıçak setine karşı yüksek hızda dönen sertleştirilmiş bıçaklarla donatılmış dönen bir tamburdan oluşan bir kesme süreci gerçekleşir. Süreçte malzeme bıçaklarla kesilirken aşınma ve ısınmanın katkısıyla kayıt yüzeyi imha edilmiş olur. Çoğu parçalayıcı, işlenmiş malzemenin gerekli parçacık boyutuna indirgendiğinde düşmesini sağlayan delikli bir elek ile donatılmıştır. Parçacıklar akıllı ekranlar sayesinde takip edilebilir ve parçacıklar yerçekimi ile eleklerden düşer veya bir vakum pompasıyla çekilir.[45]

5.1.3.1.6. Ufalama (Shredding)

Ufalama tekniği, taşınabilir olan ortamlar için geçerlidir. Söz konusu ortamlar, CD'ler, DVD'ler, disketler, manyetik bantlar ve kartuşlardır.[46] Bu teknikte, ortam birbirine kenetlenmiş döner bir bıçak setinin nesneyi kesmesiyle yapılır. Ortam ufak parçalar haline getirilirken ısıya maruz kalır. Isıya maruz kalan parçalar üzerindeki kayıt alanları aşınmayla beraber yok olur.[47] Bu teknikte saklama ortamları için kullanılan araçların ısıya maruz kaldığında katmanlarından ayrılması, böylelikle malzemelerin cinslerine göre ayrılıp ve ona göre ufalama yapılmasını sağlamaktadır.

---

[44] **A.y.**

[45] U.K. Centre for the Protection of National Infrastructure (CPNI Standard), **Secure Destruction Of Sensitive Items**, s. 19.

[46] Joint Technology Committee, "Developing an Electronic Records Preservation and Disposition Plan", s. 20.

[47] U.K. Centre for the Protection of National Infrastructure (CPNI Standard), **Secure Destruction Of Sensitive Items**, s. 20.

5.1.3.1.7. Yakma (Incineration)

Yakma tekniğinde, ortamın organik bileşenlerini yakan, malzemeyi küle indirgeyen bir yakma fırınına verilmesiyle başlar. Fırında yanan malzemeden geriye uçucu kül ve dip kül kalır. Uçucu kül, baca gazlarıyla birlikte yükselen ince parçacıklar şeklinde görülür. Dip kül ise, metaller gibi yanıcı olmayan malzemelerin katı topaklı halini alır.[48] Bu tekniğin uygulanmasında kimyasal gazların doğaya salınması da söz konusudur. Dolayısıyla yakma işleminin yapıldığı işletmenin yakma kaynaklı oluşan duman için filtreleme kapasitesine sahip olması gerekir.

5.1.3.1.8. Kesme (Cutting)

Bu teknikte, malzeme önceden belirlenmiş genişlikteki şeritler halinde dilimleyen bir bıçakla kesilir. Dilimlenmiş malzeme daha sonra 90° döndürülür ve tekrar kesilmiş bir atık malzeme üretilecek şekilde dilimlenir.[49] Bu işlem genellikle giyotin[50] adı verilen basımevi vb. yerlerde kâğıtları kesmek için kullanılan araçlara benzer makinelerce yapılır.

5.1.3.1.10. Salamuralaşma (Dry Maceration)[51]

Salamuralaşma, sabit sürücülerin hidrolik olarak ezen makinelerin bıraktığı ezme işlemidir. Ezme işlemi, sabit disk kasasına onarılamaz bir hasara neden olurken aynı zamanda iç plakayı da yok eden bir zımba kullanır. Bu kuvvet, sürücüyü yeniden bağlamak veya çalışan bir bilgisayara yeniden bağlanmamak için yeterli bir teknik olarak görülmektedir.[52]

5.1.3.1.11. Eritme (Smelting)

Eritme, geri dönüşüm noktasında yakma tekniğinden ayrılır. Eritme tekniğinde, ortam tipik olarak ince bir kül elde etmek için yakılır ve daha sonra bin santigrat dere-

[48] **A.g.s.**, s. 19.
[49] **A.y.**, s. 19.
[50] Giyotin nedir?
[51] New Zealand University of Otago, **Records Destruction Guidelines**, 2012, s. 2.
[52] Joint Technology Committee, "Developing an Electronic Records Preservation and Disposition Plan", s. 20.

ceyi aşan sıcaklıklarda eritme fırınına verilir. Eriyen kül dökülmüş, soğutulmuş ve ayrılmış sıvı mıcırla reaksiyona girerek metallerin daha fazla geri dönüşüm ve inceltme yoluyla geri kazanılmasını sağlar.[53]

5.1.3.1.12. Kimyasal İmha

Kimyasal imhada, manyetik depolama araçları**,** kayıt yüzeyleri tamamen çıkıncaya kadar kimyasal (tipik olarak asit) banyosuna batırılır.[54] Asidin içinde bekleyen malzeme özelliklerini kaybederek imha olmuş olur.

5.1.3.1.13. Elektronik Atık (E-Waste)

Güncelliğini yitirmiş ortamın imhası için sıralanan yöntem ve teknikler, kullanılmayan veya kullanılmayacak olan elektronik malzemelerin imha edilmesine yardımcı olan yöntemlerdir. Söz konusu malzemeler imha edilmiş halleriyle beraber genel olarak elektronik atık olarak görülür. Bu durumda elektronik atık, kırılmış, eskimiş veya geri dönüşüme ihtiyacı olan tüm elektronik atık biçimlerini kapsayan bir şemsiye terimdir.[55] Elektronik atık, malzemelerin işlevselliğini kaybetmesini sağlar ve geri dönüşüm için de kullanma imkânı sunmaktadır.

5.1.3.2. İmha İçin Kontrol Listesi

Elektronik belgelerin imhasında yazılım programlarıyla ortamın içindeki veriler silinmeye çalışılmaktadır. Yazılımsal olarak silinmiş veya yazılımsal olarak silinemeyen ortamların fiizksel imhası da kurum ve kuruluşlar için önemli bir süreçtir. Bu süreç başlatılmadan aşağıda sıralanan kontrol listesinin[56] de gözden geçirilmesi yararlı olacaktır.

- İmha edilecek belgeler, ilişkili olduğu güncel bir saklama planına uygun bir şekilde mi imha ediliyor?

---

[53] U.K. Centre for the Protection of National Infrastructure (CPNI Standard), **Secure Destruction Of Sensitive Items**, s. 20.

[54] **A.g.s.**, s. 19.

[55] Corporate Document Destruction, "e-Waste Destruction and Recycling," (Çevrimiçi) https://www.corporatedocumentdestruction.com.au/e-waste-destruction-and-computer-recycling-melbourne/e-waste-destruction-and-recycling, 21 Eylül 2019.

[56] Kentucky Department for Libraries and Archives, **Public Records Division, Destruction of Public Records: A Procedural Guide**, s. 18.

- Kurum ve kuruluş imha edeceği belgelerin saklanmasına gerek duymuyor mu?
- İmha edilecek belgeler güncel veya bekleyen bir soruşturmaya dâhil midir veya erişimi gerekli midir?
- Kurum içi gerekli izinler alınmış mıdır?
- İmha edilecek belgeler, özel bir güvenlik gerekçesiyle tutulmasına gerek kalmamış mıdır?
- İmha edilecek belgeler yüksek güvenlik seviyesine sahip olup, güvenli imha edilmeleri için kilitli konteynerlerde veya kurum içinde mi imha edilecek?
- Uygun hizmet sağlayıcı ile iletişime geçildi mi?
- Belgelerin taşınabileceği kamyon veya kamyonet kapalı kasalı mıdır?
- İmha hizmetini verecek olan firmanın imha yetki sertifikası var mıdır?
- İmha edilecek belgeler kurumdan toplanılan günde mi yapılacak?
- İmha firmasından sertifika alındı mı?
- Kurum belge yönetim sisteminde imha edilmiş belge ve ayrıntılı bilgisi geçildi mi?

5.2. ADLİ BİLİŞİM (DIGITAL FORENSICS) ARAÇLARI VE BUNLARIN ELEKTRONİK BELGE İMHASIYLA İLİŞKİSİ

Adli bilişim, bilgisayar biliminin ve araştırma prosedürlerinin uygun arama otoritesinden sonra dijital kanıtların analizini, aitlik zincirini, matematikle doğrulama, doğrulanmış araçların kullanımı, tekrarlanabilirlik, raporlama ve olası uzman sunumunu içeren yasal bir amaç için uygulanması olarak tanımlanmaktadır.[57] Diğer bir tanıma göre de;

"Adli bilişim, Disketlerden, sabit disklerden ve çıkartılabilir disklerden delil elde etme amacıyla veri kurtarma işlemi olan ve elektronik delillerin muhteva ettiği bilgileri, delil inceleme süreçlerini, hukuki ve etik sorumlulukları göz önünde bulundurarak, delilin bütünlüğünü koruyarak ve maddi gerçeği açığa çıkarmak amacıyla;

[57] Ken Zatyko, "Commentary: Defining Digital Forensics," **Forensic Magazine**, Feb/March 2007, s. 1, (Çevrimiçi) https://www.forensicmag.com/article/2007/01/commentary-defining-digital-forensics, 13. Eylül 2019.

kopyalama, belirleme, çözümleme, yorumlama ve belgeleme süreçlerinin bütününe adli bilişim adı verilmektedir."[58]

Adli bilişimin imha uygulamalarına dâhil edilmesi iki açıdan anlamlı olur. Bu açılardan birincisi, silinmiş verinin adli bilişim teknikleriyle elde edilmesinin mümkün görünmesidir. Nitekim, bazı uzmanlara göre adli bilişim, güvenli silme için en büyük tehdit sayılmaktadır.[59] Bu tehdit şüphesiz silinmiş verinin elde edilmesinde kullanılan tekniklerdir. Yasal olarak silinmesi uygun görülmüş ve imha edilmiş olan belgelerin yetkisiz kişilerce adli bilişim tekniklerini kullanmak suretiyle elde edilmiş olması, imha işleminin uygulanmasındaki sorunları beraberinde getirmektedir. Adli bilişimin imha teorisiyle ilişkisinin birinci açısı bu şekilde iken ikinci açısı, adli bilişim teknikleri kullanılarak elde edilen verilerin daha sonrası için nasıl bir imha sürecine girdiğidir. Türkiye'deki adli bilişimi ilgilendiren yasal düzenleme bakıldığında bu imha sürecinin nasıl başladığını anlayabiliriz.

Adli bilişimin Türkiye'deki yasal çerçevesi Türkiye Büyük Millet Meclisinin 4 Aralık 2004'te kabul ettiği ve 1 Haziran 2005'te yürürlüğe giren 5271 sayılı Ceza Muhakemesi Kanunu (CMK) ile sağlanmaktadır. Kanunun yürürlüğe girmesiyle, 4 Nisan 1929 tarihli ve 1412 sayılı Ceza Muhakemeleri Usulü Kanunu yürürlükten kaldırılmıştır. CMK'nın 134. maddesine göre düzenlenen adli bilişim, "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"[60] başlığı altında açıklanmıştır. Ayrıca, aynı maddeye, 7 Temmuz 2018 tarihinde eklenen şu üç cümle imha açısından da önemlidir. Bunlar;

"(1) *Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur.* (2) *Hâkim kararını en geç yirmi dört saat içinde verir.* (3) *Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir*"[61]

---

[58] Sean Barry, "Smoking Microchips Tells It All: Computer Forensic Experts Mine Hard Drives For Data That Too-Clever Users Thought Long Deleted," (Çevrimiçi) http://www.dataforensics.com/articles/ smoking_microchip_tells_it_all.pdf, 15 Nisan 2014; Leyla Keser Berber, **Adli Bilişim**, Ankara, Yetkin Yayınları, 2004, s. 39; Akt: Muharrem Özen ve Gürkan Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)," **Ankara Barosu Dergisi**, S. 1, s. 43-77.

[59] Hughes, Commins ve Coughlin, "Disposal of Disk and Tape Data by Secure Sanitization," s. 29.

[60] "5271 sayılı Ceza Muhakemesi Kanunu," Madde: 134, **Resmi Gazete**, Sayı: 25673, Tarih: 17.12.2004, (Çevrimiçi) http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf, 21 Nisan 2019.

[61] "5271 sayılı Ceza Muhakemesi Kanunu," Madde: 134.

şeklinde ifade edilmiştir. CMK, adli bilişim için dayanak olmuş olsa da, bazı durumlarda verinin imha edilmesini de düzenlemiştir. Fakat bu verinin nasıl imha edilmesi gerektiği noktasında herhangi bir ifade yoktur. Verinin nasıl imha edilmesi gerektiği ele alınmamış olsa da imha kelimesinden kasıt, elde edilen/mevcut tüm kopyalar ve geride bunlara ait izlerin bırakılmaması anlamını düşündürmektedir. Nitekim söz konusu kâğıt ortam olsaydı, bu kâğıtların imha edilmesi, bunların tamamen yok edilmesi anlamına gelirdi. Bu açıdan daha karışık olsa da elektronik verinin imha edilmesi de bu gözle değerlendirilmelidir. Arşiv imha teorisinin adli bilişim açısından yasal dayanağına bakıldığında CMK'nın 134. maddesi önemlidir.

Adli bilişimin imha teorisiyle ilişkisinin birinci açısı olan olan silinmiş verinin geri getirilme tekniklerinden bahsetmek önemlidir. Ayrıca, adli bilişimin çalışma mantığını ve arşivsel fonksiyonları nasıl desteklediğini anlamak için verinin depolandığı alanlarda veya ortamlarda veriye erişimin yazılımsal ve donanımsal olarak nasıl olduğunu görmek yararlı olacaktır.

Bir depolama cihazından verilere erişim normalde bir birim monte etmeyi ve ardından dosyaları dosya sistemi üzerinden kopyalamayı veya açmayı içerir. Ortamdaki sinyalleri algılamak için donanım gerekli olduğu gibi, sinyalleri bit akışlarına çevirmek için de ayrı bir donanım ve yazılım gereklidir. Söz konusu bit akışlarını mevcut çalışan bilgisayar ortamına taşımak için de yine donanıma ve yazılıma ihtiyaç duyulur. Gerekli tüm donanım ve yazılım sağlandıktan sonra tüm dosyalar veya dosyaların bileşenleriyle veriyle etkileşime geçilebilir. Dosya sistemi genellikle kullanıcı ve temel veriler arasında arabuluculuk rolü oynar ve dosya düzeyinde etkileşimi kolaylaştırmak için tasarlanmıştır (örneğin, dosya adlandırma, zaman damgalarını görüntüleme, erişim kontrolleri gibi). Dosya sistemi, kullanıcıdan "bilgileri nerede ve nasıl sakladığı" konusunda karmaşık bilgileri "gizlemeye" yarar. Birçok amaç için, dosya sistemi çok değerli bir soyutlama mekanizmasıdır, çünkü kullanıcıların temeldeki verileri anlamalarını veya doğrudan erişmelerini gerektirmez. Dosya sistemi tarafından gizlenen temel verilere ilgi duyanlar, bunun yerine, depolama ortamında bulunan tüm verilerin sektör bazında düşük düzeyli kopyaları olan disk görüntüleri oluşturabilir ve bunlarla etkileşime girebilir. Disk görüntüsünün incelenmesi, sürücü kullanıcılarının bilinçli

olarak veya kasıtlı olarak orada bırakmadıkları ancak önemli bağlamsal bilgilerin izleri olarak hizmet edebileceği önemli miktarda bilgiyi ortaya çıkarabilir.[62]

Adli bilişimin elektronik belgenin imhasıyla ilişkisi yukarıda açıklanan iki temel açıdan değerlendirilmiştir. Adli bilişimin arşivlerle veya arşivcilikle ilişikisine baktığımızda belgelerin provenans, orijinal düzen ve aitlik zinciri açılarından da ilişkisi bulunmaktadır. Aşağıda bu ilişkiler açıklanmaya çalışılmıştır.

Arşivler, tek tek dosyalar veya paketlenmiş dizinler yerine, disk görüntülerini temel edinme birimleri olarak ele alarak çeşitli adli bilişim uygulamalarını ve yöntemlerini içerebilir. Yazma engelleyicilerini kullanmak, tam disk görüntüleri oluşturmak ve dosyalarla ilişkilendirilmiş verileri çıkarmak, provenansı, orijinal düzeni ve aitlik zincirini sağlamak için önemlidir. Adli bilişim yöntemlerinin arşiv ilke ve uygulamalarına dâhil edilmesi, arşivlerin bilgi ve belgelerin tanımlanmasında söz sahibi tek kurum olmasındaki sürdürülebilirliği destekleyecektir. Ayrıca, hassas bilgileri açığa çıkarmak için kullanılan adli bilişim araçları, erişimin tanımlanması, işaretlenmesi, düzenlenmesi ve kısıtlanması için kullanılabilir.[63]

Anlaşılacağı üzere adli bilişim, arşivcilerin ve belge yöneticilerinin birçok noktada arşivcilik ilke ve prensiplerinini tamamlamalarını sağlar. Bu ilke ve prensipler, provenans, orijinal düzen, aitlik zinciri ve hassas bilgilerin tanımlanması olarak sıralanabilir. Adli bilişim provenans ilişkisinde, belgelerin üretim bağlamı hakkında gerekli bilgilerin tanımlanması, elde edilmesi ve kaydedilmesi işlemleri açısından anlamlıdır. Adli bilişim ile orijinal düzen ilişkisinde, orijinal klasör yapılarını, dosya ilişkilerini, ilgili uygulamaları ve kullanıcı hesaplarını yansıtması açısından anlamlıdır. Adli bilişim aitlik zinciri ilişkisinde, belgelerin nasıl elde edildiğinin belgelenmesi ve herhangi bir dönüşüm yapılıp yapılmadığının görülmesi ve verilerin yanlışlıkla değiştirilmediğinden emin olmak için yerleşik yazılımsal ve donanımsal mekanizmaların kullanılması açısından değerlidir. Adli bilişim ile hassas bilgilerin tanımlanması ilişkisinde, bilginin nerede olduğuna bakılmaksızın kişisel olarak tanımlamayı sağlayan

[62] Christopher A. Lee, "Archival Application of Digital Forensics Methods for Authenticity - Description and Access Provision," s. 4-5, (Çevrimiçi) http://ica2012.ica.org/files/pdf/Full%20papers%20upload/ica12Final00290.pdf, 1 Mayıs 2019.

[63] Lee, **a.g.m.**, s. 5.

düzenleme, iptal etme, kapatma veya kısıtlama için işaretleyicilerin kullanımını desteklemesi açısından önemlidir. Bu ilişkiler üzerinde çalışmalar yapan farklı kurumları görmek mümkündür. Bunlar; Stanford Üniversitesi Kütüphaneleri ve Akademik Bilgi Kaynakları Merkezi (Stanford University Libraries and Academic Information Resources -SULAIR), Londra'daki İngiliz Kütüphanesi (British Library) ve ABD'de Kuzey Carolina Üniversitesi Kütüphane ve Bilgi Bilim Okuludur (UNC School of Information and Library Science).[64]

Arşivcilerin ve belge yöneticilerin adli bilişim ile ilişkilerini daha iyi anlayabilmek adına aşağıda sıralanan maddelere bakılabilir:[65]

- Öncelikle arşivcilerden suçları çözmeleri veya kötü niyetli kullanıcıları yakalamaları beklenmemelidir.
- Teknolojik çözümler denenip başarısız olunduğunda veya farklı bir çözüm de mevcut olmadığında verilerin nasıl kurtarılabileceğini tanımlamak için adli bilişim araçlarına başvurabilir.
- Her zaman hemen görünmeyen yerlerden kanıt elde edebilmek, sistemi bildiklerinden neyin nerede bulunabileceğinin farkındadırlar.
- Dosyalarda yapılan işlemlerin temel özelliklerde (örneğin zaman damgaları) geri dönüşü olmayan değişiklikler yapmamasını sağlamak.
- Yeni teknolojilerle uyumluluğu sağlayabilmek (Güncel format uyumluluğu bazı veri türleri diğerlerinden çok daha hızlı ve sık değişebilir).
- Dijital materyallerle uğraşmak için hâlihazırda mevcut olan çok çeşitli alet ve teknikleri öğrenmek.
- Arşivciler ve belge yöneticileri tarafından yapılan işlemleri belgelemek için uygulamalar (spying, office spying programs) oluşturulur, böylece başkaları onların neleri değiştirebileceklerini bilecektir.
- Dijital adli bilişim için gereken teknik bilgi ile dijital malzemeler arasında ciddi örtüşmeler olduğunu bilirler.

[64] Porter Olsen, "An Introduction to Digital Forensics for Archivists," Sunum Dosyası, (Çevrimiçi) https://digitalapersonarkiv.files.wordpress.com/2014/08/an-introduction-to-digital-forensics-for-archivists.pdf, 25 Şubat 2019.

[65] Olsen, **a.y.**

Adli bilişim, gelişmiş ekipmana sahip uzmanlar yardımıyla farklı veri kurtarma teknikleri kullanır. Normal amacı, normal yöntemler kullanılarak verilere erişimin mümkün olmadığı durumlarda veri saklama ortamlarına erişim alanında uzmanlaşmış yetkin kişilerce ve gerekli donanıma sahip laboratuarlarda sağlanabilir. Bunun yanında arızalı sabit disk sürücülerinden veri kurtarmak ve yasal keşifler yapmak da adli bilişimin amacıdır. Adli şirketler, elektronik aletler kullanarak silinemeyen ancak korunan verileri bir disk sürücüsünde başarıyla kurtarabilir.[66] Söz konusu adli bilişim araçlarında kullanılan bazı algoritmalar vardır. Bunlar aşağıda sıralanmıştır:

5.2.1. Hash Algoritmaları

Arşivleme üstveri üreticisinin bir işlevi, uzun süreli arşivleme için toplanan her dijital belge için bir hash değeri (özet) hesaplamaktır. Günümüzde, çeşitli amaçlarla kullanılan farklı şifreleme hash algoritmaları bulunmaktadır. Güvenli Hash Algoritmalar (Secure Hash Algorithms, SHA'lar) olarak bilinen bir şifreleme hash işlevi kümesi genellikle farklı uygulamalar için kullanılır. Arşivsel üstveri üretmek amacıyla, SHA-2 veya SHA-256 kullanılmaktadır. Bunlar haricinde diğer hash değerlerini hesaplamak için başka şifreleme hash algoritmaları (MD5, SHA1 ve SHA-256) kullanmak da mümkündür.[67]

5.2.2. Hamming ve Golay Algoritmaları (ECC)

ECC Hata Tespiti: Bir sürücü sektörü baş tarafından okunur. Bir okuma hatası olasılığını belirlemek için bir hata algılama algoritması kullanılır. Bir hata durumunun olası görülmemesi durumunda sektör işlenir ve okuma işleminin başarıyla sonuçlandığı kabul edilir. Bunun haricinde diğer hata yönetim mantığı çerçevesinde kullanılan kodlar da söz konusudur. Bunlar;[68] ECC hata düzeltme, otomatik yeniden deneme, gelişmiş hata düzeltme ve hatadır. Söz konusu kodlar aşağıda açıklanmıştır:

---

[66] Gordon Hughes ve Tom Coughlin, **Tutorial on Disk Drive Data Sanitization**, 2007, s. 10. (Çevrimiçi) https://tomcoughlin.com/Coughlin/Techpapers/DataSanitizeTutorial121206b.pdf, 30 Mart 2019.

[67] Sekie Amanuel Majore, Hyunguk Yoo ve Taeshik Shon, "Secure and Reliable Electronic Record Management System Using Digital Forensic Technologies," **The Journal of Supercomputing**, C. 70, S. 1, 2014; s. 160, DOI 10.1007/s11227-014-1137-6.

[68] Wright, Kleiman, ve Sundhar R.S., "Overwriting Hard Drive Data: The Great Wiping Controversy," s. 251.

ECC hata düzeltme: Kontrolör, hatayı denemek ve düzeltmek için sektör için yorumladığı ECC kodlarını kullanır. Bir okuma hatası bu seviyede çok hızlı bir şekilde düzeltilebilir ve genellikle "otomatik düzeltme" olarak kabul edilir.

Otomatik yeniden deneme: Bir sonraki aşama, verileri tekrar okumaya çalışmadan önce sürücü plakasının tam bir dönüş gerçekleştirmesini beklemekten ibarettir. Kaçak manyetik alan değişimleri, sürücü okuma hatasına neden olan yaygın bir durumdur. Bu dalgalanmalar ani hareket ve sıcaklık değişimlerinden kaynaklanabilir. Hata bir yeniden deneme sonrası düzeltilirse, çoğu sürücü "yeniden denedikten sonra düzeltilecek" hata koşulunu değerlendirir.

Gelişmiş hata düzeltme: Birçok sürücü, ilk denemeden sonraki denemelerde, normal düzeltme protokollerinden daha yavaş ve daha karmaşık, ancak daha fazla başarı şansına sahip olan daha gelişmiş hata düzeltme algoritmalarına neden olur. Bu hatalar "çoklu okumalardan sonra kurtarıldı" veya "gelişmiş düzeltmeden sonra kurtarıldı" uyarılarını verir.

Hata: Sürücünün sektörü okuyamaması durumunda, sürücü kontrol cihazına okuma hatası bildiren bir sinyal gönderir. Bu tür bir başarısızlık, kurtarılamaz bir okuma hatasıdır. Modern kodlama şemaları (PRML[69] ve EPRML[70]), sürücü kafasının okuduğu ve veri bütünlüğü kaybı olmadan önemli ölçüde değişmek üzere bir sabit diske yazdığı analog değerlere izin veren geniş bir tolerans aralığına sahiptir. Sonuç olarak, önceki bir yazma değerinin belirlenmesi de stokastik (değişken ve rastlantısal) bir süreçtir.

5.3. Vaka Analizleri (İmhaya Yönelik Örnekler)

Vakalar, imha yöntem ve tekniklerinin yerinde uygulanması açısından önem taşır. Bu nedenle çalışmada vakalara da yer verilmiştir.

[69] PRML (Partial-Response Maximum-Likelihood, Kısmi Yanıt En Yüksek İhtimal), veri depolamada, bir manyetik diskin veya manyetik bant sürücüsünün kafasından elde edilen zayıf bir analog sinyali dijital bir sinyale dönüştürmek için kullanılan bir yöntemdir (Wright, Kleiman, ve Sundhar R.S., "Overwriting Hard Drive Data: The Great Wiping Controversy," s. 245).

[70] EPRML (Extended Partial-Response Maximum-Likelihood, Genişletilmiş Kısmi Yanıt - En Yüksek İhtimal), PRML'nin geliştirilmiş hali olup sabit sürücülerde uygulanabilir olma özelliğine sahiptir (Craig Wright, Dave Kleiman, ve Shyaam Sundhar R.S., "Overwriting Hard Drive Data: The Great Wiping Controversy," s. 245).

5.3.1. Vaka 1[71]

Bir okul, ilkokul eğitimini geliştirmek için, eski ilkokul öğrencilerinin şuan lisede nasıl bir profile sahip olduğunu değerlendirmek istemektedir. Söz konusu okul, ilkokulda eğitimi iyileştirmenin yollarını belirlemek amacıyla bir çalışma yürütmek üzere bir araştırma kuruluşu ile sözleşme yapmaya karar verir. Okul, The Family Educational Rights and Privacy Act (FERPA) çalışmaları istisnası kapsamında araştırma organizasyonu ile yazılı bir anlaşma imzalar. Anlaşmada, aşağıda belirtilen, verilerin gizliliğini ve güvenliğini korumak için açık kurallar ve veri yönetimi gereksinimleri belirlenmiştir:

a) Araştırmanın tamamlanması 8 ayı bulacaktır,
b) Okul tarafından sağlanan veriler, araştırmada belirtilen amaçlar haricinde kullanılmayacaktır,
c) Araştırma kuruluşu, verilere erişimi sınırlandırmak ve güvenli kullanımı sağlamak için tedbirler almak zorundadır,
d) Yüksek şifreleme mekanizmaları için standartlara uygun dosya aktarım işlemi gerçekleştirmelidir,
e) Çalışmanın yürütülmesi için ihtiyaç duyulmayan veriler ve 8 ayın sonunda eldeki veriler imha edilecektir,

Kurum, sözleşmenin sonunda, araştırma için kullanılan araştırma veri setinin güvenli bir şekilde kuruma iade edileceğini, bulguların gelecekteki çoğaltılması veya değerlendirilmesi için gerekli olması durumunda dosyayı arşivleyeceğini ve araştırma organizasyonu tarafından tutulan kalan herhangi bir bölge verisini imha edilmesi gerekmektedir. Yazılı anlaşma ayrıca, araştırma kuruluşunun kullanacağı belirli veri imha yöntemini de öngörmektedir: Bu durumda, veri dosyalarının üzerine rastsal bilgi yazan ve böylece kurtarılamayan verilerin tamamını oluşturan güvenli bir üzerine yazma yardımcı programıyla yapılır. Yazılı anlaşma, araştırma organizasyonu içindeki verilerden çalışma için kullanılmasından sorumlu olan kişiyi ve proje sonunda imhalarından sorumlu olan kişiyi açıkça tanımlar. Anlaşma ayrıca, araştırma kuruluşunun,

[71] U.S. Department of Education Privacy Technical Assistance Center, **Best Practices for Data Destruction**, s. 8.

verileri yok etmekten sorumlu olan kişi tarafından imzalanacak olan veri imha uygulamalarını envantere koyması istenir. Envanterde, bir imha sertifikasyon formu da bulundurulur. Sözleşmenin sonunda, araştırma kuruluşu çalışma veri setini güvenli bir şekilde bölgeye geri gönderir ve verilerin üzerine yazmak için üzerinde anlaşılan bir aracı kullanarak kalan verilerin imha edilmesini sağlar. İmha, yerel idare tarafından sağlanan form, açıklamalı olarak imhadan sorumlu kişi tarafından imzalanır. Çalışmanın yürütülmesi amacıyla, araştırma kuruluşuna yerel idare tarafından sağlanan ulaşım araçları, doldurulmuş doğrulama formu ile idareye güvenli bir şekilde iade edilir.

SONUÇ

Arşiv uygulamaları, geleneksel anlamda belgelerin, üretilmesi, tanımlanması, düzenlenmesi, korunması, kullanılması ve değerlendirilmesi aşamalarının takip edilmesiyle belgelerin süresiz saklanılması veya imha edilmesi ile neticelenmektedir. Farklı işlemlerden oluşan arşiv çalışmaları, tarihin ilk arşiv kurumlarının faaliyete geçmesinden itibaren arşivciler tarafından uygulanmaktadır. Mesleki uygulama ilkelerine ilişkin teorik yaklaşımlar zaman içerisinde hem meslektaşlar hem de arşivlerden yararlanan araştırmacılar tarafından geliştirilmiştir. Yüzyılı aşkın bir zamandan beri arşivciler tarafından uygulanmakta olan bu ilkeler günümüz arşivlerinde fiilen yürütülen hizmetler bakımından belirgin bir öneme sahiptir. Ancak kabul görmüş arşiv ilkelerine dayanan bu uygulamalar; arşiv belgelerinin üzerine kaydedildiği bilgi taşıyıcılarının çeşitlenmesiyle birlikte üzerinde yeniden düşünülen uygulamalar haline geldiler. Bu durum, mevcut teorik yaklaşımların söz konusu yeni sorunlar karşısında -kısmen- yeni çözüm yolları ve yeni yaklaşımlar sunmasını da beraberinde getirdi. Geleneksel -kâğıt-ortam için uygulanan yukarıdaki aşamaların, -ortam değişikliği dikkate alınarak- elektronik ortama uyarlanması gerekmektedir. Belgelerin, üretilmesi, tanımlanması, düzenlenmesi, korunması, kullanılması ve değerlendirilmesi aşamalarının, elektronik ortamda uygulama fırsatı sunan EBYS'lerde arşiv uygulamalarının etkin ve yeterli bir şekilde tasarlanmasıyla verimlilik noktasında geleneksel anlamdaki katkılar elde edilmektedir. Tam tersi durumunda bile büyük hasarlara yol açabilecek durumlarla karşılanabilir.

Günümüzde elektronik ortamdaki belgelerin üretimi ve kullanımı EBYS'lerle sağlanmaktadır. Ancak saklama süreleri ve bu süreler sonunda belgelerin imha edilmesinin nasıl yapılacağı netlik kazanmış değildir ve EBYS'ler bu konuda yetersiz sayılır. Ayrıca, elektronik belgelerin imha edilmesiyle ortam kaynaklı geride bırakılan izlerden, silinmiş olan belgelere erişim mümkün görünmektedir. Elektronik belgelerin ve izlerinin tamamen yok etmenin mümkün olup olmadığı tartışılan bu araştırmada, öncelikle imhayı anlamlı kılacak arşivsel değerlendirmenin dünyadaki geleneksel anlayışlarından bahsedildi. Değerlendirmenin diğer arşiv işlemleriyle temel bir işlevi olması, özellikle imhayla yakından ilgili olması, değerlendirmeyi daha da önemli hale getirmektedir.

Temel arşiv uygulamalarından olan değerlendirme, fiziksel ortamdaki belgeler için uygulanan arşiv teorilerinin nasıl oluşturulduğunun ve günümüze kadar hangi evrelerden geçtiğinin bilinmesi, günümüz elektronik ortamdaki belgelerin nasıl bir yaklaşımla ele alınması gerektiğini göstermek açısından önemlidir. Özellikle belgelerin değerlendirilmesine ilişkin teorilerin nasıl ortaya atıldığı ve bu teorilerin ne kadar başarılı olduğunu bilmek, her ne kadar belgenin bulunduğu ortam farklılık arz etse de, yaklaşımların belirlenmesinde takip edilmesi gerekli adımlardır.

Özellikle Almanya, İngiltere ve ABD bağlamında arşivsel değerlendirmenin Türkiye'deki arşivsel değerlendirmeyi de etkilediğini söylemek mümkündür. Koruma (arşivlerin kültürel miras ve uzun vadede kanıtlayıcı değeri) için değerlendirme yapan Almanya, imha etmek (idari, mali ve kısa vadeli amaçlar yer kazanma gibi) için değerlendirme yapan İngiltere değerlendirme anlayışları, Schellenberg'ing her iki yaklaşımı sentezlemesiyle ABD'de iki yaklaşımın tertibi şeklinde değerlendirmeyi mümkün kılmıştır. Batılıların custodial olarak nitelendirdiği dönem olan geleneksel arşivcilik ve değerlendirme işlevi, bilgisayar ve internetin belgeler için yeni bir ortam sunmasıyla söz konusu dönemin bitişini gerçekleşmiştir. Yeni ortamla beraber custodial dönemi, post-custodial dönem olarak karşımıza çıkmıştır. Post-custodial dönem, önceki dönemde geçerli olan değerlendirme anlayışlarının ortama bağlı olarak modeller sunmasını gerekli kılmıştır. Özellikle elektronik belge yönetim sistemleri modelleri olarak adlandırabileceğimiz Avrupa idari modeli olan arşivsel model, Anglo-Sakson modeli olan belgelerin yaşam döngüsü modeli ve Avustralya modeli olan belge sürekliliği modeli günümüz elektronik ortamdaki belgelerin sistem süreçlerine ilişkin bilgiler vermektedir. Bu modeller ayrıca önceki değerlendirme anlayışlarının döneme göre yeniden şekillenmiş niteliği taşır.

Söz konusu modeller, teorik bir düşünce olmaktan ziyade, günümüz elektronik belge yönetim sistemlerinin uygulanması için yazılı dokümanlar da sunmaktadır. Avrupa idari modeli için ortaya konan MoReq2010 ve öncesi sürümler, Avrupa Birliği (AB) ülkeler için referans olmakla beraber, AB aday adayı ülkeler için de bir rehber niteliğindedir. Belgelerin yaşam döngüsü için ABD Savunma Bakanlığı tarafından hazırlanmış olan DOD 5015.2-STD dokümanı Anglo-Sakson yaklaşımının sistemsel halini yansıtır. Yine Avustralya belge sürekliliğini ortaya koyan Frank Upward'ın belge

yönetimi ve arşivi birleştiren iki temel yazısı önemlidir. Bu dokümanlar, yaklaşım ve modele bağlı olarak farklı uygulama yazılımlarının sistem standartları olarak kullanılmasını sağlamaktadır. Söz konusu dokümanların sistem kriterlerinde elektronik imhanın, belgelerin geride izler bırakmayacak şekilde imha edilmesini ön görmektedir. Buradaki izlerden kasıt sistemi meydana getiren yazılımsal ve donanımsal bileşenlerin barındırdıkları veri veya çeşitli tekniklerle silinmiş olsa bile bu bileşenlerdeki veriye tekrar erişim imkânının olmasıdır. Bu elektronik belge ve izlerinin imha edilmesi sorunu, arşivcilik mesleğinin karşı karşıya olduğu güncel ve önemli sorunlardan biri olan bilgi teknolojileri olarak bilinen yeni teknolojiler tarafından dolaylı olarak üretilen sorunlardır. Arşivciliğin önemli aşamalarından olan imha uygulamalarının elektronik ortamda da gerçekleştirilmesi, ortamdan kaynaklı problemleri beraberinde getirmektedir. Belgelerin yaşam döngüsünde önemli bir süreç olan belgelerin değerlendirilmesi ve değerlendirme sonucunda gerekli imha uygulamalarının yapılması, elektronik ortam için kaçınılmazdır.

Konuya ilişkin elektronik belge yönetim sistemlerine yönelik uluslararası standartlara bakıldığında, elektronik imhanın ve elektronik işlem izlerinin farkındalığı açıkça ortaya konmuştur. Elektronik belge ve izlerinin tamamen nasıl yok edileceği ise yazılımsal olarak verinin üzerine yazma ve donanımsal olarak da fiziksel imha yöntemleriyle olabileceği şeklinde değerlendirilmektedir. Ancak bu yöntemlerin ne şekilde olacağını başka dokümanlarda görmekteyiz. Bu dokümanlar, Almanya, ABD, Avustralya, İngiltere, Kanada, Rusya ve Yeni Zelanda gibi gelişmiş ülkeler tarafından uluslararası elektronik veri ve izlerinin imhası için kullanılan standartlardır. Bu standartların özellikle bazı ülkelerdeki askeri kurumlarca hazırlanmaları dikkat çekicidir. Söz konusu standartların uygulama yazılımı halinde ticari amaçlarla kamu dışında özellikle özel sektör tarafından hazırlandığı görülmektedir. Birçok yazılım söz konusu iken bunların kısmi işlevli olarak ücretsiz kullanıldığı gibi tam işlevli olanların ise ücretli olduğu görülmektedir. Yukarıda ifade edilen ülkeler bağlamında geliştirilen standartlardaki işlevleri yerine getiren söz konusu yazılımların bir kısmı yazılımsal ve donanımsal olarak imha edilmiş veriye ve izlerine tekrar erişim imkânı vermezken bazılarında tam tersi bir durum söz konusudur. Bu nedenle yazılımsal olarak hazırlanan

veri imha yöntem ve tekniklerin tamamının istenen şekilde veriyi imha etmesi mümkün değildir. Ayrıca, tek bir yöntemle, silinmek istenen verinin yazılım ve donanım bileşenlerinden silinmesi de imkânsızdır. Bu yüzden verinin bulundukları ortamın tanımlanması daha sonra tanımlanan bileşenlerdeki veriyi ve bileşenlerin kendisini imha etmek veriyi tamamen yok etmeye yardımcı olur.

Elektronik veri ve izlerinin tamamen yok edilmesinin Türkiye'deki kamu kurum ve kuruluşlarındaki durumunu değerlendirdiğimizde yasal düzenlemelerin bu durum üzerindeki payı büyüktür; ancak belge yönetimi ve arşiv hizmetlerine yönelik düzenlemelerin tarihi süreçte çeşitli nedenlerle sürekli olarak değiştirildiği ve bu değişikliklerin bir bütün oluşturmadığı görülmektedir. Bu nedenle, arşiv uygulamaları açısından önemli olan arşiv imha teorisinin elektronik ortam için uygulanmamasında yazal düzenlemelerdeki değişikliğin de etkisi olduğu düşünülmektedir. Evrak imha uygulamalarına yönelik çıkarılan ilk nizamnamenin 102 yıl önce yayınlanmış olması arşiv imha uygulamalarının Türkiye'de bir geçmişe sahip olduğunu ve buna yönelik yasal düzenlemenin de yapıldığını göstermiş olsa da istenilen uluslararası seviyeye gelinememiştir. Yasal düzenlemelerin eksikliği yanında Türkiye tarihindeki ekonomik, sosyal ve kültürel değişimler de arşivlere yönelik uygulamaları sekteye uğratmış veya geç uygulanmasına neden olmuştur. Söz konusu uygulamaların ikincil mevzuat ile hayata geçirilmesi söz konusu olmuştur. Ancak bu durum alanda eksikliği başat şekilde hissedilen birincil düzeydeki mevzuat eksikliğinin giderilmesini sağlamak için yeterli olmamıştır. 1988 yılının Mayıs ayında yayınlanan Devlet Arşiv Hizmetleri Hakkındaki yönetmelik ve 1988 yılının Ekim ayında yayınlanan evrak ve malzemenin yok edilmesine yönelik kanun ile çok önemli gelişmeler söz konusu olmuşsa da daha sonraki düzenlemeler bu düzenlemelerin bütünlüğünü ve teknolojik gelişmelerin hızlı seyrini yakalamak için yeterli olmamıştır. Örneğin, Devlet Arşiv Hizmetleri Hakkındaki Yönetmelik, 2005 yılında bazı maddelerinin değiştirilmiş olması teknolojik yeniliklerin getirdiği zorunlulukların kurumlarda arşiv temelli olarak uygulanmasını sağlayamamıştır. Özellikle elektronik belgelerin imhası ile ilgili süreçlerin EBYS standardı olan TS 13298 gibi düzenlemelerde yer almaması da bu durumun devam etmesine yol açmıştır. Bu standartta, elektronik belgenin imhasının yanı sıra belge izleri noktasında da hiçbir açıklama yer almamaktadır.

2016 yılında kurulan KVKK ile beraber hazırlanan ikincil düzenleme ve rehberler kişisel verilerin elektronik ortamda hangi yöntemlerle silineceğini ifade etmesi açısından önemli bir gelişme olarak görülmektedir. Bu düzenlemenin gerekliliği yanında Devlet arşiv hizmetlerine yönelik benzer çalışmanın olmayışı bütünlük açısından olumsuz bir durumdur. 11 nolu Cumhurbaşkanlığı Kararnamesiyle de Devlet Arşivleri Başkanlığı Hakkındaki düzenlemeler belirtilmiştir. Elektronik verinin imhasını içeren bir düzenlemenin kararnamede Devlet Arşivleri Başkanlığı tarafından yapılacağını belirten hiçbir madde görülmemektedir. Yayınlanan Devlet Arşiv Hizmetleri hakkındaki yönetmelikte elektronik imha yöntem ve tekniklerin belirtilmesi konusunda kurum üst amirlerine yetki verildiği görülmektedir. Bunun yanı sıra özelliği gereği imha şekli kendi mevzuatında belirlenmiş belgenin ilgili mevzuat gereği uygunlanması istenmektedir. İmha yöntem ve tekniklerin kurum belge yönetimi ve arşiv hizmetlerine ilişkin yönergelerinde yer alması gerektiğine dikkat çekilmemiştir. Türkiye'deki durum bu şekilde özetlenebilir.

Arşiv uygulamaları açısından önemli bir aşama olan elektronik belge ve izlerinin imha edilmesi problemini ele alan bu araştırma, elektronik ortamdaki belge ve izlerinin güncel ortam ve güncelliğini yitirmiş ortam olarak ayrılması gerektiği sonucuna varmıştır. Varılan bu sonuca göre güncel ortamdaki verinin silinmesinde yazılımsal yöntem ve teknikler kullanılması gerektiğine dikkat çekilmektedir. Üzerine yazmak ve manyetiksizleştirmek dikkat çekilen en etkili yöntemlerdir. Güncelliğini yitirmiş ortamdaki verinin imhasında ise hem yazılımsal hem de donanımsal (fiziksel) imha yöntemleri söz konusudur. Yazılım için üzerine yazma ve manyetiksizleştirme kullanılmaktadır. Güncelliğini yitiren saklama ortamları için üzerine yazma işleminin yeterli görülmediği, bu işlemden sonra ortamın veya ortamların demanyetize edilmesinin de gerekliliği sonucu da elde edilmiştir. Fiziksel imha için de pek çok teknik kullanılmaktadır. Eritme, yakma, parçalama bunlardan sadece birkaçıdır. Elde edilen bu sonuçlarla beraber güncel ve güncelliğini yitirmiş ortamdaki verinin imhası sadece veriyi silmekle veya verinin bulunduğu donanımı imha etmekle yok olmayacağı sonucunu da ortaya koymaktadır. Ayrıca bunların sistemlerde bıraktıkları izlerin de silinmesi gerekliliği de söz konusudur. Sistemlerdeki izlerin tanımlanması ayrıca gerekli ve önemlidir. Tanımlanan sistem izleri sistem içindeki çeşitli uygulama izleri, veri tabanı izleri,

yazılım izleri, format izleri ve kopya/duplikasyon izleridir. Bunlar yazılımsal izler olarak ifade edilmektedir. Donanımsal anlamdaki izlere ise internet/intranet izleri, tarayıcı (arama motorları) izleri, işletim sistemi izleri, farklı uygulama (medya oynatıcılar, fotoğraf araçları, indirme araçları, arşivleyiciler, ofis programları, diğer programlar) izleri, ağ izleri, sunucu (server) izleri, depolama izleri, yedekleme izleri, erişim izleri, yazıcı/tarayıcı izleri, mobil izleri, bulut izleri, elektronik imza izleri ve taşınma/dönüşüm/transfer (belge devri) izleridir.

Elektronik belgelere yönelik izlerde, özellikle internet günlüğünün, bireysel izlerin, sistem izlerinin ve çeşitli üçüncü parti programların silinmesi önemlidir. İnternet günlüğünün silinmesinde en çok kullanılan arama motorlarının ve iletişim programlarındaki izlerin silinmesi de gereklidir. Bireysel izlerin silinmesinde, çeşitli listeler, loglar, önbellek, geçici dosyalar, indirilenler ve diğer kişisel izler önem arz etmektedir. Sistem izlerinin silinmesinde, kayıt izleri, taslak dosyalar, sistem geçmişi ve çeşitli log dosyalarının göz önünde bulundurulması gerekir. Son olarak çeşitli üçüncü parti programlarındaki izlerin silinmesinde, önbellekteki veriler, loglar, geçici dosyalar, en son kullanılan dosya listesi ve uygulamaların bıraktığı diğer izlerin silinmesi arşiv imha teorisinin gerçekleştirilmesini sağlamaktadır.

Elektronik belgelerin imha edilmesinde kullanılan iki temel yöntem vardır. Bunlar; üzerine yazma ve fiziksel imhadır. İki temel yöntem yanında birçok imha tekniği bulunmaktadır. Bunun yanında elektronik ortamdaki imhanın gelecekteki teknolojilerin kullanımına göre değişebileceği açıktır. Yeniden kullanılacak ortam (sabit sürücüler, yeniden yazılabilir diskler vb.) için de üzerine yazma işlemi gerçekleştirilir. Çalışır durumdaki sabit diskler de tamamen fiziksel olarak tahrip edilmeli ya da içindeki bilgilerin ayıklanması yoluna gidilmelidir. Eğer sabit sürücü çalışamaz durumdaysa veya kullanım ömrünün sonuna gelindiyse fiziksel olarak yok edilmelidir.

Hem elektronik belgeyi (bulunduğu ortama göre) hem de elektronik belgenin yazılımsal ve donanımsal izleri imha etmek için uluslararası imha standartlarına göre geliştirilen yazılımlar kullanılmaktadır. Bu yazılımlar ticari amaçla geliştirilmiş tam işlevli ve imha standartlarına uygun olarak çalışmaktadır. İmha edilmek istenen veriyi zamansal olarak en kısa sürede imha eden yöntemler de tam işlevli olan yazılımlarda mevcuttur. Gelişmiş ülkelerin kendi standartlarını oluşturduklarını, veri imha alanında

kendi iç çözümlerini ortaya koyduklarını ve bu çözümlerini ticari bir araç olarak kullanabileceklerini göstermektedir; ancak bu yazılımların yazılımsal veya donanımsal olarak veriye tekrar erişim sağlayabilecek araç ve yöntemlere izin vermeme kabiliyetinin olması önemlidir. Türkiye'de böyle bir yazılım henüz geliştirilmemiştir. Ancak kamu yönetiminde etkin belge yönetim ve arşiv fonksiyonlarını yerine getirmek için bu yazılımlara acilen ihtiyaç duyulmaktadır. Bunun için yasal düzenlemelerin ve teknik bilginin arşivsel bilgiyle bütünleşmiş bir yaklaşımı ortaya konmalıdır. Ayrıca elektronik imhanın başarılı bir şekilde yapılabilmesi için teori, teknoloji, değişim yönetimi ve proje yönetimi ile ihtiyaç duyulan diğer temel bilgi ve belgeler de gereklidir.

Dijital ortam geleneksel ortama göre daha fazla belge üretimini tetikledi. Özellikle üretime hazırlık malzemelerinin elektronik ortamda imha edilme gerekliliği zaman geçtikçe daha fazla hissedilmektedir. Sistem üzerinde, çok fazla belgenin duramayacağı ve bunun için dijital imha mühendisliklerinin ortaya çıkması muhtemeldir. Bu konuda hangi politikalar oluşturulursa oluşturulsun, kamu kurum ve kuruluşlarındaki çalışanların izleyebilmeleri için açık kurallar ve -modern çağın arşiv uygulamaları söz konusu olduğunda- etkili yöntemler kullanmak önemlidir. İmha konusundaki kötü algının da kaldırılması ancak bu şekilde mümkün görünmektedir.

Türkiye'de kamu kurum ve kuruluşlarındaki elektronik belge yönetimi ve arşiv uygulamalarının temel bileşenlerinden olan imhanın hem belge için hem de belge izleri için tasarlanması gereklidir. Ayrıca ihtiyaç duyulan yazılımın da geliştirilip EBYS içinde kullanılması mümkün hale getirilmelidir. Bunlar haricinde, fiziksel imhanın kurum içinde yapılabilmesinin kurgusu düşünülmelidir. İhtiyaç duyulan yazılımın geliştirilmesi, birçok kurumun ortak çalışma ürünü olarak ortaya konulabilir. Öncelikle Devlet Arşivleri Başkanlığı ve Adalet Bakanlığının kurumlardaki belgeler için hukuki imha kodları belirlemeleri gerekir. Daha sonra bu kodlara bağlı olarak TÜBİTAK ve BTK'nın teknik desteği sağlanmalıdır. Kamu kurumlarında uygulanması için TÜBİTAK, özel sektörde uygulanması için de BTK görevlendirilebilir. Ayrıca bu konuda bilinçlendirme programları kapsamında Milli Eğitim Bakanlığı ile Devlet Arşivleri Başkanlığı iştirakinde sınıf içi ve sınıf dışı ders ortamlarında hatta üniversitelerde ortak çalışmalar yapılabilir. Ayrıca askeri kurumlar için ASELSAN'ın bilgi ve tecrübesinden yararlanılabilir.

KAYNAKÇA

"3473 sayılı tarihli Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanun:"	**Resmi Gazete**, Sayı: 19949, Tarih: 04.10.1988 http://www.resmigazete.gov.tr/arsiv/19949.pdf, 14 Haziran 2019. (Son Erişim Tarihi: 3 Aralık 2019)
"5070 sayılı Elektronik İmza Kanunu:"	**Resmi Gazete**, 23 Ocak 2004, S. 25355.
"5271 sayılı Ceza Muhakemesi Kanunu:"	Madde: 134, **Resmi Gazete**, Sayı: 25673, Tarih: 17.12.2004, (Çevrimiçi) http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf, 21 Nisan 2019. (Son Erişim Tarihi: 3 Aralık 2019)
"Devlet Arşiv Hizmetleri Hakkında Yönetmelik:"	**Resmi Gazete**, Sayı: 19816, Tarih: 16.05.1988, Madde 39, (Çevrimiçi) http://www.resmigazete.gov.tr/arsiv/19816.pdf, 13 Haziran 2019. (Son Erişim Tarihi: 3 Aralık 2019)

"Devlet Arşiv Hizmetleri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik:"	**Resmi Gazete**, Sayı: 24487, Tarih: 08.08.2001, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2001/08/20010808.htm#6, 13 Haziran 2019. (Son Erişim Tarihi: 3 Aralık 2019)
"Devlet Arşiv Hizmetleri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik:"	**Resmi Gazete**, Sayı: 25735, Tarih: 22.02.2005, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2005/02/20050222-8.htm, 13 Haziran 2019. (Son Erişim Tarihi: 3 Aralık 2019)
"Devlet Arşiv Hizmetleri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik:"	**Resmi Gazete**, Sayı: 25735, Tarih: 22.02.2005, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2005/02/20050222-8.htm, 21 Haziran 2019. (Son Erişim Tarihi: 3 Aralık 2019)
"Devlet Arşiv Hizmetleri HakkındaYönetmelik:"	Madde 45, **Resmi Gazete**, Sayı: 19816, Tarih: 16.05.1988, (Çevrimiçi) http://www.resmigazete.gov.tr/arsiv/19816.pdf, 13 Haziran 2019. (Son Erişim Tarihi: 3 Aralık 2019)

"Devlet Arşiv Hizmetleri HakkındaYönetmelik:"	**Resmi Gazete**, Sayı: 30922, Tarih: 18.10.2019, (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2019/10/20191018-9.pdf, 25 Ekim 2019. (Son Erişim Tarihi: 3 Aralık 2019)
"Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi-Kararname Sayısı 11:"	**Resmi Gazete**, Sayı: 30480, Tarih: 16.07.2018, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2018/07/20180716-1.pdf, 13 Haziran 2019. (Son Erişim Tarihi: 3 Aralık 2019)
"Kayıtlı Elektronik Posta (KEP) Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik:"	**Resmi Gazete**, Sayı: 28036, Tarih: 25.08.2011, (Çevrimiçi) http://www.resmigazete.gov.tr/eskiler/2011/08/20110825-7.htm, 21 Haziran 2019. (Son Erişim Tarihi: 3 Aralık 2019)
"Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik:"	Madde 5, **Resmi Gazete**, Sayı: 30224, Tarih: 28.10.2017, (Çevrimiçi) Haziran 2019 tarihinde http://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm, 13 Haziran 2019. (Son Erişim Tarihi: 3 Aralık 2019)

"Marmara Üniversitesi Kurumsal Belge Yönetimi Yönergesi:"	Sayı: 337-3-C, Tarih: 28.07.2015, (Çevrimiçi) http://dosya.marmara.edu.tr/www/mevzuat/yeni4/mu_kurumsal_belge_yonetimi_yonergesi_senato_web_versiyonu.pdf, 21 Haziran 2019. (Son Erişim Tarihi: 3 Aralık 2019)
"Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun Hükmünde Kararname ve İçişleri Komisyonu Raporu:"	Esas No: 1/418, Tarih: 04.04.1988, (Çevrimiçi) https://www.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d18/c014/tbmm18014005ss0073.pdf, 14 Haziran 2019. (Son Erişim Tarihi: 3 Aralık 2019)
"Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production:"	Sedona Conference, 2003.
"The History of Hacking:"	(Çevrimiçi) http://plaza.ufl.edu/ysmgator/projects/project2/history.html, 11 Kasım 2019. (Son Erişim Tarihi: 3 Aralık 2019)

"What is in the Index.dat files?"	(Çevrimiçi) https://www.milincorporated.com/a3_index.dat.html, 12 Temmuz 2019. (Son Erişim Tarihi: 3 Aralık 2019)
A. Lee, Christopher:	"Archival Application of Digital Forensics Methods for Authenticity - Description and Access Provision," (Çevrimiçi) http://ica2012.ica.org/files/pdf/Full%20papers%20upload/ica12Final00290.pdf, 1 Mayıs 2019. (Son Erişim Tarihi: 3 Aralık 2019)
Adam, Azad:	**Implementing Electronic Document and Record Management Systems**, New York, Auerbach Publications, 2008.
Amanuel Majore, Sekie, Hyunguk Yoo ve Taeshik Shon:	"Secure and Reliable Electronic Record Management System Using Digital Forensic Technologies," **The Journal of Supercomputing**, C. 70, S. 1, 2014; s. 160, ss. 149–165, DOI 10.1007/s11227-014-1137-6.
American Bar Association:	**Record Retention And Destruction Current Best Practices**, 2003, (Çevrimiçi) https://apps.americanbar.org/buslaw/newsletter/0019/materials/record-retention.pdf, 28 Aralık 2017. (Son Erişim Tarihi: 28 Aralık 2017)
Ankara Üniversitesi:	"e-BEYAS Uygulama Kuralları," (Çevrimiçi) http://beyas.ankara.edu.tr/uygulama-kurallari/, 22 Haziran 2019. (Son Erişim Tarihi: 04 Aralık 2019)
AOMEI Backupper:	"Backup Scheme," (Çevrimiçi) https://www.backup-utility.com/screenshot/en/adv/backup/popup/enable-backup-scheme.png, 21 Temmuz 2019. (Son Erişim Tarihi: 04 Aralık 2019)
Appraisal and Disposal:	(Çevrimiçi) http://www.paradigm.ac.uk/workbook/pdfs/04_appraisal_disposal.pdf, 10 Kasım 2016. (Son Erişim Tarihi: 4 Aralık 2019)
Archive Making:	Archive Making, Oxford: The Clarendon Press, 1922.

Archives New Zealand Part of Part of the Department of Internal Affairs:	"Methods of Destruction," July 2016/F1, v1.0. (Çevrimiçi) https://records.archives.govt.nz/assets/Guidance-new-standard/16-F1-Methods-of-destruction.docx, 07 Aralık 2017. (Son Erişim Tarihi: 7 Aralık 2017)
Archives New Zealand:	**Annual Report 2004**, Wellington, Archives New Zealand, 2004.
Archives of Manitoba Government Records Office:	**Recordkeeping Fact Sheet, Recordkeeping Standard**, 2019, (Çevrimiçi) https://www.gov.mb.ca/chc/archives/gro/recordkeeping/docs/recordkeeping_standards_fact_sheet.pdf, 31 Mayıs 2019. (Son Erişim Tarihi: 4 Aralık 2019)
Arşivcilik Terimleri Sözlüğü:	**Arşivcilik Terimleri Sözlüğü**, Çev. ve Gnş. Bekir Kemal Ataman, İstanbul, Librairie de Péra, 1995.
Association for Information and Image Management International (AIIM):	**Recommended Practice: Analysis, Selection, and Implementation of Electronic Document Management Systems (EDMS)**, AIIM International, USA, 2009.
Ataman, Bekir Kemal:	"Enformasyon Bilimlerine Fütüristik Bir Yaklaşım," **Bilgi Dünyası**, C. 9, S. 1, 2008, ss. 67-89.
Atherton, Jay:	"From Life Cycle to Continuum: Some Thoughts on the Records Management - Archives Relationship," **Archivaria,** Winter 1985-1986, C. 21, ss. 43-51.
Attri, Aruna:	"10 Best File Eraser Software 2019," (Çevrimiçi) https://www.stellarinfo.com/blog/best-file-eraser-software/, 1 Kasım 2019. (Son Erişim Tarihi: 4 Aralık 2019)

Aydın, Bilgin:	"Osmanlı Devleti'nde Evrak İmha ve Muhafazasına Dair Neşredilen İlk Nizamname Layihası," **Arşiv Araştırmaları Dergisi**, , S. 1, 1999.
Aydın, Cengiz:	"Elektronik Belgelerin Arşivlenmesi ve Erişim," **Yayımlanmamış Doktora Tezi**, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, 2010.
Bağcılar Belediyesi:	**Kişisel Veri Saklama ve İmha Politikası**, 2018, (Çevrimiçi) http://www.bagcilar.bel.tr/Files/Dokuman/kvk_2018/KVKVeriSaklamaveimhapolitikasi.pdf, 13 Kasım 2018. (Son Erişim Tarihi: 4 Aralık 2019)
Barry, Sean:	"Smoking Microchips Tells It All: Computer Forensic Experts Mine Hard Drives For Data That Too-Clever Users Thought Long Deleted," (Çevrimiçi) http://www.dataforensics.com/articles/smoking_microchip_tells_it_all.pdf, 15 Nisan 2016. (Son Erişim Tarihi: 4 Aralık 2019)
Bayın, Gamze, Gözde Yeşilaydın ve Okan Özkan:	"Bulut Bilişimin Sağlık Hizmetlerinde Kullanımı," **Sosyal Bilimler Dergisi**, S. 48, 2016, s. 233-253.
Beal, Vangie:	"Structure Data," (Çevrimiçi) https://www.webopedia.com/TERM/S/structured_data.html, 13 Ekim 2019. (Son Erişim Tarihi: 4 Aralık 2019)
Beal, Vangie:	"Unstructured Data," (Çevrimiçi) https://www.webopedia.com/TERM/U/unstructured_data.html, 13 Ekim 2019. (Son Erişim Tarihi: 4 Aralık 2019)
Booms, Hans:	"Gesellschaftsformen und Uberlieferangsbildung; Zur Problematik archivalischer Quellenbewertung" [Social Systems and the Selection of Records; On the Problems of Appraisal in Archives], **Archivalische Zeitschrift**, 1972, C. 68, ss. 3-40.

Breuel, Thomas M.:	"The Future of Document Imaging in the Era of Electronic Documents," (Çevrimiçi) https://pdfs.semanticscholar.org/8867/20e7c6fae33799e9768af3e365dde4f8d6ac.pdf, 19 Şubat 2019. (Son Erişim Tarihi: 4 Aralık 2019)
Brooks, Philip Coolidge:	"The Selection of Records for Preservation," **American Archivist**, October 1940, C. 3, S. 4, ss. 221-234.
California Records & Information Management (CalRIM):	**Electronic Records Management Handbook**, 2002, (Çevrimiçi) https://www.documents.dgs.ca.gov/osp/recs/ermhbkall.pdf, 11 Temmuz 2019. (Son Erişim Tarihi: 11 Temmuz 2019)
Cambridge Dictionary:	"Capture", (Çevrimiçi) https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/capture , 28 Aralık 2018. (Son Erişim Tarihi: 4 Aralık 2019)
Cambridge Dictionary:	"Data Capture", (Çevrimiçi) https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/data-capture , 28 Aralık 2018. (Son Erişim Tarihi: 4 Aralık 2019)
Clark, John F.:	"History of Mobile Applications: Theory and Practice of Mobile Applications," (Çevrimiçi) http://www.uky.edu/~jclark/mas490apps/History%20of%20Mobile%20Apps.pdf, 14 Kasım 2019. (Son Erişim Tarihi: 4 Aralık 2019)
Clark, Tom:	**Designing Storage Area Networks: A Practical Reference for Implementing Fibre Channel IP SANs**, Second Edition, Addsion-Wesley, Boston, 2003.
Corporate Document Destruction:	"e-Waste Destruction and Recycling," (Çevrimiçi) https://www.corporatedocumentdestruction.com.au/e-waste-destruction-and-computer-recycling-melbourne/e-waste-destruction-and-recycling, 21 Eylül 2019. (Son Erişim Tarihi: 4 Aralık 2019)

Couture, Carol:	"Archival Appraisal: A Status Report," **Archivaria**, Spring 2005, No: 59, ss. 83-107.
Craig, Barbara L.:	"Doing Archival Appraisal in Canada. Results from a Postal Survey of Practitioners' Experiences, Practices, and Opinions," **Archivaria**, Fall 2007, C. 64, ss. 1-45.
Cunningham, Adrian:	Relationships Between the ISO 16175 Series of Standards and Other Products of ISO/TC46/SC11: Archives/Records Management, https://www.ica.org/sites/default/files/PCOM_2012-06_ISO%20paper_ACunningham_EN.pdf, 2 Haziran 2019. (Son Erişim Tarihi: 4 Aralık 2019)
Çiçek, Niyazi:	"Belgelerin Dokümanter Yapısı," **Arşiv Dünyası,** S. 13, 2012, s. 32-38.
Çiçek, Niyazi:	**Kurumsal Bilgi ve Belge Yönetimi**, 2. bs., İstanbul, Marmara Belediyeler Birliği Kültür Yayınları, 2018, s. 110.
Dartmouth College:	**The Document Life Cycle: Definitions, Supporting Technologies, and Applications**, (Çevrimiçi) https://www.dartmouth.edu/~library/recmgmt/forms/DocLifeCycle.pdf, 6 Ocak 2019. (Son Erişim Tarihi: 4 Aralık 2019)
Dascher, Ottfried:	"Archivar und Historiker. Zum Standort eines Beruf im Wandel von historischen Interessen und Methoden" [Archivist and Historian. The State of a Trade Changed by Historical Interests and Methods], **Der Archivar**, 1983, C. 36.
Data Destroyers:	"Data Carrier Sanitization," (Çevrimiçi) https://www.datadestroyers.eu/technology/data_carrier_sanitize.html, 31 Temmuz 2019. (Son Erişim Tarihi: 4 Aralık 2019)
Dealna:	"Three Types of Server Hardware," (Çevrimiçi) https://dealna.com/en/Article/Post/1391/Three-Types-of-Server-Hardware, 17 Temmuz 2019. (Son Erişim Tarihi: 4 Aralık 2019)
Delaney, Hayden ve Briar Francis:	"Electronic Signatures and Their Legal Validity in Australia," (Çevrimiçi) https://www.findlaw.com.au/articles/5777/electronic-signatures-and-their-legal-validity-in-.aspx, 27 Temmuz 2019. (Son Erişim Tarihi: 4 Aralık 2019)

DGD Deutsche Gesellschaft für Datenschutz GmbH:	"Erasure Standards," (Çevrimiçi) https://dg-datenschutz.de/services/data-erasure/data-erasure-standards/royal-canadian-mounted-police-tssit-ops-ii/?lang=en, 29 Mart 2019. (Son Erişim Tarihi: 29 Mart 2019)
DLM Forum Foundation:	**MoReq2010®: Modular Requirements for Records Systems — Volume 1: Core Services & Plug-in Modules**, 2011, (Çevrimiçi) http://moreq2010.eu/, 31 Ocak 2019. (Son Erişim Tarihi: 5 Aralık 2019)
DocuSign:	"What are digital signatures?," (Çevrimiçi) https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq, 22 Kasım 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Doğuş Üniversitesi:	**Kişisel Veri Saklama ve İmha Politikası**, (Çevrimiçi) https://www.dogus.edu.tr/docs/default-source/dokumanlar/ki%C5%9Fisel-verileri-saklama-ve-imha-politikas%C4%B1.pdf?sfvrsn=79ec4bf8_0, 21 Haziran 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Dr. İshak Keskin:	Dr. İshak Keskin ile yapılan görüşme.
Dr. Öğr. Üyesi M. Fahri Furat:	Dr. Öğr. Üyesi M. Fahri Furat ile yapılan görüşme.
Dudullu OSB Boğaziçi Üniversitesi Teknopark A.Ş.:	**Kişisel Verilerin Korunması Politikası,** (Çevrimiçi) http://www.budotek.com.tr/wp-content/uploads/2019/02/kisisel.pdf, 21 Haziran 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Duranti, Luciana:	"The Concept of Appraisal and Archival Theory", **American Archivist**, Spring 1994, C. 57, S. 2, ss. 328-344.
Eastwood, Terry v.d.:	**Currents of Archival Thinking**, Santa Barbara, California, Libraries Unlimited, 2010.

Eastwood, Terry:	"Appraising Digital Records for Long-Term Preservation", **Data Science Journal**, December 2004, C. 3, ss. 202-208.
eDocuments:	"Creation of Structured e-Document," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/indexe527.html?page_id=71, 13 Ekim 2019. (Son Erişim Tarihi: 5 Aralık 2019)
eDocuments:	"Creation of Unstructured e-Documents," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/index9902.html?page_id=46, 13 Ekim 2019. (Son Erişim Tarihi: 5 Aralık 2019)
eDocuments:	"Descriptive Metadata," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/index55e8.html?page_id=403, 11 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
eDocuments:	"Trust Management Service," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/index6e40.html?page_id=759, 13 Ekim 2019. (Son Erişim Tarihi: 5 Aralık 2019)
eDocuments:	"Deletion/Destruction of e-Documents," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/index9bef.html?page_id=54, 14 Ekim 2019. (Son Erişim Tarihi: 5 Aralık 2019)
eDocuments:	"Digitisation of Paper," (Çevrimiçi) https://joinup.ec.europa.eu/site/isa_edocuments/edocuments/index5534.html?page_id=6, 13 Ekim 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Edwards, Claire:	"UK G-Cloud is A Model Other Countries Should Follow," 2018, (Çevrimiçi) https://www.pinsentmasons.com/out-law/analysis/uk-g-cloud-model-countries-should-follow, 24 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
ESRI:	(Çevrimiçi) https://www.esriuk.com/en-gb/home, 11 Temmuz 2019. (Son Erişim Tarihi: 3 Aralık 2019)

European Communities:	**MoReq Specification-Model Requirements for the Management of Electronic Records**, Bruxelles- Luxembourg, CECA-CEE-CEEA, 2001, (Çevrimiçi) https://ec.europa.eu/idabc/servlets/Doc1faf.pdf?id=16847, 31 Ekim 2018. (Son Erişim Tarihi: 5 Aralık 2019)
European Communities:	**Model Requirements for the Management of Electronic Records (MoReq2),** Update and Extension, France, 2008, (Çevrimiçi) https://www.project-consult.de/Files/MoReq2_body_v1_0.pdf, 29 Ekim 2018. (Son Erişim Tarihi: 5 Aralık 2019)
European Communities:	**MoReq Specification-Model Requirements for the Management of Electronic Records**, Bruxelles- Luxembourg, CECA-CEE-CEEA, 2001, (Çevrimiçi) https://ec.europa.eu/idabc/servlets/Doc1faf.pdf?id=16847, 31 Ekim 2018. (Son Erişim Tarihi: 5 Aralık 2019)
European Telecommunications Standards Institute:	**ETSI TS 102 640-4 V2.1.1 (2010-01)**: **Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Part 4: REM-MD Conformance Profiles**, (Çevrimiçi) https://www.etsi.org/deliver/etsi_ts/102600_102699/10264004/02.01.01_60/ts_10264004v020101p.pdf, 20 Haziran 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Evans, Chris:	"DAS vs. NAS vs. SAN: Which is best for virtual storage?", 2009, (Çevrimiçi) https://www.computerweekly.com/tip/DAS-vs-NAS-vs-SAN-Which-is-best-for-virtual-storage, 18 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Fishbein, Meyer H.:	"A Viewpoint on the Appraisal of National Records," **American Archivist**, April 1970, C. 33, S. 2, ss. 175-187.
Fisher, Tim:	"40 Free Data Destruction Software Programs: Completely Free Disk Wipe And Hard Drive Eraser Software Utilities," 2019, (Çevrimiçi) https://www.lifewire.com/free-data-destruction-software-programs-2626174?print, 8 Mart 2019. (Son Erişim Tarihi: 5 Aralık 2019)

Florida Department of State Division of Library and Information Services:	**Electronic Records and Records Management Practices**, 2010, (Çevrimiçi) https://dos.myflorida.com/media/31109/electronicrecordsmanagementpractices.pdf, 14 Ekim 2016. (Son Erişim Tarihi: 5 Aralık 2019)
Frank Upward kimdir?,	(Çevrimiçi) https://recordscontinuum.info/wiki/UpwardFrank, 3 Ocak 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Franks, Patricia C.:	"Retention & Disposition of Records Residing in a Public Cloud: A Risk Management Approach," International Symposium October 17, (Presentation), 2014, (Çevrimiçi) https://interparestrust.org/assets/public/dissemination/IPT_20141017_InternationalSymposium2_Franks_RetentionDispositionInPublicCloud_Presentation.pdf, 7 Aralık 2017. (Son Erişim Tarihi: 5 Aralık 2019)
Furat, Mehmet Fahri:	"Arşivcilik Hizmetlerinde Profesyonelleşme Süreci ve Türkiye," **Yayımlanmamış Doktora Tezi**, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, 2009
GeeksforGeeks:	"Network Devices," (Çevrimiçi) https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/, 15 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Geng, Lihua:	"The Research of Digital Library Mass Information Storage System Architecture," International Symposium on Computers & Informatics (ISCI 2015), (Çevrimiçi) https://download.atlantis-press.com/article/17628.pdf, 17 Temmuz 2019, DOI: 10.2991/isci-15.2015.245. (Son Erişim Tarihi: 5 Aralık 2019)
Goffinet, Kevin Patrick: ve Timothy S. Seevers	**Method For Providing Document Traceability**, United States of America, Patent Number: US 2006/0265332 A1, Nov. 23, 2006.

Google Support:	"Güçlü Bir Şifre ve Daha Güvenli Bir Hesap Oluşturma," (Çevrimiçi) https://support.google.com/accounts/answer/32040?hl=tr, 14 Kasım 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Ham, F. Gerald:	"Archival Strategies for the Post-Custodial Era," **The American Archivist**, Summer 1981, C. 44, S. 3, ss. 207-216.
Harran, Martin v.d.:	"A Method for Verifying Integrity & Authenticating Digital Media," **Applied Computing and Informatics**, 2017, S. 14, ss. 145–158, s. 147, DOI: 10.1016/j.aci.2017.05.006.
Havelsan A.Ş.:	**Evraka Elektronik Doküman ve Belge Yönetim Sistemi, Ürün Açıklaması Dokümanı**, (Çevrimiçi) http://www.havelsan.com.tr/files/files/document/2732018151047452_bilgi-ve-iletisim-teknolojileri-evreka.pdfa, 18 Mayıs 2019. (Son Erişim Tarihi: 18 Mayıs 2019)
Hellmer, Erica:	"Authenticity in Electronic Archives: Securing Digital Records," **Unpublished Master Thesis**, Mid Sweden University, Institution for Archives and Information Science, 2015.
Henkoğlu, Türkay:	**Bilgi Güvenliği ve Kişisel Verilerin Korunması**, Ankara, Yetkin Yayınları, 2015.
Her Majesty's Stationery Office:	**Committee on Departmental Records Report**, London, 1954. This 1954 report is otherwise known as The Grigg Report after the name of its chairman, Sir James Grigg.
Hofman, Chris:	"You Only Need to Wipe a Disk Once to Securely Erase It," 2016, (Çevrimiçi) https://www.howtogeek.com/115573/htg-explains-why-you-only-have-to-wipe-a-disk-once-to-erase-it/, 14 Eylül 2019. (Son Erişim Tarihi: 5 Aralık 2019)

Hug, Richard A. ve Leon Presser:	**Version Management System**, United States of America Patent, Patent Number: 5,806,078, September 8, 1998. (Çevrimiçi) https://patentimages.storage.googleapis.com/87/f0/fa/71287d769cc9e5/US5806078.pdf, 11 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Hughes, Gordon F., Daniel M.Commins ve Tom Coughlin:	"Disposal of Disk and Tape Data by Secure Sanitization," **IEEE Security and Privacy**, C. 7, No: 4, July/August 2009, ss. 29-34.
Hughes, Gordon ve Tom Coughlin:	**Tutorial on Disk Drive Data Sanitization**, 2007, (Çevrimiçi) https://tomcoughlin.com/Coughlin/Techpapers/DataSanitizeTutorial121206b.pdf, 30 Mart 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Huth, Geof:	"Retention and Disposition of Records: How Long to Keep Records and How to Destroy Them", **Archives Technical Information Series,** 41, 2002, (Çevrimiçi) www.archives.nysed.gov/common/archives/files/mr_pub41.pdf, 5 Mayıs 2016. (Son Erişim Tarihi: 5 Aralık 2019)
ICS JMR:	"Wipe Out Storage Devices Part 1," (Çevrimiçi) https://ics-iq.com/blog/wipe-out-storage-devices-part-1/, 17 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
International Council on Archives (ICA):	**Principles and Functional Requirements for Records in Electronic Office Environments – Module 2: Guidelines and Functional Requirements for Electronic Records Management Systems**, 2008, (Çevrimiçi) www.ica.org, 31 Mayıs 2019. (Son Erişim Tarihi: 5 Aralık 2019)
International Council on Archives (ICA):	**Principles And Functional Requirements For Records In Electronic Office Environments: Overview of Implementation Guidance and Training Products**, 2013, (Çevrimiçi) https://www.ica.org/sites/default/files/1%20Overview.pdf, 14 Eylül 2019. (Son Erişim Tarihi: 5 Aralık 2019)
International Organization	**15489-1: Information and Documentation – Records Management – Part 1: General,** 2001.

for Standardization (ISO):	
International Organization for Standardization (ISO):	**ISO 23081-1 Information and Documentation- Records Management Processes-Metadata for Records, Part 1: Principles, Second Edition**, 2017, (Çevrimiçi) https://www.sis.se/api/document/preview/922676/, 31 Mayıs 2019. (Son Erişim Tarihi: 5 Aralık 2019)
International Records Management Trust:	"Module 3: Managing The Creation Use And Disposal Of Electronic Records," **Training in Electronic Records Management**, Ed. Laura Millar, London, 2009.
International Records Management Trust:	**Modul-3: Managing the Creation, Use and Disposal Of Electronic Records**, Ed. Laura Millar, London, 2009.
ISO:	**19005-1:2005 Document management -- Electronic Document File Format For Long-Term Preservation -- Part 1: Use of PDF 1.4 (PDF/A-1).**
İstanbul Teknik Üniversitesi Arı Teknokent Proje Geliştirme Planlama A.Ş.:	**Kişisel Verilerin Korunması Politikası**, (Çevrimiçi) https://www.aritekno-kent.com.tr/tr/hakkinda/kisisel-verilerin-korunmasina-iliskin-ilkeler, 21 Haziran 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Jaikar, Amol v.d.:	"Performance Analysis of NAS and SAN Storage for Scientific Workflow," Conference: 2016 International Conference on Platform Technology and Service (PlatCon), (Çevrimiçi) http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7456814&is-number=7456759, 17 Temmuz 2019, DOI: 10.1109/PlatCon.2016.7456814. (Son Erişim Tarihi: 5 Aralık 2019)

Jay Atherton Kimdir?	(Çevrimiçi)https://archivaria.ca/archivar/index.php/archivaria/article/view/11233/12172, 3 Ocak 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Jefcoat, Katie Moss:	"A Comprehensive List of Data Wiping and Erasure Standards, Cryptographic Erasure (Crypto Erase)," 2017, (Çevrimiçi) https://www.blancco.com/blog-comprehensive-list-data-wiping-erasure-standards/, 24 Şubat 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Jenkinson, Hilary:	**A Manual of Archive Administration Including the Problem of War Archives and Archive Making**, Oxford, The Clarendon Press, 1922.
Jiang, Yu-fen ve Ping Wang:	"Study on Electronic Records Filing of Mobile Terminal," 4th International Conference on Social Science and Higher Education (ICSSHE 2018), **Advances in Social Science, Education and Humanities Research (ASSEHR)**, C. 181, (Çevrimiçi) https://download.atlantis-press.com/article/25903689.pdf, 25 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Johnson, Judy J. ve James R. McElroy:	**Computer Based Records Management System Method**, United States of America, Patent Number: 5.813.009, Sep. 22, 1998.
Joint Technology Committee:	"Developing an Electronic Records Preservation and Disposition Plan", Version 1.0, **JTC Resource Bulletin,** 2014, (Çevrimiçi) http://www.ncsc.org/~/media/Files/PDF/About%20Us/Committees/JTC/JTC%20Resource%20Bulletins/6JTC%20E%20Records%2010%20FINAL.ashx, 11 Mayıs 2016. (Son Erişim Tarihi: 5 Aralık 2019)
Kandur, Hamza:	**Elektronik Belge Yönetimi Sistem Kriterleri Referans Modeli (v.2.0),** 2. bs., Ankara, Devlet Arşivleri Genel Müdürlüğü Cumhuriyet Arşivi Daire Başkanlığı, 2006.
Kearton, Antonia ve Graham, Susan:	"Best Practice in Disposing of Records," 2005, s. 4, (Çevrimiçi) https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/element6-EU.pdf, 13 Ekim 2018. (Son Erişim Tarihi: 13 Aralık 2019)

Kentucky Department for Libraries and Archives Public Records Division:	**Destruction of Public Records: A Procedural Guide**, 2007, (Çevrimiçi) https://kdla.ky.gov/records/Documents/Destruction%20Guidelines.pdf, 28 Aralık 2017. (Son Erişim Tarihi: 5 Aralık 2019)
Keser Berber, Leyla:	**Adli Bilişim**, Ankara, Yetkin Yayınları, 2004.
Keskin, İshak:	"Arşivcinin Efemerası," (Yayına hazır makale).
Keskin, İshak:	"Osmanlı Bürokrasisinde Evrak İmha Uygulamalarına Dair Gözlemler", **Türk Devlet Yönetimi Geleneği** kitabı içinde, (Ed.) Cengiz Buyar, Mehmet Kıldıroğlu, Murat Kocobekov, (3-4 Nisan 2014 tarihinde **I. Uluslararası Türk Devlet Yönetimi Geleneği Kongresi'**nde sunulan bildiri), Bişkek, 2016, s. 315.
Keskin, İshak:	"Osmanlı Bürokrasisinde Evrak İmha Uygulamalarına Dair Gözlemler," **Türk Devlet Yönetimi Geleneği**, (Ed.) Cengiz Buyar, Mehmet Kıldıroğlu, Murat Kocobekov, Bişkek, 2016.
Keskin, İshak:	**Arşiv Kanunlarının Anatomisi**. İstanbul, Yeditepe Yayınevi, 2016.
Ketelaar, Eric:	"Archival Theory and the Dutch Manual," **Archivaria**, Spring 1996, C. 41, ss. 31-40.
Kişisel Verileri Koruma Kurumu:	"Facebook Nezdinde Gerçekleşen Veri İhlalinin Değerlendirilmesi ile ilgili Kişisel Verileri Koruma Kurulunun 11.04.2019 tarih ve 2019/104 Sayılı Kararı Özeti," (Çevrimiçi) https://www.kvkk.gov.tr/Icerik/5450/2019-104, 15 Haziran 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Kişisel Verileri Koruma Kurumu:	**Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)**, Ankara, 2018, (Çevrimiçi) 21 https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf, 21 Haziran 2019. (Son Erişim Tarihi: 5 Aralık 2019)

Kişisel Verileri Koruma Kurumu:	**Kişisel Veri Saklama ve İmha Politikası**, s. 8, (Çevrimiçi) https://www.kvkk.gov.tr/Icerik/5386/KVKK-KISISEL-VERI-SAKLAMA-ve-IMHA-POLITIKASI, 15 Haziran 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Kişisel Verileri Koruma Kurumu:	**Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Rehberi**, Ankara, 2018.
Koerber, Mark:	"A Critique of the Records Continuum Model," Unpublished Minor Thesis for the Masters of Information Management (Archives and Records Management), University of South Australia, School of Information Technology & Mathematical Science, Adelaide, 2017.
Kolsrud, Ole:	"The Evolution of Basic Appraisal Principles - Some Comparative Observations," **American Archivist**, Winter 1992, C. 55, S. 1. ss. 26-39.
Kristinsdottir, Kristjana:	"The Turning Point in 1985. The History of Appraisal and Disposal of Records in Iceland," **ArchivaI Science**, June 2003, C. 3, S. 2, ss. 199-204.
Külcü, Özgür:	**Kurumsal Bilgi Sistemleri ve Belge Yönetimi: Organizasyonlarda Bilgi ve Belge Yönetimi Sistemlerinin Temel İlkeleri**, İstanbul, Hiperlink Yayınları, 2018.
Larsson, Magnus:	"Sanitization of Embedded Network Devices Investigation of Vendor's Factory Reset Procedures," **Unpublished Master Thesis**, KTH Royal Institute of Technology School of Information and Communication Technology (ICT) Department of Communication Systems, Stockholm, Sweden, 2015.
Lee, Cal:	"Emulation, Migration and Long-Term Preservation of Electronic Records," (Çevrimiçi) https://www.asu.edu/ecure/2001/ppt/lee.ppt, 22 Kasım 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Lifewire:	"What Is a Codec and Why Do I Need It?" (Çevrimiçi) https://www.lifewire.com/what-exactly-is-odec-2483426, 1 Kasım 2019. (Son Erişim Tarihi: 5 Aralık 2019)

Louise Spiteri Kimdir?	(Çevrimiçi) https://dal.academia.edu/LouiseSpiteri, 3 Ocak 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Mabbs, Alfred W.:	"The Public Record Office and the Second Review," **Archives**, 1967-1968, C. 8, ss. 180- 184.
Mckemmish, Sue:	"Yesterday, Today and Tomorrow: A Continuum of Responsibility," **Proceedings of the Records Management Association of Australia 14th National Convention**, 15-17 Sept 1997, (Çevrimiçi) https://monash.figshare.com/articles/Yesterday_today_and_tomorrow_a_continuum_of_responsibility/4037433, 4 Mayıs 2018. (Son Erişim Tarihi: 5 Aralık 2019)
MediaClone:	"Secure Erase Protocols and Methods," (Çevrimiçi) https://www.mediaclone.net/v/vspfiles/downloads/SecureErase.pdf, 19 Eylül 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Meisner, Heinrich Otto:	"Schutz und Pflege des staatlichen Archivgutes mit besonderer Berucksichtigung der Kassationsproblems" [The Protection and Care of Public Records with a Special View to the Problems of Appraisal], **Archivalische Zeitschrift**, 1939, C. 45, ss. 34-51.
Menne-Haritz, Angelika:	"Elektronik Kayıtların Değerlendirilmesi, İmhası ve Provenans İlkesi: (Unutmak İçin Değil) Erişim İçin Değerlendirme", **Arşivcilik Metinleri** (109-123), Nurettin Özyakup (Çev.), İshak Keskin (Haz.), İstanbul, Yeditepe, 2008.
Microsoft:	"Windows Support," (Çevrimiçi), https://support.microsoft.com/en-ph/help/4057281/windows-7-support-will-end-on-january-14-2020, 31 Ekim 2020. (Son Erişim Tarihi: 5 Aralık 2019)
Mil Incorporated:	"Mil Shield," (Çevrimiçi) https://www.milincorporated.com/milshield2.html, 12 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Minnesota Historical Society:	"Electronic Records Management Guidelines, File Formats," (Çevrimiçi) http://www.mnhs.org/preserve/records/electronicrecords/erfformats.php, 10 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)

Modern Public Records:	**The Government Response to the Report of the Wilson Report**, London, Her Majesty's Stationery Office, 1982.
Müller, Karl Otto:	"Fragen der Aktenaussscheidung" [Questions on Appraisal], **Archivalische Zeitschrift**, 1926, C. 36, ss. 188-215.
MySQL Enterprise Backup User's Guide (Version 4.1.3):	**MySQL Enterprise Backup User's Guide (Version 4.1.3)**, "4.3.3 Making a Differential or Incremental Backup," 2019, (Çevrimiçi) https://docs.oracle.com/cd/E17952_01/mysql-enterprise-backup-4.1-en/mysqlbackup.incremental.html, 20 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
National Archives and Records Administration (NARA):	"Bulletin 2012-02," (Çevrimiçi) https://www.archives.gov/records-mgmt/bulletins/2012/2012-02.html, 7 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
National Archives of Australia (NAI):	**Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records**, Exposure Draft, 2004, (Çevrimiçi) https://mayaarbina-ginting.weebly.com/uploads/1/0/6/1/10612501/digital_recordkeeping.pdf, 7 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
National Records of Scotland:	**Electronic Records Management Systems**, (Çevrimiçi) https://www.nrscotland.gov.uk/record-keeping/electronic-records-management/electronic-records-management-systems, 29 Haziran 2019. (Son Erişim Tarihi: 5 Aralık 2019)
National Standard of Canada:	**CAN/CGSB-72.34-2017 –Electronic Records as Documentary Evidence**, Gatineau-Canada, Canadian General Standards Board, 2017, (Çevrimiçi) http://publications.gc.ca/collections/collection_2017/ongc-cgsb/P29-072-034-2017-eng.pdf, 24 Mayıs 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Networking Components and Devices:	**Networking Components and Devices**, (Çevrimiçi) https://sureshvcetit.files.wordpress.com/2019/03/network-components.pdf, 15 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)

New South Wales Government:	"State Archives and Records," (Çevrimiçi) https://www.records.nsw.gov.au/recordkeeping/advice/retention-and-disposal/destruction-of-records, 7 Aralık 2017 (Son Erişim Tarihi: 5 Aralık 2019); Queensland Police Service, **Records Retention and Disposal Handbook,V.2.1**, 2004, (Çevrimiçi) https://www.police.qld.gov.au/rti/published/policies/Documents/QPS%20Records%20Retention%20and%20Disposal%20Handbook%20v21.pdf, 7 Aralık 2017. (Son Erişim Tarihi: 7 Aralık 2017)
New York State Archives	**Preservation of Electronic Records Workbook**, 2011, (Çevrimiçi) http://www.archives.nysed.gov/common/archives/files/workshops_handouts_erecords_preservation.pdf, 1 Ağustos 2019. (Son Erişim Tarihi: 5 Aralık 2019)
New Zealand University of Otago:	**Records Destruction Guidelines**, 2012, (Çevrimiçi) https://www.otago.ac.nz/administration/corporaterecords/otago015244.pdf, 7 Aralık 2017. (Son Erişim Tarihi: 5 Aralık 2019)
Northern Territory Government of Australia, Department of Corporate and Information Services:	**Standard 5- Disposal**, [t.y.], (Çevrimiçi) http://www.nt.gov.au/dcis/info_tech/records_policy_standards/records_management_standards/standard5_disposal.shtml, 7 Aralık 2017. (Son Erişim Tarihi: 7 Aralık 2017)
O'Brien, Irene E:	**Appraisal and Disposal Policy**, Preserving the Archival and Historic Memory of Glasgow, 2011, v.5, (Çevrimiçi) https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/element7-GCA.pdf, 11 Mayıs 2016. (Son Erişim Tarihi: 5 Aralık 2019)
OceanTech:	"Network Equipment Recycling and Data Destruction," (Çevrimiçi) https://www.oceantech.com/2015/01/09/network-equipment-data-destruction/, 15 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)

Ohio Electronic Records Committee:	**Ohio Trustworthy Information Systems Handbook**, 2011, (Çevrimiçi) http://ohioerc.org/wp-content/uploads/2014/09/TISHandbook1.pdf, 25 Şubat 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Olsen, Porter:	"An Introduction to Digital Forensics for Archivists," Sunum Dosyası, (Çevrimiçi) https://digitalapersonarkiv.files.wordpress.com/2014/08/an-introduction-to-digital-forensics-for-archivists.pdf, 25 Şubat 2019. (Son Erişim Tarihi: 5 Aralık 2019)
On, Abdulcebar ve Necaatin Barışçı:	"Web Tabanlı Elektronik Belge Yönetim Sistemi," The Second International Symposium on Innovative Technologies for Engineering and Science, ISITES2014, Karabük Üniversitesi, 18-20 June 2014, ss. 1951-1956, (Çevrimiçi) http://isites.info/PastConferences/ISITES2014/ISITES2014/papers/B6-ISITES2014ID328.pdf, 14 Mayıs 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Onyejekwe, Kele:	"Erasing the Past: How to Expunge a Client's Criminal Record," 2016, (Çevrimiçi) https://www.americanbar.org/groups/young_lawyers/publications/tyl/topics/client-development/erasing past-how-expunge-clients-criminal-record/, 11 Nisan 2019. (Son Erişim Tarihi: 11 Nisan 2019)
Özdemirci, Fahrettin v.d.:	**Elektronik Belge Yönetimi ve Arşivleme Sistemi: Geçiş Süreci ve Uygulama Yönetimi**, Ankara, 2013.
Özdemirci, Fahrettin:	"Cumhuriyet Dönemi Milli Arşivimizin Örgütsel Yapılanma Gereksinimleri,", **Bildiriler: Müzeler, Kütüphaneler, Yayınevleri, Telif Hakları**, Ed. Zeki Dilek, Mustafa Akbulut, Zeynep Bağlan Özer, Reşide Gürses, Banu Karababa Taşkın, Ankara, Atatürk Kültür, Dil ve Tarih Yüksek Kurumu Başkanlığı, 2009.
Özdemirci, Fahrettin:	**Kurum ve Kuruluşlarda Belge Üretiminin Denetlenmesi ve Belge Yönetimi**, İstanbul, Türk Kütüphaneciler Derneği, 1996.
Özen, Muharrem ve Gürkan Özocak:	"Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)," **Ankara Barosu Dergisi**, S. 1, s. 43-77.

Papers of Reginald Lane Poole (F. 1898–1933):	Papers of Reginald Lane Poole (F. 1898–1933), (Çevrimiçi, http://www.magd.ox.ac.uk/libraries-and-archives/archives/online catalogues/poole-papers-3/, 15 Ağustos 2019) (Son Erişim Tarihi: 15 Ağustos 2019)
Pearce-Moses, Richard:	**A Glossary of Archival and Records Terminology**, Chicago, The Society of American Archivists (SAA), 2005.
Penn, Ira A. v.d.:	**Records Management Handbook,** Second Edition, New York, Routledge, 2016.
Protective Security Requirements:	"Mobile and remote working," (Çevrimiçi) https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/mobile-and-remote-working/, 25 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Quizlet:	"ICT-3.Storage Devices and Media," (Çevrimiçi) https://quizlet.com/138092983/ict-3storage-devices-and-media-flash-cards/, 18 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Realpars:	"What Is RS232 and What Is It Used for?" (Çevrimiçi) https://realpars.com/rs232/, 1 Kasım 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Revision World:	"Storing Data, Devices and Media," (Çevrimiçi) https://revisionworld.com/gcse-revision/ict/hardware/storing-data-devices-and-media, 17 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Roberts, John W.:	"Archival Theory: Much Ado About Shelving," **American Archivist**, Winter 1987, C. 50, S. 1, ss. 66-74.
Roberts, John:	"Macroappraisal Kiwi Style: Reflections on the Impact and Future of Macroappraisal in New Zealand," **Archival Science**, December 2005, C. 5, S. 2-4, ss. 185–201.
Rohr, Wilhelm:	"Das Aktenwesen der preussischen Regierung" [The Records System of the Prussian Government], **Archivalische Zeitschrift**, 1939, C. 45.

Rukancı, Fatih ve Hakan Anameriç:	"Evrak-ı Atikanın Suret-i Tasfiyesine Dair Rapor," **Belgeler**, C. 27, S. 31 2006, s. 96-110.
Saraçoğlu, Turgay:	"Veri Depolama Ağları ve Yeni Gelişen Teknolojiler," 2006. (Çevrimiçi) http://www.if.com.tr/pages/images/makaleler/if-makale-0603-1.pdf, 18 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Schellenberg, T.R.:	**Modern Archives**, Chicago, The University of Chicago Press, 1956.
Schellenberg, Theodore R.:	"Arşivsel Değerlendirme İlkeleri," **Arşivcilik Metinleri** (ss. 55-70), İlhan Bozan (Çev.), İshak Keskin (Haz.), İstanbul, Yeditepe, 2008.
Siewert, Patrick:	"Cellular Provider Record Retention Periods," 2017, (Çevrimiçi) https://articles.forensicfocus.com/2017/04/18/cellular-provider-record-retention-periods/, 25 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Singapore Personel Data Protection Commission:	**Guide to Disposal of Personal Data On Physical Medium**, 2016, (Çevrimiçi) https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-to-disposal-of-personal-data-on-physical-medium-(200117).pdf, 7 Aralık 2017. (Son Erişim Tarihi: 5 aralık 2019)
Society of American Archivists (SAA):	"Postcustodial Theory of Archives," (Çevrimiçi) https://www2.archivists.org/glossary/terms/p/postcustodial-theory-of-archives, 18 Eylül 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Society of American Archivists (SAA):	**Guidelines for Reappraisal and Deaccessioning**, Draft, 2011, (Çevrimiçi) https://www2.archivists.org/sites/all/files/GuidelinesForReappraisalAndDeaccessioningDRAFT.pdf, 20 Eylül 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Spiteri, Louise:	"Records Continuum Model,", **CNSA 2012 Conference,** 2012, (Çevrimiçi) https://www.slideshare.net/cleese6/records-continuum-model, 2 Mayıs 2018. (Son Erişim Tarihi: 5 Aralık 2019)

Staffordshire and Stoke On Trent Archive Service:	**Appraisal And Disposal Policy**, **Method of Appraisal**, 6. Rule, (Çevrimiçi) https://www.staffordshire.gov.uk/Heritage-and_archives/about/Policies/Archive-Service-Appraisal-and-Disposal-Policy.aspx, 10 Mayıs 2018. (Son Erişim Tarihi: 10 Mayıs 2018)
Stapleton, Richard:	"Jenkinson ve Schellenberg: Bir Karşılaştırma", M. Fahri Furat (Çev.), **Arşiv Dünyası**, S.14-15, 2013.
State Archives of North Carolina:	**Destruction of Electronic Records- The G.S. 132 Files**, (Çevrimiçi) https://ncrecords.wordpress.com/2014/09/26/destruction-of-electronic-records/, 15 Şubat 2019. (Son Erişim Tarihi: 5 Aralık 2019)
State of Indiana:	"What Is a QR Code and How Is It Used on IN.GOV?", (Çevrimiçi) https://www.in.gov/core/qr_code.html, 13 Ekim 2019. (Son Erişim Tarihi: 5 Aralık 2019)
State Records of South Australia:	**Cloud Computing and Records Management, Guideline Version 1**, 2015, (Çevrimiçi) https://archives.sa.gov.au/sites/default/files/documentstore/policies-guidelines/Standard/20150706_cloud_computing_and_records_management_final_v1.pdf, 26 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Stefan, Lucia:	"The Three Records Management Models", (Çevrimiçi) https://www.slideshare.net/Stelucia/records-management-models-4849738, 9 Nisan 2018. (Son Erişim Tarihi: 5 Aralık 2019)
Stellar Data Recovery Inc.:	"7 Effective Algorithms to Remove Files and Folders Permanently," 2018, (Çevrimiçi) https://www.stellarinfo.com/article/7-algorithms-to-wipe-files-folders-permanently.php, 23 Şubat 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Stephens, David O., Roderick C. Wallace:	"Electronic Records Retention: Fourteen Basic Principles". **Information Management,** 34, 4, 2000, ARMA International, s.41, (Çevrimiçi) http://www.umiacs.umd.edu/~oard/teaching/708x/spring12/readings/stephens.pdf, 14 Mayıs 2017. (Son Erişim Tarihi: 5 Aralık 2019)
Şentürk, Burçak:	"Arşivsel Değerlendirme: Arşivciliğin İlk Adımı", **Arşiv Dünyası**, S. 14-15, 2013.

Tasmanian Archive and Heritage Office:	**Approved Destruction Methods for State Records, State Records Guideline No 21**, (Çevrimiçi) 7 Aralık 2017 https://www.informationstrategy.tas.gov.au/Records-ManagementPrinciples/Document%20Library%20%20Tools/Guideline%2021%20Approved%20destruction%20methods%20for%20State%20records.pdf, 7 Aralık 2017. ((Son Erişim Tarihi: 7 Aralık 2017)
Technopedia:	"Mobile Application (Mobile App)," (Çevrimiçi) https://www.techopedia.com/definition/2953/mobile-application-mobile-app, 25 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
TechTarget:	"Brouter," (Çevrimiçi) https://searchnetworking.techtarget.com/definition/brouter, 1 Kasım 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Territory Records Office:	**Records Advice No 23- Australian Standard for Records Management**, (Çevrimiçi) https://www.territoryrecords.act.gov.au/__data/assets/pdf_file/0008/435527/Records-Advice-No-23-Australian-Standard-for-Records-Management-January-2011.pdf, 24 Mayıs 2019. (Son Erişim Tarihi: 5 Aralık 2019)
The Government Communications Security Bureau:	**The New Zealand Information Security Manual**, 2019, s. 197-212, (Çevrimiçi) https://www.nzism.gcsb.govt.nz/assets/NZISM/pdf/NZISM-V.3.2-Jul-2019.pdf, 22 Temmuz 2019. (Son Erişim Tarihi: 22 Temmuz 2019)
The InterPARES 2 Project:	"Glossary," 2019, (Çevrimiçi) http://www.interpares.org/ip2/ip2_term_pdf.cfm?pdf=glossary, 10 Ocak 2019. (Son Erişim Tarihi: 5 Aralık 2019)
The InterPARES 2 Project:	Glossary, "Migration of Records," 2019.
The National Archives of Australia:	"Designing and Implementing Recordkeeping Systems," (Çevrimiçi) http://www.naa.gov.au/recordkeeping/dirks/summary.html.

The National Archives of United Kingdom (TNA):	**Deaccessioning and Disposal Guidance For Archive Services**, 2015, (Çevrimiçi) http://www.nationalarchives.gov.uk/documents/Deaccessioning-and-disposal-guide.pdf, 11 Mayıs 2016. (Son Erişim Tarihi: 5 Aralık 2019)
The National Archives of United Kingdom (TNA):	**Requirements for Electronic Records Management Systems-1: Functional Requirements**, **2002 Revision: Final Version**, Surrey-United Kingdom, 2002.
The National Archives of United Kingdom (TNA):	**Disposal Scheduling**, 2012, (Çevrimiçi) http://www.nationalarchives.gov.uk/documents/information-management/sched_disposal.pdf, 11 Mayıs 2016. (Son Erişim Tarihi: 5 Aralık 2019)
The National Archives of United Kingdom:	**Records Management Guides-4:Active Records Management: Records Creation**, 2006.
The National Archives:	**Best Practice Guide to Appraising and Selecting Records For The National Archives**, y.y., Crown Copyright, 2013, (Çevrimiçi) http://www.nationalarchives.gov.uk/documents/information-management/best-practice-guide-appraising-and-selecting.pdf, 16 Ağustos 2019. (Son Erişim Tarihi: 5 Aralık 2019)
The National Archives:	**What is Appraisal?**, y.y., Crown Copyright, 2013, (Çevrimiçi) http://www.nationalarchives.gov.uk/documents/information-management/what-is-appraisal.pdf, 16 Ağustos 2019. (Son Erişim Tarihi: 5 Aralık 2019)
The United Methodist Church, Gene-	**Guidelines for Managing Electronic Records 2013-2016**, (Çevrimiçi) https://www.ctcumc.org/files/fileshare/digital+records+-+gcah.pdf, 1 Eylül 2019. (Son Erişim Tarihi: 5 Aralık 2019)

ral Commission on Archives and History:	
The Wilson Report:	**Modern Public Records. Selection and Access**, London, Her Majesty's Stationery Office, 1981.
Tough, Alistair G.:	"The Post-Custodial/Pro-Custodial Argument From A Records Management Perspective," **Journal of the Society of Archivists**, 2004, C. 25, 2004, S. 1, (Çevrimiçi) https://doi.org/10.1080/0037981042000199115 , 4 Ocak 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Tschan, Reto:	"Jenkinson ve Schellenberg'in Değerlendirmeye Dair Görüşlerinin Karşılaştırılması," **Prof. Dr. Şevki Nezihi Aykut Armağanı** (ss. 355-372**)**, Erkan Keser (Çev.), Gülden Sarıyıldız, Niyazi Çiçek, İshak Keskin, Sevil Pamuk (Haz.), İstanbul, Etkin Kitaplar, 2011.
Turksat Bilişim:	"Belgenet," (Çevrimiçi) https://bilisim.turksat.com.tr/, 18 Mayıs 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Turner, Jane:	"A Study of the Theory of Appraisal For Selection," **Unpublished Master Thesis**, The University of British Columbia, Department of School of Library Archival and Information Studies, 1992.
Turner, Pegeen:	"Electronic Records Retention and Destruction," 2014, (Çevrimiçi) https://www.lawyersmutualnc.com/risk-management-resources/articles/electronic-records-retention-and-destruction, 19 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Türk Dil Kurumu:	"Yonga," (Çevrimiçi) https://sozluk.gov.tr/, 26 Eylül 2019). (Son Erişim Tarihi: 5 Aralık 2019)
Türk Standartları Enstitüsü (TSE):	**TS ISO 15489-1: Enformasyon ve Dokümantasyon – Belge Yönetimi**.

Türk Standartları Enstitüsü (TSE):	**TS 13298 Elektronik Belge Yönetimi**, 2015.
Türk Standartları Enstitüsü (TSE):	**Elektronik Doküman ve Belge Yönetim Sistemi Koruma Profili, Sürüm 1.3.1**, 2014, (Çevrimiçi) https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/2231/09012015111018-3.pdf, 8 Kasım 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Türk Standartları Enstitüsü (TSE):	**Bilişim Terimleri Sözlüğü**, Ankara, Onur Matbaacılık, 2006.
Türk Standartları Enstitüsü (TSE):	**Bulut Bilişim Güvenlik ve Kullanım Standardı (Taslak)**, 2014, (Çevrimiçi) https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/1202/17032015093613-3.pdf, 21 Temmuz 2018. (Son Erişim Tarihi: 5 Aralık 2019)
Türk Standartları Enstitüsü (TSE):	**TS ISO/TR 15489-2 Enformasyon ve Dokümantasyon – Belge Yönetimi, Bölüm 2: Klavuz**, 2001, s. 23-24.
U.K. Centre for the Protection of National Infrastructure (CPNI Standard):	**Secure Destruction Of Sensitive Items**, 2014, (Çevrimiçi) https://www.cpni.gov.uk/system/files/documents/c5/e1/2017_01_20_CPNI_Secure_Destruction_Standard.pdf, 7 Mart 2019. (Son Erişim Tarihi: 5 Aralık 2019)
U.S. Department of Commerce, National Institute of Standards and	**NIST Special Publication 800-88 (Revision 1): Guidelines for Media Sanitization**, Haz. Richard Kissel v.d., Gaithersburg, 2014, (Çevrimiçi) http://dx.doi.org/10.6028/NIST.SP.800-88r1, 23 Mart 2018. (Son Erişim Tarihi: 5 Aralık 2019)

Technology (NIST):	
U.S. Department of Education, Privacy Technical Assistance Center:	**Best Practices for Data Destruction**, 2014, (Çevrimiçi) https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282014-05-06%29%20%5BFinal%5D_0.pdf, 7 Aralık 2017. (Son Erişim Tarihi: 5 Aralık 2019)
U.S. Department of Education, Privacy Technical Assistance Center:	**Best Practices for Data Destruction**, 2019, (Çevrimiçi) https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282019-3-26%29.pdf, 22 Eylül 2019. (Son Erişim Tarihi: 5 Aralık 2019)
U.S. Department of Transportation, Federal Aviation Administration:	**Electronic Signatures, Electronic Recordkeeping, and Electronic Manuals- Advisory Circular,** 2016, s. 4, (Çevrimiçi) https://www.faa.gov/documentlibrary/media/advisory_circular/ac_120-78a.pdf, 25 Temmuz 2019. (Son Erişim Tarihi: 5 Aralık 2019)
United Kingdom National Cyber Security Centre:	**CPA Security Characteristic, Overwriting Tools For Magnetic Media, Version 2.1**, 2016, (Çevrimiçi) https://www.ncsc.gov.uk/products/4secure-erase-version-10, 8 Eylül 2019. (Son Erişim Tarihi: 5 Aralık 2019)
United Kingdom National Offender Management Services:	**Archiving, Retention and Disposal Policy**, 2014, (Çevrimiçi) https://www.justice.gov.uk/downloads/offenders/probation-instructions/pi-28-2014-archiving-retention-disposal.doc, 11 Mayıs 2016. (Son Erişim Tarihi: 5 Aralık 2019)

United Nations Archives and Records Management Section:	**Records and Information Management Guidance**, [t.y.], (Çevrimiçi) https://archives.un.org/sites/archives.un.org/files/5-guidance_destroying_records.pdf, 13 Ekim 2016. (Son Erişim Tarihi: 5 Aralık 2019)
United States Code:	**TITLE 44—Public Printing and Documents**, Sec. 3542, s. 147-148, (Çevrimiçi) https://www.govinfo.gov/content/pkg/USCODE-2011 title44/pdf/USCODE-2011-title44.pdf, 21 Temmuz 2019. (Son Erişim Tarihi: 21 Temmuz 2019)
United States of America Department of Defense (USA-DoD):	**DoD 5015.2-STD: Electronic Records Management Software Applications Design Criteria Standard**, Department Of Defense Chief Information Officer, 2007.
United States Patent and Trademark Office:	(Çevrimiçi) https://assignment.uspto.gov/patent/index.html#/patent/search/resultAbstract?id=20060265332&type=publNum, 14 Kaısm 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Upward, Frank:	"Structuring the Records Continuum - Part One: Postcustodial Principles and Properties," **Archives & Manuscripts**, 1996, C. 24, S. 2.
Upward, Frank:	"Structuring the Records Continuum, Part Two: Structuration Theory and Recordkeeping," **Archives & Manuscripts**, 1997, C. 25, S.1.
Vaisey, David George:	"The Image of the Archivist, Harmonization of Training and International Mobility" (Paper delivered at the international symposium entitled "Archives and Europe Without Boundaries," Maastricht, The Netherlands, 2-5 October 1991).
Walking The Digital Tightrope,	**A Fujitsu Report,** 2016. (Çevrimiçi) http://www.fujitsu.com/global/Images/br-fujitsu-digital-tightrope-report-em-en.pdf, 25 Ekim 2016. (Son Erişim Tarihi: 5 Aralık 2019)

Walters, Tyler O.:	"Contemporary Archival Appraisal Methods and Preservation Decision-Making," **American Archivist**, Summer 1996, C. 59, S. 3, ss. 322-338.
Webopedia:	"Server," (Çevrimiçi) https://www.webopedia.com/TERM/S/server.html, 17 Ağustos 2019. (Son Erişim Tarihi: 5 Aralık 2019)
Wright, Craig, Dave Kleiman ve Shyaam Sundhar R.S.:	"Overwriting Hard Drive Data: The Great Wiping Controversy," Ed. R. Sekar and A.K. Pujari, **ICISS 2008, LNCS 5352**, Berlin Heidelberg, Springer-Verlag, 2008, ss. 243-257.
Yalçınkaya, Bahattin:	"e-Devlet Üstveri Standardının Oluşturulması ve Türkiye İçin Modellenmesi," **Yayımlanmamış Doktora Tezi**, Marmara Üniversitesi, Türkiyat Araştırmaları Enstitüsü, 2014.
Zatyko, Ken:	"Commentary: Defining Digital Forensics," **Forensic Magazine**, Feb/March 2007, ss. 1-5, (Çevrimiçi) https://www.forensicmag.com/article/2007/01/commentary-defining-digital-forensics, 13 Ağustos 2019. (Son Erişim Tarihi: 13 Ağustos 2019)
Zechel, Arthur:	"Probleme einer Wissenschaftstheorie der Archivistik mit besondere Berücksichtigung des Archivwesen der Wirtschaft" [Problems of a Science Theory on Archivistique with a Special View to Business Archives], Tradition. **Zeitschrift fur Firmengeschichte und Untemahmenbiographie**, 1965, C. 10, ss. 285-300.
Zechel, Arthur:	"Wertheorie und Kassation" [Value Theory and Disposal], **DerArchivar**, 1965, ss. 1-16.
Zimmermann, Fritz W.:	"Wesen und Ermittlung des Archivwertes. Zur Theorie einer archivalischer Wertlehre" [Nature and Appearance of Archival Value. On the Theory of Archival Appraisal], **Archivalische Zeitschrift**, 1958, C. 54.

Zylstra, Corie:	"Custodial and Post-custodial Approaches to Archives," **Sunum**, (Çevrimiçi)http://coriezylstraeportfolio.weebly.com/uploads/1/4/4/2/14421694/zylstrafinalpresentation.pptx, 17 Eylül 2019. (Son Erişim Tarihi: 5 Aralık 2019)

EKLER

Elektronik belge yönetim sistemi standartlarını benimseme aşamasında olan bir kuruluş için, takip etmesi gereken muhtemel adımlar:[1]

1. ISO 30300 ve 30301, Bu, genel olarak kayıt tutma ile ilgili olduğu için genel yönetim sistemlerinin ihtiyaç duyduğu stratejik sonuçların bir görünümünü verecektir.

2. ISO 15489 Bölüm 1, tüm formatlardaki kayıtlar için kayıt tutma gerekliliklerileyle ilgili yüksek düzeyde bir görünüm sunar.

ISO 15489 Bölüm 2, Kayıt Sistemlerinin Tasarlanması ve Uygulanması (DIRS) metodolojisi, özellikle de Sistemlerin karşılanması gereken kayıtlar için gereksinimlerin nasıl tanımlanacağını ele alan Adım C.

ISO 16175 Kısım 1, dijital kayıtlara ilişkin gereksinimlerin yüksek düzeyde görüntülenmesini sağlar.

3. ISO 16175 Bölüm 2-3, hem işletme hem de kayıt tutma sistemlerinde dijital kayıtlar için ayrıntılı kayıt tutma gereksinimleri kümesi sağlar. Bu şartlar yargı yetkisi ne olursa olsun uygulanır.

Yetki Belgesinde yer alan yasal gerekliliklere dayalı olarak, DoD5015.2 ve MoReq standartları gibi yetki alanına özgü kayıt tutma gereklilikleri.

ISO / TR 26122, Bilgi ve Belgeleme - Sistemlerin kayıt oluşturması ve yakalaması gereken bir iş sürecindeki noktaları tanımlamaya yardımcı olmak için kayıtlar için iş süreci analizi.

Dijital kayıtları yönetmek için meta veri gereksinimleri elde etmek için ISO 23081 Bölüm 1 ve 2.

[1] Adrian Cunningham, Relationships Between the ISO 16175 Series of Standards and Other Products of ISO/TC46/SC11: Archives/Records Management, 2 Haziran 2019 tarihinde https://www.ica.org/sites/default/files/PCOM_2012-06_ISO%20paper_ACunningham_EN.pdf adresinden erişildi.

İMHA YÖNTEM VE TEKNİKLERİ TERİMLERİ SÖZLÜĞÜ

Boşaltma (Clearing):	Saklama ortamına zarar vermeden bilgileri ortamdan çıkarma işlemidir.[1]
Capture (Sağlama):	Belge yönetimi teorisinde yapılandırılmış verinin sisteme dâhil edilmesidir.
Çekiçli Değirmenle İmha Etme (Hammer-Milling):	Değirmenin haznesinde yüksek hızda dönen çekiçler (tipik olarak sertleştirilmiş çelik bloklar) ile donatılmış döner bir tamburda malzemenin, bir taraftan çekiçlerle parçalanması bir taraftan da hazne duvarı ve diğer malzemelerle sürterek aşınmaya ve ısıya maruz kalarak imha edilmesidir.[2]
Hizmet dışı bırakmak (Decommissioning):	Devreden çıkarmak, servisten çıkarmak.[3]
Elektronik Atık (E-Waste):	Kırılmış, eskimiş veya geri dönüşüme ihtiyacı olan tüm elektronik atık biçimlerini kapsayan bir şemsiye terimdir.[4]
Erişime Kapatma (Deaccessioning):	Bir koleksiyonun veya malzemenin arşiv hizmetinin envanterinden / arşiv kurumu sahipliğinden resmi olarak çıkarılması işlemidir.[5]
Eritme (Smelting):	Saklama ortamının tipik olarak ince bir kül elde etmek için yakılması ve daha sonra bin santigrat dereceyi aşan sıcaklıklarda eritme fırınına verilmesidir. Böylelikle eriyen külün dökülmüş, soğutulmuş ve ayrılmış sıvı mıcırla reaksiyona girerek metallerin daha fazla geri dönüşüm ve inceltme yoluyla geri kazanılmasının sağlanmasıdır.[6]

[1] Tasmanian Archive and Heritage Office, **Approved Destruction Methods for State Records, State Records Guideline No 21**, s. 8, (Çevrimiçi) 7 Aralık 2017 https://www.informationstrategy.tas.gov.au/Records-ManagementPrinciples/Document%20Library%20%20Tools/Guideline%2021%20Approved%20destruction%20methods%20for%20State%20records.pdf, 7 Aralık 2017.

[2] **A.y.**

[3] Antonia Kearton ve Susan Graham, "Best Practice in Disposing of Records," 2005, s. 4, (Çevrimiçi) https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/element6-EU.pdf, 13 Ekim 2018.

[4] Corporate Document Destruction, "e-Waste Destruction and Recycling," (Çevrimiçi) https://www.corporatedocumentdestruction.com.au/e-waste-destruction-and-computer-recycling-melbourne/e-waste-destruction-and-recycling, 21 Eylül 2019.

[5] The National Archives of United Kingdom (TNA), **Deaccessioning and Disposal Guidance For Archive Services**, 2015, s. 31, (Çevrimiçi) http://www.nationalarchives.gov.uk/documents/Deaccessioning-and-disposal-guide.pdf, 11.05.2016.

[6] U.K. Centre for the Protection of National Infrastructure (CPNI Standard), **Secure Destruction Of Sensitive Items**, s. 20.

Expunging:	Bir mahkeme kararıyla, bir kaydın tamamını veya bir kısmını kalıcı olarak kaldırma veya yok etme sürecidir. Bazı durumlarda, bu kaldırma süreci bir belgeyi kapatma veya söz konusu belgeye erişimi kısıtlama işlemini de ifade eder.[7]
Gelişmiş Güvenli Silme (Enhanced Secure Erase):	Verilerin tamamen yok edildiğinden emin olmak için önceden belirlenmiş farklı bit desenleriyle artık alanlar dâhil olmak üzere birkaç kez verilerin üzerine yazar; ayrıca saklama ortamındaki iç hataların verinin erişimine izin verme durumunu ortadan kaldırırarak tüm kullanıcı veri alanlarına (üretici tarafından ayarlanan) üzerine yazma işlemi gerçekleştirir.[8]
Güvenli Silme (Secure Erase, SE)	Yazma düzeninde ana bilgisayardan sürücüye veri aktarımı olmayan tek geçişli bir yazma işlemi uygulanır. Güvenli silme için yazma düzeni önceden tanımlanır ve veri sürücünün içinden alınır.[9]
Hızlı Silme (Soft Deletion):	Hızlı silme, kamu yararı için açık erişimi veya iş amacıyla saklanması gerekmeyen bilgilere, bağlantıların silinmesi veya silinecek kaydın işaretlenmesi yoluyla erişilemez hale getirilmesi işlemidir. Bu silme işleminin avantajı, normal saklama sürelerini geçen belgelerde sonradan farkına varılan hataların düzeltilmesi için kayıtlara erişilmesi gerektiğinde kısa süreliğine koruma sağlamasıdır.[10]
Kesme (Cutting):	Malzeme önceden belirlenmiş genişlikteki şeritler halinde dilimleyen bir bıçakla kesildikten sonra dilimlenmiş malzemenin 90° döndürülmesiyle ve tekrar kesilmiş bir atık malzeme üretilecek şekilde dilimlenmesidir.[11]
Kimyasal İmha (Chemical Destruction):	Manyetik depolama araçlarının**,** kayıt yüzeyleri tamamen çıkıncaya kadar kimyasal (tipik olarak asit) banyosuna batırılmasıdır.[12]
Kripto Silme (Crypto Erase):	Bir şifreleme / şifre çözme anahtarı olarak adlandırılan, özel bilgiye sahip olanlar dışında herkes için okunamaz hale getirmek için şifreli bir algoritma kullanarak bilgiyi dönüştürme işlemidir. "Tek yönlü" şifreleme, ilk önce verileri şifreleyerek ve ardından verileri şifrelemek için kullanılan anahtarı imha ederek verileri kullanılamaz

[7] Kentucky Department for Libraries and Archives, **Public Records Division, Destruction of Public Records: A Procedural Guide**, s. 2.

[8] MediaClone, "Secure Erase Protocols and Methods," (Çevrimiçi) https://www.mediaclone.net/v/vspfiles/downloads/SecureErase.pdf, 19 Eylül 2019.

[9] Hughes, Commins ve Coughlin, "Disposal of Disk and Tape Data by Secure Sanitization," s. 30.

[10] Joint Technology Committee, "Developing an Electronic Records Preservation and Disposition Plan", Version 1.0, s. 20.

[11] **A.y.**, s. 19.

[12] U.K. Centre for the Protection of National Infrastructure (CPNI Standard), **Secure Destruction Of Sensitive Items**, s. 19.

	hale getirmek için şifreleme tekniklerini kullanan bir veri imha tekniğidir.[13]
Kümelenme (Aggregation):	Kayıtların aynı veya farklı veri yapısına sahip olabileceği ve veri yapısının ilgili bileşik türün temel parçası olabileceği yapılanmış bileşenler topluluğu[14] olarak ifade edilir.
Manyetiksizleştirme/De-manyetize etme (Degaussing):	Medya yüzeyinin manyetik özelliklerini değiştirerek manyetik ortamda depolanan verileri okunaksız hale getiren bir işlemdir. Güçlü bir alternatif manyetik alanın uygulanmasına maruz kalması, verilerin kaybına neden olur ve ortamı manyetik olarak nötr bir hale getirir.[15]
Parçalama (Disintegration):	Malzemenin hazne içine sabitlenmiş ikinci bir bıçak setine karşı yüksek hızda dönen sertleştirilmiş bıçaklarla donatılmış dönen bir tamburdan oluşan bir kesme süreci ile gerçekleşmesidir. Süreçte malzeme bıçaklarla kesilirken aşınma ve ısınmanın katkısıyla kayıt yüzeyi imha edilmiş olur.[16]
Salamuralaşma (Dry Maceration)[17]:	Sabit sürücülerin hidrolik olarak ezen makinelerin bıraktığı ezme işlemidir. Ezme işlemi, sabit disk kasasına onarılamaz bir hasara neden olurken aynı zamanda iç plakayı da yok eden bir zımba kullanır. Bu kuvvet, sürücüyü yeniden bağlamak veya çalışan bir bilgisayara yeniden bağlanmamak için yeterli bir teknik olarak görülmektedir.[18]
Tasfiye Etme (Disposal):	Depolama ortamını başka bir temizleme işlemine gerek kalmadan veya Windows ve Linux gibi kamuya açık işletim sistemlerinde kullanıcı dosya dizinlerini silerek atmak anlamına gelir.
Taşlama veya Fırçalama (Grinding or Scrubbing):	Disklerin imha edilmesi için kullanılır. Diskin kayıt yüzeyindeki katmanı tamamen çıkıncaya kadar aşındırıcı bir yüzeye (zımpara çarkı, taşlama veya zımparalama aygıtı gibi) karşı döndürülmesiyle yapılır.[19]
Temizleme (Purging):	En gelişmiş laboratuar tekniklerini kullanarak hedef verileri kurtarmayı olanaksız kılan fiziksel veya mantıksal teknikler uygulayarak temizleme yapan bir yöntemdir.[20]

[13] U.S. Department of Education, Privacy Technical Assistance Center, **Best Practices for Data Destruction**, s. 10.

[14] Türk Standartları Enstitüsü, **Bilişim Terimleri Sözlüğü**, Ankara, Onur Matbaacılık, 2006, s. 6.

[15] Joint Technology Committee, "Developing an Electronic Records Preservation and Disposition Plan", Version 1.0, s. 20.

[16] U.K. Centre for the Protection of National Infrastructure (CPNI Standard), **Secure Destruction Of Sensitive Items**, s. 19.

[17] New Zealand University of Otago, **Records Destruction Guidelines**, 2012, s. 2.

[18] Joint Technology Committee, "Developing an Electronic Records Preservation and Disposition Plan", s. 20.

[19] **A.g.s.**, s. 19.

[20] **NIST 800-88**, s. 43.

Ufalama (Shredding):	Ortamın birbirine kenetlenmiş döner bir bıçak setinin nesneyi kesmesiyle yapılır. Ortam ufak parçalar haline getirilirken ısıya maruz kalır. Isıya maruz kalan parçalar üzerindeki kayıt alanları aşınmayla beraber yok olur.[21]
Üzerine Yazma (Overwriting):	Manyetik saklama araçlarının imha standartlarında belirlenmiş tekniklerle rastsal verinin silinmek istenen veri üzerine yazma işlemi gerçekleştirerek yazılımsal ve donanımsal müdahaleye izin vermeyen veri imha yöntemidir.
Yakma (Incineration):	Ortamın organik bileşenlerini yakan, malzemeyi küle indirgeyen bir yakma fırınına verilmesiyle geriye uçucu ve dip kül kalan imha tekniğidir.[22]

[21] U.K. Centre for the Protection of National Infrastructure (CPNI Standard), **Secure Destruction Of Sensitive Items**, s. 20.

[22] **A.g.s.**, s. 19.

ÖZGEÇMİŞ

Ceyhan GÜLER, 1985 yılında Erzurum'da doğdu. İlk ve orta öğrenimini Erzurum'da lise öğrenimini de Konya'da tamamladı. 2005-2009 yılları arasında İstanbul Üniversitesi Edebiyat Fakültesi Bilgi ve Belge Yönetimi Bölümünde lisans eğitimi aldı. 2015 yılında aynı üniversitenin Bilgi ve Belge Yönetimi Programında yüksek lisansını *Kamu Kurumlarında Elektronik Belge Yönetimi Uygulamalarında Karşılaşılan Problemler: Teknik Şartnamelerin İncelenmesi* adlı teziyle bitirdi. 2 farklı TÜBİTAK projesinde yer aldı. Haziran 2015'te İstanbul Üniversitesi Edebiyat Fakültesi Bilgi ve Belge Yönetimi Bölümü Arşivcilik Anabilim Dalı'nda Araştırma Görevlisi olarak göreve başladı. 2015 yılından bu yana bulunduğu görevinde devam etmektedir. Güler, genel olarak bilgi ve belge yönetimi, ,arşivcilik, elektronik devlet alanlarında, özel olarak belge yönetim sistemleri, arşivsel değerlendirme, arşiv imha teorisi, elektronik belgelerin imhası konularında çalışmalarına devam etmektedir