T.C

ANKARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

HASSAS BİLGİ İÇERİKLİ KAMU BELGELERİNİN DEĞERLENDİRİLMESİ

Doktora Tezi

HASAN ÖZTÜRK

Ankara - 2025

T.C

ANKARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

HASSAS BİLGİ İÇERİKLİ KAMU BELGELERİNİN DEĞERLENDİRİLMESİ

Doktora Tezi

HASAN ÖZTÜRK

Tez Danışmanı

Prof. Dr. FATİH RUKANCI

Ankara - 2025

T.C

ANKARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

HASSAS BİLGİ İÇERİKLİ KAMU BELGELERİNİN DEĞERLENDİRİLMESİ

DOKTORA TEZİ

Tez Danışmanı: Prof. Dr. FATİH RUKANCI

TEZ JÜRİSİ ÜYELERİ

Adı ve Soyadı	İmzası
1- Prof. Dr. Fatih RUKANCI	
2- Prof. Dr. Hakan ANAMERİÇ	
3- Prof. Dr. Sacit ARSLANTEKİN	
4- Doç. Dr. Ahmet ALTAY	
5- Doç. Dr. Bahattin YALÇINKAYA	

Tez Savunması Tarihi

31.01.2025

T.C.

ANKARA ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü'ne

Prof. Dr. Fatih RUKANCI danışmanlığında hazırladığım "Hassas Bilgi İçerikli Kamu Belgelerinin Değerlendirilmesi (Ankara. 2025)" adlı doktora tezimdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

31.01.2025

Hasan ÖZTÜRK

ÖNSÖZ

Bilgi çağının dinamik yapısı, bilgi üretimi, paylaşımı ve kullanımına dair olanakları her geçen gün daha da genişletmektedir. Ancak, bu dönüşüm beraberinde bilgiyi koruma ve doğru yönetme sorumluluğunu da artırmıştır. Bilginin yönetiminde, bazı bilgilerin diğerlerine kıyasla daha yüksek bir hassasiyete sahip olduğu gerçeği, bu bilgilerin potansiyel zararının da büyük olduğunu göstermektedir. Bu durum, sosyal ağ ortamlarında sıklıkla gözlemlenmekte, belirli fotoğraf ve videoların yalnızca "hassas içerik" uyarılarıyla erişime açılmasına sebep olmaktadır. Sosyal medya platformlarındaki bu uygulamalar, hassas içeriklerin korunması adına önemli bir önlem niteliğindedir. Bu bakımdan hassas bilgi içeren her türlü ortamın ve içeriğin benzer düzeyde yönetilmesi gerekmektedir. Özellikle kamu belgelerinde yer alan hassas bilgiler, toplumun güvenliği ve bireylerin mahremiyeti açısından büyük önem taşımaktadır. Hassas bilgi içeren kamu belgelerinin ulusal arşiv kurumlarına aktarım süreci boyunca belge yönetimi ve arşivcilik esasları doğrultusunda nasıl yönetileceği ve değerlendirileceğinin kapsamlı bir şekilde incelemesi gerekmektedir. Ülkemizde kamu kurumları, bilgi-belge güvenliği ve gizliliği hususunda çeşitli mevzuat düzenlemelerine tabi olup ulusal arşiv kurumumuz olan T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı'nın direktifleri doğrultusunda belge yönetimi ve arşivleme süreçlerini yürütmektedir. Bu çalışma, kamu belgelerinin hassasiyet açısından değerlendirilmesi ve arşive intikali sürecini araştırmaktadır. Bu sebeple, hassas bilgi içeren kamu belgelerinin daha etkin bir şekilde yönetilmesine ve arşivlenmesine katkı sağlayacağı; denetim ve yönlendirme makamlarına, karar vericilere ve bu alanda çalışan araştırmacılara yol gösterici bir perspektif sunacağı ümit edilmektedir.

Tez çalışmam boyunca, desteğini her zaman yanımda hissettiğim; yönlendirmeleri ve motivasyonlarıyla büyük katkılar sunan değerli danışmanım Prof. Dr. Fatih RUKANCI'ya içtenlikle teşekkür ederim. Tez izleme komitesinde bilgisi ve farklı bakış

açısıyla tez sürecini zenginleştiren Prof. Dr. Hakan ANAMERİÇ'e, sürekli yardım ve destekleriyle yanımda olan Doç. Dr. Ahmet ALTAY'a gönülden teşekkürlerimi sunarım. Tez savunma jürisinde yer alarak çalışmaya önemli katkılar sunan Prof. Dr. Sacit ARSLANTEKİN'e ve Doç. Dr. Bahattin YALÇINKAYA'ya değerli değerlendirmeleri ve yapıcı geri bildirimleri için teşekkür ederim. Çalışmanın çıkış noktasından itibaren olgunlaşmasını sağlayarak yazım sürecine ilham katan Doç. Dr. Lale ÖZDEMİR ŞAHİN'e ayrıca teşekkür ederim.

Bartın Üniversitesi Bilgi ve Belge Yönetimi bölümünde birlikte görev aldığım tüm değerli öğretim elemanlarına teşekkürlerimi sunarım. Her zaman yanımda olan, kolaylaştıran ve çözüm sağlayan Dr. Öğr. Üyesi Nuri TAŞKIN, Arş. Gör. Dr. Mehmet Kürşat DEĞER ve Arş. Gör. Ceren Bilge SEFEROĞLU'na şükranlarımı sunarım.

Araştırma sürecimde bana kapılarını açan kurumlara, dönüş sağlayan ulusal arşiv kurumlarına ve değerli bilgilerini benimle paylaşan uzmanlara teşekkür ederim.

Bu tez çalışmasının bir diğer önemli kısmı da ailem ve dostlarımın manevi desteğidir. Her zaman yanımda olan, beni motive eden ve çalışmalarımda bana güç veren değerli dostum Ali Eren KARAKANLI'ya, aileme ve arkadaşlarıma da sonsuz teşekkürlerimi sunarım. Bu çalışmanın her aşamasında desteğini ve sevgisini esirgemeyen Mesude GÜLER'e teşekkür ederim. Sağladığı manevi güç, bu süreci daha anlamlı kıldı.

Hasan ÖZTÜRK

İÇİNDEKİLER

ÖNSÖZ ..... **İ**

İÇİNDEKİLER ..... **İİİ**

KISALTMALAR ..... **Vİİ**

TABLOLAR LİSTESİ ..... **Vİİİ**

GÖRSELLER LİSTESİ ..... **İX**

ŞEMALAR LİSTESİ ..... **X**

GRAFİKLER LİSTESİ ..... **Xİ**

ŞEKİLLER LİSTESİ ..... **Xİİ**

I. BÖLÜM: GİRİŞ **1**

I.1. Amaç ve Önem 4

I.2. Kapsam 5

I.3. Araştırma Problemi, Sorular ve Hipotez 6

I.4. Yöntem 7

I.5. Kaynaklar 11

I.6. Düzen 12

I.7. Terimler 13

II. BÖLÜM: HASSAS BİLGİ MEVZUATI **16**

II.1. Kavramsal Çerçeve 16

II.2. Hassas Bilgi Kavramı 18

II.3. Mevzuat Düzenlemelerinde Hassas Bilgi 21

II.3.1. Ulusal ve Uluslarüstü Mevzuat Düzenlemelerinde Hassas Bilgi 22

II.3.2. Türkiye'deki Mevzuat Düzenlemelerinde Hassas Bilgi 30

II.3.3. Hassas Bilgilerin İşlenmesi 38

II.4. Hassas Bilgi Türleri 55

II.4.1. Kişisel Tanımlanabilir Bilgiler 58

II.4.1.1. Sağlık Bilgisi 61
II.4.1.2. Finansal ve Ticarî Bilgiler 62
II.4.1.3. Sosyal ve Özel Hayat Bilgileri.....63
II.4.2. Kamu Kaynaklı Bilgiler 63
II.4.3. İhtisas Alanı ve Sektör Bilgileri 67
III. BÖLÜM: HASSAS BİLGİ İÇERİKLİ KAMU BELGELERİ.....71
III.1. Hassasiyet Değerlendirmesi Yöntem ve Süreci.....75
III.1.1. Anonimleştirme-Maskeleme.....83
III.1.2. Redaksiyon 86
III.1.3. Kapatma/Kapalı Tutma.....89
III.1.4. Kamu Yararına Erişime Sunmak 92
III.2. Hassasiyet Değerlendirmesi Zorlukları 93
III.2.1. Bağlam ve İlişki Kurma.....95
III.2.2. Zaman 99
III.2.3. Belge Hacmi, Kaynak ve Bütçe.....103
III.2.4. Mevzuat 104
III.2.5. Sosyal ve Kültürel Farklılıklar 106
III.2.6. Kişisel Bakış ve Deneyim 108
III.3. Geleneksel Değerlendirme ve İnsan Değerlendirici 109
III.4. Dijital Değerlendirme ve Yardımcı Araçlar 112
IV. BÖLÜM: ULUSAL ARŞİVLERDE HASSASİYET DEĞERLENDİRMESİ YAKLAŞIMLARI 122
IV.1. İngiltere (The National Archives/TNA) 122
IV.2. Amerika Birleşik Devletleri (National Archives and RecordsAdministration/NARA) 125
IV.3. Yeni Zelanda (Archives New Zealand) 128

IV.4. İskoçya (National Records of Scotland) 130
IV.5. Estonya (National Archives of Estonia) 132
IV.6. İsviçre (Swiss Federal Archives) 133
IV.7. Kanada (Library and Archives Canada) 134
IV.8. Slovenya (Archives of the Republic of Slovenia) 137
IV.9. Türkiye'deki Yaklaşım 140
V. BÖLÜM: HASSASİYET DEĞERLENDİRMESİ SÜRECİNE İLİŞKİN UZMAN GÖRÜŞÜ ARAŞTIRMASI 156
V.1. Görüşme Sorularının Hazırlanması 156
V.2. Çalışma Grubu 157
V.3. Görüşmenin Uygulanması 160
V.4. Araştırmanın Geçerliği ve Güvenirliği 162
V.5. Veri Analizi 164
V.6. Bulgular 166
V.6.1. Kelime Bulutu 169
V.6.2. Tema ve Kategorilerin Kod Matrisi 169
V.6.3. Tema Trendleri 171
V.6.4. Tema: Hassas Bilgi 172
V.6.4.1. Kategori: Hassas Bilgi Mevzuatı 173
V.6.4.2. Kategori: Hassas Bilgi Kapsamı 174
V.6.4.3. Kategori: Hassas Bilgi Tespiti 175
V.6.5. Tema: Hassasiyet Değerlendirmesi 177
V.6.5.1. Kategori: Değerlendirme Yaklaşımı 178
V.6.5.2. Kategori: Fiziksel ve Dijital Değerlendirme 180
V.6.6. Tema: Değerlendirme Zorlukları ve Çözümler 181
V.6.6.1. Kategori: Süreç Zorlukları 183

V.6.6.2. Kategori: Objektifliği Sağlamaya Yönelik Çözümler.....189
V.6.6.3. Kategori: Zamana Yönelik Çözümler.....190
V.6.6.4. Kategori: Mozaik Yapıya İlişkin Çözümler.....191
V.6.6.5. Kategori: Erişime Sunmaya Yönelik Çözümler.....193
V.6.7. Tema: Teknoloji Yardımlı Değerlendirme.....195
V.6.7.1. Kategori: Yardımcı Araçların Rolü.....196
V.6.7.2. Kategori: Yapay Zekâ.....198
V.6.7.3. Kategori: Otonom Değerlendirme.....201
V.6.7.4. Kategori: Bilgi Edinme Hakkı Talebi.....202
V.6.7.5. Kategori: Hukukî, Teknik ve Etik Problemler.....204
V.6.8. Tema: Danışma Kurulları ve Kaynakları.....205
V.6.8.1. Kategori: Kurulların Yapısı.....207
V.6.8.2. Kategori: Kişilerin Niteliği.....209
V.6.8.3. Kategori: Rehber/Kılavuz Oluşturmak.....210
VI. BÖLÜM: DEĞERLENDİRME, SONUÇ VE ÖNERİLER.....212
KAYNAKÇA.....233
EKLER.....256
Ek 1: Etik Kurul İzni.....256
Ek 2: Aydınlatılmış Onam Formu.....258
Ek 3: Yarı Yapılandırılmış Görüşme Formu.....261
Ek 4: Uzman Görüş Daveti Mail Örneği.....264
Ek 5: Kod Kitabı.....265
ÖZET.....268
SUMMARY.....270

KISALTMALAR

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AP	Avrupa Parlementosu
BAYS	Bütünleşik Arşiv Yönetim Sistemi
BEHK	Bilgi Edinme Hakkı Kanunu
BETSİS	Belge Tarama Sistemi
Bkz.	Bakınız
BM	Birleşmiş Milletler
CLIR	Council on Library and Information Resources (Kütüphane ve Bilgi Kaynakları Konseyi)
DAB	Devlet Arşivleri Başkanlığı
EBYS	Elektronik Belge Yönetim Sistemi
FOIA	Freedom of Information Act (Bilgi Edinme Hakkı Kanunu)
GDPR	General Data Protection Regulation (Genel Veri Koruma Tüzüğü/GVKT)
ICA	International Council on Archives (Uluslararası Arşiv Konseyi)
IFLA	International Federation of Library Associations (Uluslararası Kütüphane Dernekleri Federasyonu)
IP	Internet Protocol (İnternet Protokolü)
KVKK	Kişisel Verilerin Korunması Kanunu
NARA	National Archives and Records Administration (ABD Ulusal Arşivler ve Kayıtlar İdaresi)
NATO	North Atlantic Treaty Organization (Kuzey Atlantik Antlaşması Örgütü)
OECD	Organisation for Economic Co-Operation and Development (Ekonomik Kalkınma ve İş birliği Örgütü)
TCK	Türk Ceza Kanunu
TNA	The National Archives (İngiltere Ulusal Arşivleri)
TSE	Türk Standartları Enstitüsü

TABLOLAR LİSTESİ

Tablo 1. Görüşme Yapılan Kurumlar 10

Tablo 2. Ulusal Düzenlemelerde Hassas Bilgi 35

Tablo 3. Uluslarüstü Düzenlemelerde Hassas Bilgi 36

Tablo 4. Veri Maskeleme İşlemi 85

Tablo 5. Mevzuat, Standartlar ve Rehber 141

Tablo 6. Katılımcıların Mezun Oldukları Bölümler 158

Tablo 7. Katılımcıların Eğitim Düzeyleri 158

Tablo 8. Katılımcıların Görev Süreleri 159

Tablo 9. Görüşme Tarihleri ve Süreleri 161

Tablo 10. Geçerlik ve Güvenirlik Uygulamaları 162

Tablo 11. Araştırma-Görüşme Soruları Tema İlişkisi 168

Tablo 12. Temaların ve Kategorilerin Katılımcılara Göre Dağılımı 170

Tablo 13. Hassas Bilgi Temasına Ait Kategori ve Kodlar 172

Tablo 14. Hassasiyet Değerlendirmesi Temasına Ait Kategori ve Kodlar 177

Tablo 15. Değerlendirme Zorlukları ve Çözümler Temasına Ait Kategori ve Kodlar..182

Tablo 16. Teknoloji Yardımlı Değerlendirme Temasına Ait Kategori ve Kodlar 195

Tablo 17. Danışma Kurulları ve Kaynakları Temasına Ait Kategori ve Kodlar.....206

Tablo 18. Hassasiyet Değerlendirmesi Kontrol ve Tanımlama Listesi 228

GÖRSELLER LİSTESİ

Görsel 1. Veri Koruma ve Gizlilik Yasaları 23

Görsel 2. Hong Kong: Siyasî Hassas Meseleler 124

Görsel 3. Faili Meçhul Cinayet.....125

Görsel 4. 1961-1963 ABD Dışişleri Gelen-Giden Telgraflar 126

Görsel 5. 1969-1973 Vaka Raporları 127

Görsel 6. Kraliyet Topçusu G. N. Taylor 129

Görsel 7. Penman Ailesine İlişkin Belge 130

Görsel 8. Yüksek Mahkeme Belgelerine Erişim Talebi 131

Görsel 9. Kraliyet Ofisi Görüşleri- Ölümlü Kaza Soruşturmaları.....132

Görsel 10. Anonimleştirilmiş Belge 134

Görsel 11. 1960-1985 Alberta Üniversitesi Siyasî Faaliyetler 135

Görsel 12. Erişim Sınırı Olan Belge Talebi 136

Görsel 13. Görüşme Verilerine Ait Kelime Bulutu.....169

ŞEMALAR LİSTESİ

Şema 1. Araştırmanın Yöntem Çerçevesi.....9

Şema 2. Hassas Bilgi Sınıflaması.....57

Şema 3. Hassasiyet Değerlendirmesi Kontrol ve Tanımlama İş Akış Şeması.....230

GRAFİKLER LİSTESİ

Grafik 1. 114 Ülkenin Bilgi Edinme Muafiyetleri 38

Grafik 2. Katılımcılara Göre Tema Trendleri.....171

Grafik 3. Hassas Bilgi Mevzuatı 173

Grafik 4. Hassas Bilgi Kapsamı 174

Grafik 5. Hassas Bilgi Tespiti.....176

Grafik 6. Değerlendirme Yaklaşımı 178

Grafik 7. Fiziksel ve Dijital Değerlendirme 180

Grafik 8. Süreç Zorlukları 183

Grafik 9. Objektifliği Sağlamaya Yönelik Çözümler.....189

Grafik 10. Zamana Yönelik Çözümler 190

Grafik 11. Mozaik Yapıya İlişkin Çözümler.....192

Grafik 12. Erişime Sunmaya Yönelik Çözümler.....193

Grafik 13. Yardımcı Araçların Rolü.....196

Grafik 14. Yapay Zekâ 199

Grafik 15. Otonom Değerlendirme.....201

Grafik 16. Bilgi Edinme Hakkı Talebi 203

Grafik 17. Hukukî, Teknik ve Etik Problemler 204

Grafik 18. Kurulların Yapısı.....207

Grafik 19. Kişilerin Niteliği 209

Grafik 20. Rehber/Kılavuz Oluşturmak 210

ŞEKİLLER LİSTESİ

Şekil 1. Redaksiyon İşlemi 88

Şekil 2. Dijital Hassasiyet Değerlendirmesi Girdi, Süreç ve Çıktı.....114

Şekil 3. Millî Gizlilik Dereceleri 143

I. BÖLÜM: GİRİŞ

Bilgi üretimi; finans, sağlık, eğlence ve eğitim gibi birçok endüstri ve sektörün önemli bir parçasıdır. Üretilen ve işlenen bilgi/veri hacminin büyümesi, bilginin niteliğine bağlı olarak koruma düzeyini etkilemektedir. Veri miktarının fazlalığı, potansiyel olarak daha yüksek bilgi ihlali risklerini ortaya çıkarmaktadır. Bu durum özellikle finans kuruluşları, sağlık hizmeti sağlayıcıları ve kamu kurumları gibi büyük miktarlarda hassas veya gizli bilgi/belge bulunduran organizasyonlar için zorlayıcı olabilir. Ne kadar çok bilgi üretilir ve depolanırsa, bu bilgileri taşıyan belgelerin etkin bir şekilde yönetilmesi ve güvenliklerin sağlanması o kadar zorlaşmaktadır. Belge üretiminin doğal olarak varlık gösterdiği yapılarda – özellikle kamu kurumlarında – vatandaşların haklarını korumak, veri ihlali risklerini azaltmak ve hassas bilgi taşıyan belgelerin korunmasını sağlamak için kurumların bilgi güvenliği ve gizliliği önlemlerini uygulaması beklenmektedir.

Bilginin niteliği, ihtiyaç duyulan koruma düzeyini etkileyebilmektedir. Örneğin, ticarî sırlar veya fikrî mülkiyet kamuya açık genel bilgilerden daha yüksek düzeyde koruma gerektirebilir. Bu durum, ticarî sırların ve gizli bilgi içeren belgelerin kaybolmasının veya çalınmasının kurumlar için önemli malî ve itibarî sonuçlar doğurabilmesinden kaynaklanmaktadır. Ayrıca hukukî problemlere de yol açmaktadır. Kamuda ve birçok sektörde, kurumların belirli belge türlerini korumasını gerektiren düzenlemeler bulunmaktadır. Bu düzenlemelere uyulmaması, maddî veya kişi hürriyetini sınırlandıran ciddi cezalara sebep olmaktadır. Kişisel bilgiler, finansal bilgiler, ticarî sırlar ve fikrî mülkiyet gibi hassas bilgilerin kamu kurumlarında dolaşımda olması, depolanması ve paylaşılması giderek artarken, bu bilgileri yetkisiz erişime karşı korumak oldukça önemli hale gelmektedir. Kurumların bu tür bilgi taşıyan belgeleri etkili bir şekilde korumak için mevzuat, standartlar ve politikalar çerçevesinde gizlilik anlaşmaları, kısıtlı erişim kontrolleri ve ağ faaliyetlerinin izlenmesi gibi ek güvenlik önlemleri

almaları gerekebilir. Kamu bağlamında bilgi güvenliğinin sağlanması, kamu veya özel kurumlarda bireylerin güvenliğinin sağlanmasında büyük ölçüde etkilidir. Özellikle anılan içerikteki belge dolaşımının yürütüldüğü kamu kurumlarında bilgi güvenliği ve gizliliğine daha fazla ihtiyaç duyulmaktadır.

Bilgi ve veri güvenliği; gizli, hassas veya değerli bilgilerin kamu ve kişi hakları dikkate alınarak yetkisiz erişim, kullanım, ifşa ve değişikliklerden korumanın güvence altına alınmasını içeren bir süreçtir. Bu süreç, öncelikle bilgi varlıklarına yönelik potansiyel tehditlerin ve güvenlik açıklarının belirlendiği bir risk değerlendirilmesini içermektedir. Her tehdidin ve güvenlik açığının potansiyel etkisinin değerlendirilmesi, uygulanacak güvenlik kontrollerinin ve prosedürlerinin ana hatlarını oluşturmaktadır. Kamu veya özel kurumlarda bilgi/belge güvenliği söz konusu olduğunda gizlilik (*confidentially*), bütünlük (*integrity*) ve erişilebilirlik (*availability*) ilkeleri güvenliği oluşturan temel unsurlar olarak ifade edilmektedir (Tipton, 1998, s. 1; Tekerek, 2008, s. 133; Rukancı, Anameriç ve Başar, 2021, s. 107). Bilginin gizlilik esaslı olarak değişime ve bozulmaya uğramadan bütünlüğü korunarak yetkili kullanıcılar tarafından erişilmesi bilgi güvenliğinin sağlanabilmesi için esastır. Gizlilik, belgenin içeriği ile ilgili bir değerlendirme ilkesidir. Gizliliğe aykırı ifadeler kişi mahremiyeti ve kamu güvenliğini etkileyebilmektedir. Hassas/nitelikli kişisel bilgilere erişimi kapatmak, yetkisiz kişiler tarafından erişimini engellemek gizlilik ilkesine bağlı olarak kamu kurumlarındaki belge yönetimi ve arşiv süreçlerinde uygulanmaktadır. Gizlilik risklerinin yeterince ele alınmaması ve veri ihlallerinin yaşanması, bu tür belgelerin yer aldığı arşivlere ve kamuya olan güveninin zarar görebileceği anlamına gelmektedir (Lemieux ve Werner, 2024, s. 3). Bu süreçte ayrıca belge içeriğinin ortama (*medium*) bağlı olarak değiştirilme, bozulma, eskime ve tahribata uğramadan bütünlüğünün korunması gerekmektedir.

Kamu kurumlarında hassas bilgi içeren belgeler bulunmaktadır. Toplumların kolektif hafızasını oluşturan, tarihî, idarî, kültürel ve bilimsel öneme sahip kamu

belgeleri, arşiv belgesi kimliği kazanarak arşiv kurumlarına aktarılmaktadır. “Arşivler kişi ve kurumların belirli bir zaman süresi içerisinde kendi yaşamı ve işleyişi için kullanmak amacıyla ürettikleri belgeleri organize eden bir sistem olarak nitelendirilebilir” (Rukancı, Anameriç ve Başar, 2023, s. 8). Sosyal devlet olmanın bir gerekliliği olarak özellikle vatandaşların doğumundan ölümlerine kadar biriken veriler toplanarak arşivlenmektedir. Bu süreçte veri ihlallerinin en az düzeyde tutulması kamu ve kişi haklarının korunmasına yardımcı olacaktır. 2017 yılında IBM (International Business Machine/ Uluslararası İş Makinesi) desteği ile yapılan bir araştırmaya göre, hassas bilgi ihlalinin ortalama maliyeti 3,62 milyon dolardır (Ponemon Institute, 2017, s. 1). Bilgi ihlalinin maddî olduğu kadar kişiler için utanç ve ayrımcılık, kurumlar özelinde itibar zedelenmesi ve adaletsizlik gibi manevi zararları da bulunabilmektedir. Bu duruma sebebiyet veren belgeler, bilgi güvenliği ve gizliliği gözetilerek tam veya kısıtlı kapatma işlemlerine tabi tutulmaktadır. Kamu kurum ve kuruluşlarında “gizlilik” ve “gizli belge” hususu içerisinde yer alan hassas bilgi içeren belgeler, toplumun güvenliğini sağlamak, vatandaşların haklarını korumak ve kurumları işler kılmak için son derece önemlidir.

Bu çalışmada hassas bilgi içeren kamu belgelerinin hassasiyet değerlendirmesi bir süreç yönetimi bakış açısı ile incelenmektedir. Bu çerçevede, kurumların doğal faaliyetleri sonucu üretilen arşiv belgeleri arasında hassas bilgi içerenlerin güvenliği ve mahremiyetinin sağlanmasına yönelik süreçlerin yapılandırılması, yönetilmesi ve denetlenmesine dair öneriler sunulmaktadır. Çalışmada, hassas verilerin sınıflandırılması, risk değerlendirmesi, yetki kontrol mekanizmalarının oluşturulması ve bu süreçlerin sürdürülebilir bir şekilde yürütülmesi için gerekli adımlar ayrıntılı olarak incelenmektedir.

I.1. Amaç ve Önem

Arşivler gizlilik ve bilgi güvenliği misyonuyla kamu ve kişi haklarını koruyarak, bilgileri/belgeleri güvenli, doğru ve yetkilendirilmiş erişime açık bir şekilde muhafaza etmektedir. Bu süreç veri koruma yasaları, fikri mülkiyet hakları ve gizlilik düzenlemeleri gibi ulusal/uluslararası yasal düzenlemelere ve etik standartlara uygun olarak gerçekleştirilmelidir. Arşivler ait olduğu toplumda kişisel ve kurumsal bilgilerinin gizliliğini koruma yükümlülüğünü üstlenmektedir. Hassas bilgiler içeren belgelerin yönetilmesi ve arşivlenmesi bu sürecin en kritik safhasıdır. Belgelerin hassas bilgi kontrollerinin sağlandığı önemli bir süreç olan hassasiyet değerlendirmesi çoğu ulusal arşiv tarafından yürütülmektedir. Ülkemizde belgelerin gizliliği olarak bilinen bu süreçteki uygulamalar, içerik (*content*) odaklı bir yön ile ilgilenmektedir. Hassas bilgi içeren belgelerin hassasiyet değerlendirmesi işleminden geçmesi bilgi güvenliğinin ve gizliliğinin sağlanması için özen gösterilmesi gereken bir adımdır. Bu bağlamda çalışmanın temel amaçları:

- Türkiye'de belge güvenliği ve gizliliğinin geliştirilmesine katkı sağlayacak "hassasiyet değerlendirmesi süreci" konusunda bilgi ve farkındalık oluşturmak,
- Hassasiyet değerlendirmesi sürecinde karşılaşılan zorlukları tespit etmek, çözüm geliştirmek, bu konuda hukukî, teknolojik, yönetimsel yaklaşımların geliştirilmesine katkı sağlamak olarak belirlenmiştir.

Belirtilen amaçlara ulaşabilmek amacıyla ilgili literatür araştırması, ulusal arşivlerden örnekler ve ayrıca konu uzmanı yetkililer ile görüşmeler yapılmıştır. Bu bağlamda, araştırma sonuçlarının ilgili alanda çalışan akademisyenler, profesyoneller ve politika yapıcıları için kapsamlı bir kaynak oluşturması; Türkiye'deki araştırma boşluğunu kavramsal ve pratik düzeyde doldurması beklenmektedir.

I.2. Kapsam

Araştırma, kamu belgelerinin güvenliği ve gizliliği konusunun odak bir yönü olan hassasiyet değerlendirmesi sürecini kapsamaktadır. Hassasiyet değerlendirmesi, çeşitli faktörler doğrultusunda hassas olan belgelerin ulusal arşive intikali sürecinde ve sonrasında yönetimini içermektedir. Bu kapsamda literatür araştırması başta olmak üzere çalışma, hassas bilgi içeren belgeler konusundaki yaklaşımları ele alan araştırmaları kapsamaktadır. Bunun yanı sıra çalışmada öncelikle dünyada ve Türkiye'de gizlilik/koruma mevzuatında yer alan hassas bilgi türlerine ve işlenme koşullarına değinilmiştir. Belirlenen ülkeler seçilirken; farklı coğrafya, kültür, idarî teşkilat ve yönetim şeklinden unsurların yansıtılması amaçlanmıştır. Ancak benzer coğrafya ve kültürden örneklerdeki farklılıkların yansıtılabilmesi amacıyla bazı örnekler de yer almaktadır. Çeşitli ülkelerin, uluslarüstü kuruluşların ve Türkiye'nin hassas bilgi türleri konusundaki sınıflamaları ve işlenme koşulları aktarıldıktan sonra arşiv uygulamaları kapsamında hassas bilgi türlerine dair bir sınıflama geliştirilmiştir.

Çalışma kapsamında uygulamadaki faaliyetlerin yansıtılabilmesi amacıyla farklı ulusal arşivler örnek olarak sunulmuştur. Bu kurumların hassasiyet değerlendirmesi konusundaki arşiv mevzuatı, rehber/kılavuz dokümanları ve çevrimiçi katalogları incelenmiştir. Ulusal arşiv örnekleri belirlenirken uygulamaya yön veren, yenilikçi, köklü ve çalışma konusuna uygun olması kriterleri göz önünde bulundurulmuştur. Ayrıca e-posta yazışmaları ile ön görüşmeler yapılmış, kurumların ilgili alandaki faaliyetlerine ilişkin bilgi talepleri ve gelen dönüşler belirleyici olmuştur. Bununla birlikte ülkemizde yürürlükte olan arşiv mevzuatı, Devlet Arşivleri Başkanlığı'nın web sayfasında yer alan dokümanlar ve çalışmalar bu kapsamda değerlendirilmiştir.

Çalışma kapsamında yapılan görüşmelerde yer alacak kişilerin belirlenmesi yöntem bölümünde (1.4. Yöntem) ifade edildiği üzere maksimum bir çeşitlilik anlayışına göre yapılmıştır. Ağırlıklı olarak ülkemizde çalışmalar yürüten kamu uygulamasında yer

alan veya bu alanda bilimsel çalışmalar yürüten katılımcılar tercih edilmiştir. Bu noktada idarî bakımdan farklı kurumlarda görevli kişiler, çalışma kapsamına uygun olarak seçilmiştir. Hassasiyet değerlendirmesi konusunda öncü bir kurum olan İngiltere Ulusal Arşivi'nden ve Londra Wellcome Kütüphanesinden katılımcıların yer alması hem uluslararası katılımcı çeşitliliğini sağlanmış hem de nitelikli bulguların gelişmesine katkı sağlamıştır.

I.3. Araştırma Problemi, Sorular ve Hipotez

Araştırmanın temel problemi "*Türkiye'de hassasiyet değerlendirmesi süreci hakkında; hukukî, teknolojik ve arşivcilik uygulamaları konusunda bilgi ve farkındalık eksikliğinin bulunması*" olarak belirlenmiştir.

Araştırma problemi kapsamında konunun genel olarak anlaşılabilmesi amacıyla aşağıdaki sorulara cevap aranmaktadır:

- Dünyada ve Türkiye'de veri koruma/gizlilik veya kişisel veri mevzuatında hangi bilgiler hassas olarak nitelendirilmektedir? Bu bilgilerin kapsamı, tespiti ve işlenme koşulları nasıl belirlenmelidir?
- Hassas bilgi içerikli belgelere yönelik değerlendirme süreci (hassasiyet değerlendirmesi) nasıl yürütülmelidir? Bu süreç fiziksel ve dijital ortama göre farklılık oluşturur mu?
- Hassasiyet değerlendirmesi sürecinde yaşanan zorluklar nelerdir? Bu zorluklar hangi yöntemler ile çözülebilir?
- Dijital hassasiyet değerlendirmesi nedir? Dijital araçların/yazılımların hassasiyet değerlendirmesi sürecinde fonksiyonları/katkıları nelerdir? Bu araçlar hassasiyet değerlendirme sürecinde kullanılmalı mıdır?
- Hassasiyet değerlendirmesi sürecinde danışma/gizlilik kurullarının ve kaynaklarının (rehber, kılavuz, talimatname vs.) rolü ve niteliği ne olmalıdır?

- Hassasiyet değerlendirmesi konusunda ulusal arşivlerin uygulamaları nelerdir? Türkiye'deki mevcut durum nedir?

Araştırma problemi ve soruları çerçevesinde araştırmanın temel hipotezi (H1); "*Türkiye'de hassas bilgi güvenliğini sağlamak amacıyla, T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı başta olmak üzere kamu kurumlarında hassasiyet değerlendirmesi sürecinin doğru yönetimi için yasal düzenlemeler, kapsamlı politika belgeleri, rehberler, kontrol listeleri, danışma kurulları oluşturulmalı ve güçlü bir dijital altyapı geliştirilmelidir*" olarak tanımlanmıştır. Bu kapsamda araştırmanın temel hipotezine bağlı olarak oluşturulan alt hipotezler aşağıda sıralanmıştır:

- Hassasiyet değerlendirmesi sürecinde, yürürlükte olan gizlilik/koruma mevzuatında listelenen hassas bilgi türleri, belge içeriklerinde bulunan yeni veya gelişen hassas veri türlerini tanımlamakta yetersiz kalmaktadır (H1.1).
- Hassasiyet değerlendirmesi sürecinde, değerlendiricilere yardımcı olacak kontrol listeleri ve kılavuzlar gibi rehber dokümanların hazırlanması sürecin etkinliğini artıracaktır (H1.2).
- Dijital araçlar ve yazılımlar, hassasiyet değerlendirme sürecinde tespit, belge hacmini yönetme, uzman bilgisi sağlama, danışma ve uyarı mekanizmalarını geliştirme bakımından yönetimi olumlu yönde etkileyecektir (H1.3).

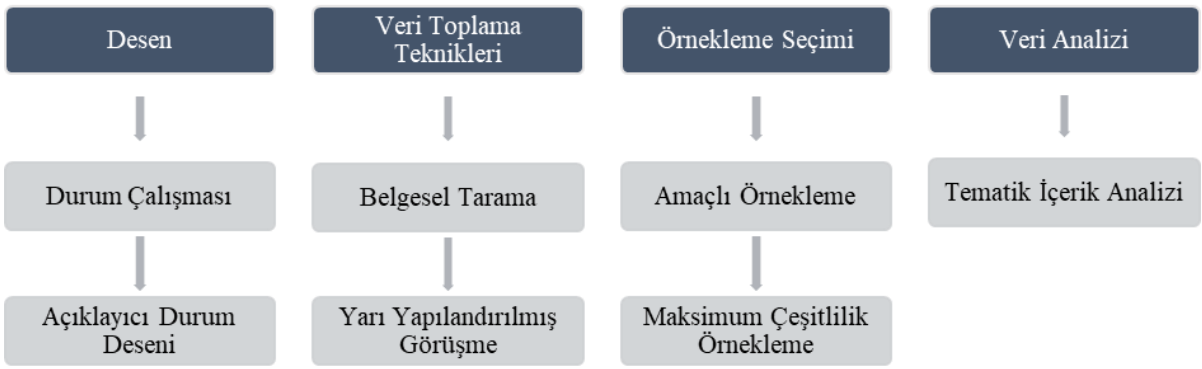
I.4. Yöntem

Araştırmada odaklanılan konu ve sorular bağlamında derinlemesine verilere ulaşabilmek amacıyla nitel araştırma yöntemleri tercih edilmiştir. Nitel araştırma "gözlem, görüşme ve doküman analizi gibi nitel veri toplama yöntemlerinin kullanıldığı, algıların ve olayların doğal ortamda gerçekçi ve bütüncül bir biçimde ortaya konmasına yönelik nitel bir sürecin izlendiği araştırmalardır" (Yıldırım ve Şimşek, 2021, s. 37). Nitel araştırma desenleri arasından durum çalışması kullanılmıştır. Durum çalışması deseni:

> Araştırmacının gerçek yaşam, güncel sınırlı bir sistem (bir durum) ya da belli bir zaman içerisindeki çoklu sınırlandırılmış sistemler (durumlar) hakkında çoklu bilgi kaynakları (örneğin gözlemler, mülakatlar, görsel-işitsel materyaller ve dokümanlar ve raporlar) aracılığıyla detaylı ve derinlemesine bilgi topladığı, bir durum betimlemesi ya da durum temaları ortaya koyduğu nitel bir yaklaşımdır (Creswell, 2013, s. 97).

Bu desenin bir türü olan açıklayıcı durum çalışması (*explanatory case study*), "nedensel ya da çıkarımsal bir araştırma sorusunu takip eden çalışmalarda kullanışlı" (Berg ve Lune, 2019, s. 333) olduğundan bu yaklaşım doğrultusunda hareket edilmiştir. Araştırmanın veri toplama sürecinde öncelikle doküman inceleme (belgesel tarama) yöntemi kullanılmıştır. "Doküman incelemesi, araştırılması hedeflenen olgu veya olgular hakkında bilgi içeren yazılı materyallerin analizini kapsar" (Yıldırım ve Şimşek, 2021, s. 189). Bu doğrultuda konuya ilişkin literatürde yer alan dokümanlar sistematik olarak analiz edilerek içindekiler bölümü yapılandırılmış ve bir kuramsal çerçeve oluşturulmuştur. Sonrasında sosyal bilimlerde ve nitel araştırmalarda en sık kullanılan veri toplama aracı olan görüşme uygulanarak "bireylerin konu kapsamındaki deneyimlerine, tutumlarına, görüşlerine, şikâyetlerine, duygularına ve inançlarına ilişkin bilgiler elde etmek" mümkün olmuştur (Yıldırım ve Şimşek, 2021, s. 127). Araştırmada, çeşitli kurumlarda görevli ilgili konuda bilgi sahibi olan, uygulama tecrübesi olan veya bilimsel çalışmalar yürümüş uzmanlara yarı yapılandırılmış görüşme soruları yönetilmiştir. Yarı yapılandırılmış görüşme, "araştırmacı tarafından önceden belirlenmiş ya da görüşme sırasında ortaya çıkan konulara göre yeni soruların da sorulabildiği bir görüşme yöntemi olarak nitel araştırmalarda yaygın olarak kullanılan bir veri toplama yöntemidir" (Güler, Halıcıoğlu ve Taşkın, 2015, s. 115). Belirli bir konuda daha fazla bilgi edinmek ve katılımcılardan daha esnek cevaplar almak amacıyla kullanılmaktadır. Çalışmada yer alan katılımcılar belirlenirken amaçlı örnekleme yaklaşımlarından

maksimum çeşitlilik örnekleme yöntemine başvurulmuştur. Amaçlı örneklemenin amacı çalışmaya uygun olan katılımcıların seçilmesidir. "Amaçlı bir örneklem geliştirilirken, araştırmacılar bu evreni temsil eden denekleri seçmek için özel bilgilerini veya uzmanlıklarını bazı gruplarla ilgili olarak kullanırlar" (Berg ve Lune, 2019, s. 67). Maksimum çeşitlilik örneklemesi ise "genellikle bir araştırmacının çalışmanın başlangıcında maksimum farklılığı sağlamak istediğinde seçilmekte, ideal bir nitel araştırmada bulguların farklı bakış açılarını veya farklılıkları yansıtma olasılığını artırmaktadır (Creswell, 2013, s. 298). Katılımcıların çalışma amacına bağlı olarak maksimum çeşitlilikte olması görüş ve bilgiler çeşitliliğini artırmıştır. Verilen bilgilere bağlı olarak çalışma için oluşturulan araştırma yöntemi çerçevesi aşağıdaki (Şema 1'de sunulan) gibidir.



Şema 1. Araştırmanın Yöntem Çerçevesi

Odak konuda bilimsel çalışmaları olan veya kamu ve arşiv uygulamalarında görev alan 7 kurumdan 8 gönüllü katılımcı ile görüşmeler yapılmıştır. Görüşmelerin yapıldığı kurumlar, anılan niteliklere sahip kişilerin çalıştığı yerler olmasına göre belirlenmiştir. Bu kurumlar ve katılımcı sayıları Tablo 1'de belirtilmiştir.

Tablo 1. Görüşme Yapılan Kurumlar

Kurum adı	***n***	***%***
T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı	1	12,5
Millî Savunma Bakanlığı	2	25.0
Bartın Üniversitesi	1	12,5
Basın İlan Kurumu	1	12,5
Anadolu Ajansı	1	12,5
The National Archives (UK)	1	12,5
London Wellcome Library	1	12,5
Toplam	8	100

Odak konu gereği çeşitli veriler elde edileceği düşünülerek bir kurumda birden fazla kişi ile görüşülmüştür. Bu sebeple belirlenmiş olan kurumlarda görüşmelerin yapılacağı kişi sayısı değişkenlik göstermiştir. Görüşme yapılacak kişi sayısının artması çalışmanın geçerliliği ve güvenilirliğine pozitif yönde katkı sağlayacağından birden fazla görüş değerlendirilmiş, görüşmelere veri doygunluğu sağlayacak bulgular oluşana kadar devam edilmiştir.

Görüşmelerden elde edilen bulgular düzenledikten sonra tematik içerik analizi ile değerlendirilmiştir. "Tematik analiz, verilerdeki örüntüleri (temaları) belirleme, analiz etme ve raporlama için kullanılan bir yöntemdir. Tematik analiz, veri setini en küçük boyutlarda düzenlenmesini ve derinlemesine (zengin) betimlenmesini sağlamaktadır" (Braun ve Clarke, 2019, s. 875). Analiz işleminde bilgisayar destekli nitel veri analiz programı olan MAXQDA Analytics Pro (24.6.0 versiyonu) kullanılarak analiz ve görselleştirmeler gerçekleştirilmiştir.

I.5. Kaynaklar

Araştırma konusu ile ilgili kavramsal arka planın ve literatürün oluşturulabilmesi amacıyla, 2022 yılında başlayan ve çalışma sonuçlanana kadar devam eden süreçte bilgi merkezleri ve bibliyografik kaynaklar taranmıştır. Aynı zamanda yerli ve yabancı literatürde var olan kaynakların tespiti amacıyla basılı ve elektronik araştırma araçlarından taramalar yapılmıştır. "*Sensitive*", "*sensitivity review*", "*sensitive information*", "*sensitive data*", "*confidentiality*", "*information security*", "*appraisal*", "*redaction*", "hassas", "hassasiyet değerlendirmesi", "hassas bilgi", "gizlilik", "bilgi güvenliği", "değerlendirme", "redaksiyon", gibi anahtar kelimeler kullanılarak aşağıda belirtilen çevrimiçi kütüphane ve arşivlerin katalogları, veritabanları, e-kitaplar vb. kaynaklardan tarama yapılmıştır:

- İngiltere Ulusal Arşivi Web Sitesi
- Ankara Üniversitesi Kütüphanesi
- Bartın Üniversitesi Kütüphanesi
- Library, Information Science and Technology Abstact
- ScienceDirect
- Web of Science
- Scopus
- Taylor&Francis
- Google Scholar
- ProQuest Dissertations & Theses Global
- YÖKTEZ

Çalışmada İngiltere Ulusal Arşivi'nin yayınlamış olduğu rehber/kılavuz niteliğindeki kaynaklar temel başvuru kaynağı olarak kullanılmıştır. Bununla birlikte McDonald'ın 2019 yılında hazırlamış olduğu "*The FACTS of Technology-Assisted Sensitivity Review"*

başlıklı doktora tezi ve yazarın ilgili pek çok çalışması yol gösterici olmuştur. Temel kavramların kullanımında 2009 yılında T.C. Başbakanlık Devlet Arşivleri Genel Müdürlüğü tarafından yayınlanan "Belge Yönetimi ve Arşiv Terimleri Sözlüğü"; güncel bir kaynak olması bakımından 2023 yılında T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı tarafından yayınlanan "Arşiv Terimleri" sözlüğü; ve uluslararası terminolojik uyumun izlenebilmesi amacıyla 2005 yılında Amerikan Arşivistleri Derneği (Pearce-Moses hazırladığı) tarafından yayımlanan A Glossary of Archival and Records Terminology dikkate alınmıştır. Çalışmanın yazım sürecinde, biçimsel düzenlemeler Ankara Üniversitesi Sosyal Bilimler Enstitüsü'nün 2015 yılında yayımladığı Tez Yazım Yönergesi'ne; kaynakça ve metin içi alıntılar ise APA (American Psychological Association)'nın 2020 yılında yayımlanan 7. versiyonuna uygun olarak hazırlanmıştır.

I.6. Düzen

Tez, toplam altı bölümden oluşmaktadır. Birinci bölüm, tezin genel çerçevesini sunan giriş kısmıdır. Bu bölümde, araştırmanın amacı, önemi ve kapsamı ile ele alınan araştırma problemi, sorular ve hipotezler detaylı şekilde açıklanmıştır. Ayrıca çalışmada izlenen yöntem, kullanılan kaynaklar, terimlerin tanımları ve tezin genel düzenine ilişkin bilgiler de bu bölümde yer almaktadır.

İkinci bölüm, tezin temelini oluşturan kavramsal çerçevenin açıklanmasıyla başlamaktadır. Ardından, hassas bilgi kavramı ele alınarak, bu kavramın ulusal ve uluslararası mevzuattaki yeri detaylı bir şekilde incelenmiştir. Bu kapsamda, Türkiye'deki mevzuat düzenlemeleri ve hassas bilgilerin işlenmesine ilişkin hukukî çerçeve ile uygulamalara da yer verilmiştir. Bölümün devamında hassas bilgi türleri, odak konu doğrultusunda sınıflandırılmıştır.

Üçüncü bölüm, hassas bilgi içeren kamu belgelerinin incelenmesi ve değerlendirilmesine odaklanmaktadır. Bu süreçte karşılaşılan zorluklar ele alınmış;

geleneksel insan değerlendirme yöntemleri ile dijital teknolojilerin sunduğu araçlar karşılaştırılarak her iki yaklaşımın süreç üzerindeki etkileri değerlendirilmiştir.

Dördüncü bölüm, hassasiyet değerlendirme sürecine ilişkin ulusal arşivlerin faaliyetlerini ele almaktadır. Bu kapsamda, mevzuat, kılavuzlar, web siteleri ve kataloglardan örnekler sunulmuştur. Ayrıca, Türkiye'deki hassasiyet değerlendirmesiyle ilgili mevzuat ve ulusal arşivin çalışmaları değerlendirilmiştir.

Beşinci bölüm, konuya ilişkin bir uzman görüşü araştırmasını içermektedir. Uzmanlardan alınan görüşler, tematik bir analizle incelenmiş ve sunulmuştur.

Altıncı ve son bölümde, tezin tüm bölümleri değerlendirilerek elde edilen sonuçlar doğrultusunda önerilere yer verilmiştir. Ayrıca bu bölümde, araştırmada kullanılan kaynaklar, ilgili ekler ile Türkçe ve İngilizce özetler bulunmaktadır.

I.7. Terimler

Arşiv: "Tabi olunan mevzuat hükümlerine, mesleki ilke ve standartlara uygun biçimde sahip olduğu arşiv değeri taşıyan belgeleri koruma ve hizmete sunma sorumluluğunu yerine getiren türü ve görev kapsamına göre çeşitli ölçek ve türlerde oluşturulmuş bilgi-belge merkezi" (Arşiv Terimleri, 2023, s. 17).

Arşivci: "Arşiv belgelerinin belirlenmesi, tanımlanması, korunması, düzenlenmesi ve kullanıma sunulması işlemlerini ya da bu işlemlerden en az birini ilgili mevzuat ve standartlara uygun olarak yerine getirebilen, arşivcilik eğitimi almış kişi" (Arşiv Terimleri, 2023, s. 20).

Arşivcilik: "Arşivi; varlık nedeni, etki alanı, bileşenleri ve etkileşimde bulunduğu diğer tüm unsurları ile birlikte inceleyen bilim dalı" (Arşiv Terimleri, 2023, s. 20).

Arşiv Mevzuatı: "Bir ülkede arşivlerin korunması, erişilebilirliği ve güvenliği ile arşivlerin örgütlenmesini düzenleyen yasa ve normlar hiyerarşisinin tümünü kapsayan düzenlemeler" (Arşiv Terimleri, 2023, s. 19).

Belge: “Kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin resmî iş ve işlemleri neticesinde oluşan, kanıtsal ve hukukî değere sahip, üretim biçimleri ve donanım ortamları ne şekilde olursa olsun bir bilgiyi içeren yazılmış, çizilmiş, resmedilmiş, görüntülü, sesli veya elektronik kayıt” (Arşiv Terimleri, 2023, s. 26).

Belge Yönetimi: “Kurum ve kuruluşların faaliyetleri sonucu üretilen tüm belgeleri, üretim aşamasından itibaren ele alarak belirlenmiş ölçüt, kural ve standartlar çerçevesinde değerlendirmek, düzenlemek, ayıklamak ve istenildiğinde hizmete sunmak için gerçekleştirilen arşive devir öncesi gerçekleştirilen uygulama ve teoriler bütünü” (Arşiv Terimleri, 2023, s. 29).

Bilgi Edinme Hakkı: “Demokratik ve şeffaf yönetimin gereği olan eşitlik, tarafsızlık ve açıklık ilkelerine uygun olarak kişilerin bilgi isteklerinin karşılanması talebine ilişkin hak ve sorumluluklar” (Arşiv Terimleri, 2023, s. 31).

Değerlendirme: “Belgelerin durumunu güncel, idarî, yasal ve malî kullanımına, delil niteliğine veya bilgi değerine, düzen ve formuna, diğer belgelerle ilintisine dayanarak değerlendiren temel bir belge yönetimi/arşivleme işlemi” (Belge Yönetimi ve Arşiv Terimleri Sözlüğü, 2009, s. 14).

Elektronik Belge Yönetimi: “Herhangi bir kurum veya organizasyonun faaliyetleri sonucunda üretilen elektronik belgelerin, yaşam döngüsü olarak ifade edilen üretim, kullanım, dosyalama ve arşivleme evreleri boyunca sistematik olarak elektronik ortamlarda saklanması ve yönetimi” **(**Belge Yönetimi ve Arşiv Terimleri Sözlüğü, 2009, s. 20).

Gizlilik: “Belirli bilgi veya belgelere yüklenen ve böylece onlara erişimi sınırlayan veya özel hayata saygı gerektiren durum ya da hükümet tarafından devlet güvenliğinin korunması amacıyla belirli belgelere, içeriklerine ve kullanımına getirilen kısıtlama” (Belge Yönetimi ve Arşiv Terimleri Sözlüğü, 2009, s. 23).

Hassas: “Potansiyel olarak utanç verici olan, bireylerin gizli tutulmasını bekleyebileceği, kamu denetiminden korunması gereken yasal, malî veya kişisel nedenlerden dolayı gizlilik içeren bilgiler” (Pearce-Moses, 2005, s. 357).

Hassasiyet Değerlendirmesi: Kamu belgelerinin, kamuya veya bireylere yönelik itibar, mahremiyet ve güvenlik gibi potansiyel risklerini belirleme, analiz etme ve bu riskleri etkili bir şekilde değerlendirme sürecidir.

Kişisel Veri: “Kişilerin çeşitli alanlarda hizmet aldıkları kamu kurum ve kuruluşları ile yetkilendirilmiş özel kurumlarca mevzuat gereğince tutulan, depolanan, korunan ve zamanı geldiğinde yok edilen veriler” (Arşiv Terimleri, 2023, s. 85).

Mozaik Hassasiyet: Bilgi kırıntılarının bir araya getirilmesi veya birbiriyle doğrudan bağlantılı olmayan bilgi ve belgeler arasında kurulan ilişkiler sonucunda ortaya çıkan hassasiyet durumunu ifade etmektedir.

Redaksiyon: “Redaksiyon, bireyin mahremiyetini korumak, gizli bilgilerin tehlikeye atılmasını engellemek amacıyla belgedeki hassas bilgilerin, genel kullanıma veya görme yetkisi olmayan birine sunulmadan önce maskeleme veya kaldırma işlemidir” (Pearce-Moses, 2005, s. 336).

Sınırlama/Kısıtlama: “Arşiv belgelerinin/materyalinin tarihine, tasnif ve yıpranmışlık düzeyine, gizlilik özelliğine, kişisel veri içermesine göre veya araştırma talebi yoğunluğuna göre getirilen sınırlama” (Arşiv Terimleri, 2023, s. 122).

II. BÖLÜM: HASSAS BİLGİ MEVZUATI

II.1. Kavramsal Çerçeve

Kamu belgelerinin çeşitli niteliklerde bilgi taşıması, gizlilik ve hassasiyet oluşturan her bilgi türü için güvenlik düzeyinin farklı önlemler gerektirmesine ve uygulanacak mevzuat, standart ve politikaların seçimine etki etmektedir. Kurumların doğal faaliyeti sonucu üretilen belgelerin arşivsel değer (*archival value*) taşımaları durumunda yönetim ve erişim süreci arşiv döneminde [güncel dolaşımda olunmayan] devam etmektedir. Bu noktada arşivsel değeri olan hassas içerikli belgelerin değerlendirilmesi ve arşiv yönetiminin sağlanması ayrı bir sorundur. Arşivsel değer, belgenin "yönetsel, kanıtsal, mali, tarihi, entelektüel, kültürel, antik, kendine özgü (manevi), yasal ve parasal (maddi)" unsurlar gibi devam eden değerler taşımasıdır (Arşiv Terimleri, 2023, s. 21). Belgenin muhtemel arşivsel değeri, içerik (*content*) yönlü değerleme anlayışına göre yapılmaktadır. Bu bakımdan belge içeriğinin güvenlik ve gizlilik bakımından yönetimi, bu değer ölçütlerini taşıması durumunda arşiv belgesi vasfı kazandıktan sonra arşiv iş süreçleri doğrultusunda yürütülmeye devam etmektedir. Arşiv belgelerinin gizlilik hususu, içerikteki bilgilerin değerlendirilmesi yoluyla belirlenmektedir. Bu noktada bazı bilgi türlerinin diğerlerinden daha hassas/özel bir nitelik taşıması doğaldır (Etzioni, 2014, s. 1277).

Arşivlerde arşivsel değer ölçütlerini karşılayan hassas bilgi içeren belgeler muhafaza edilmektedir. Özellikle bireyler, kurumlar ve uluslararası ilişkileri içeren hassas belgelerin açıklanması durumunda ciddi sonuçlar doğabilmektedir. Bu tür içeriğine sahip belge veya belge gruplarının sınırlandırılması ya da kapatılması kapalı/kısıtlı arşiv (*dark archives*) kavramı ile nitelendirilmektedir. Kapalı arşivler, "arşivlerdeki belge gruplarının veya tek tek belgenin/materyalin genellikle hukukî ve idari sakıncalar ve tedbirler nedeniyle belirlenmiş bir süre için erişime kapalı veya sadece

yetkili kişilerce erişilebilir olması durumu" olarak tanımlanmaktadır[1] (Arşiv Terimleri, 2023, s. 81). Kapalı arşiv bakış açısı ile kısıtlama, belge içeriğindeki hassas bilgilerin mevzuatta yer alması ya da kurumun belirlemiş olduğu gerekçeler doğrultusunda uygulanmaktadır. "Arşivler olağanüstü durumlar hariç bu tür içeriğe sahip veya mevzuat gereğince gizlilik dereceli olanlar dışındakilerini tasnif ederek kullanıma açmak durumundadırlar" (Rukancı, Anameriç ve Başar, 2023, s. 27). Kapalı arşivlerde belgelerin gizlilik derecelerine/seviyelerine göre içeriğindeki gizli veya hassas bilgi unsurları doğrultusunda kapatılma veya sınırlama süreleri/koşulları oluşmaktadır. Gizlilik seviyesi "bilmesi gereken kişiler dışındakilere açıklanması veya verilmesi ulusal güvenlik veya kişisel güvenlik açısından sakıncalı görülen, içerdiği bilgi/veri nedeniyle gizli olması gerektiğine karar verilen belge/materyal, yayın, kayıt ortamı" olarak ifade edilmektedir (Arşiv Terimleri, 2023, s. 65). Hassas bilgi içeren belgelerin gizlilik dereceleri ve arşivsel yönetimi Türkiye'de "belge gizliliği" kapsamında uygulanmakta olup ayrı bir işlem olarak değerlendirilmemektedir. Gizlilik kapsamına giren arşivsel değeri olan hassas belgeler, pek çok ulusal arşiv tarafından ayrı bir husus olarak ele alınarak temel arşiv işlemlerinden "değerlendirme (*appraisal*)" sürecinin odak bir safhasıdır. Bu bakımdan hassas bilgileri tanımak, doğru bir şekilde sınıflandırmak ve arşiv yönetimi süreçlerinde ayrı bir yön ve titizlik gerektiren bir durum olarak değerlendirmek gerekmektedir.

Neyin hassas ve hassas olmadığının belirlenmesi, belgenin hassas bilgi içermesi durumunda hangi işlemlerin yapılacağına karar verilmesi, erişim kısıtlaması ve yetkilendirmesi süreçlerinin yürütülmesi, kurumlarda belge güvenliğinin sağlanması için gereklidir. Bu kapsamda kamu belgeleri esaslı olarak hassas bilgi kavramının doğru anlaşılması, bilgi edinme hakkı bağlamında erişim sürecinin aksatılmaması için elzemdir.

[1] Hassasiyet, telif hakkı ve teknik sorunlar genellikle kapalı arşiv nitelendirmesi için uygun gerekçeler olarak ifade edilmektedir (Jaillant, 2022a, s. 534).

Bir bilgi türünü hassas yapan nedir? sorusu kamudaki bilgi güvenliği ve gizliliğinin temin edilebilmesi cevaplanması gerekmektedir.

II.2. Hassas Bilgi Kavramı

Hassas (*sensitive*) terimi Türkçe'ye Arapça'dan geçmiş olup duyarlı olarak da ifade edilmektedir. Duyarlılık, sosyal veya vicdani bir durum karşısındaki hassasiyet ile birlikte gizlilik ve güvenliğe dayalı bir yaklaşımı ifade etmektedir. Hassas bilgi kavramının anlamı ve yorumlanması tartışma konusudur ve kavramın pratikte uygulanması zordur. Bu sebeple hassas bilgi olgusunun kavramsallaştırmaları çeşitlidir ve çoğu araştırma alanı bu olguları tamamen tanımlayan veya açıklayan bir kavramsallaştırma içermez (Thompson ve Kaarst-Brown, 2005, s. 255). Tüm özel yaklaşımların bir sentezinin yapılmasına ve ilgili konu uzmanlığı ile birleştirilmesine ihtiyaç vardır. Hassas bilgiler genellikle kamu kurumları, özel veya tüzel kişiler ile ilgili çeşitli bilgi niteliğine sahip olan, çoğunlukla kişisel bilgilerden oluşan ve erişilmesi durumunda risk oluşturan bilgilerdir. Kamu kurumlarının görevleri dolayısıyla da ürettikleri belgelere göre hassasiyet sıfatı değişebilir. Her kurumun farklı hassas bilgi ve belgeleri olabilir. Bu sebeple hassas bilgiler genellikle özel bir nitelik taşır ve her kurumun belirlediği çerçevede, sınırlı bir erişime tabi tutulabilir veya belirli bir süreyle erişime kapatılabilir.

İlk bakışta "gizli bilgi" kavramı ile "hassas bilgi" kavramı büyük ölçüde benzer veya aynı koşulu karşılayan durumlar için düşünülebilir. Fakat gizli olarak nitelendirilen her bilgi ayrımcılık, utanç, itibar zedelenmesi veya risk oluşturmaz. Terim olarak "gizlilik", hukuk alanına mahsus bir kavram olduğundan "gizli olma durumu" olarak karşılık bulmaktadır. Ceza muhakemesi ve ceza hukuku bağlamında "gizlilik", yürütülen işlemlere yalnızca ilgililerin katılabilmesi veya soruşturma sürecinde elde edilen bilgilerin kamuya açık hale getirilmemesi şeklinde açıklanmaktadır (Parlar ve Hatipoğlu 2008, s. 3975; Centel ve Zafer, 2011, s. 94; Çakır, 2012, s. 230). Bu bakımdan kamu

belgelerindeki gizliliğin hukukî statüsü, arşivcilikteki gizlilik kavramından farklı bir şekilde ele alınır. Arşivcilik bağlamında gizlilik, belgelerin belirli bir süre boyunca erişime kapalı tutulması ve yalnızca yetkili kişilerin erişebilmesiyle ilgilidir. Hukuk bağlamında ise gizlilik, yargısal süreçlerin adil şekilde yürütülmesi, kişisel hakların korunması ve soruşturma süreçlerinde delillerin güvence altına alınması amacına hizmet eder. Bu nedenle, hukukî gizlilik, kamu yararı ve adaletin sağlanması açısından zorunlu bir prensip olarak değerlendirilirken, arşivcilikte gizlilik daha çok belgenin niteliğine ve saklama süresine bağlı olarak değişen bir uygulamadır. Hassas olarak tanımlanan bilgiler belirtilen olumsuzluklar ile birlikte gizlilik kaygısı taşıyan odak bir kavram olarak ifade edilebilir. Bununla birlikte gizli bilgiler ilgili kişiden veya üçüncü bir taraftan açık veya gizlilik esasına göre elde edilen bilgiler olduğundan hassas olabilir veya olmayabilir. Her iki kavram arasında önemli benzerlikler bulunsa da gizli olan bilgiler, hassas olanlardan önemli ölçüde farklı erişim yönetimi gerektirebilir (Sillitoe, 1988, s. 9). Gizlilik çatı bir kavram olarak kabul edilirken hassasiyet potansiyel risk unsurlarına dayanmaktadır.

Hassas bilgiler, doğası gereği bir başkası tarafından bilinme kaygısıyla utanç verici (küçük düşürücü veya aşağılayıcı) değerlendirme eğilimindeki bilgilerdir. Hassas bilgiler söz konusu olduğunda kişisel veriler ile büyük ölçüde bağlantı kurulup açıklanması halinde kişisel verilere göre daha büyük zararlara yol açabilme ihtimali bulunan koruma önceliği olan hukukî varlıklar düşünülmektedir (Bulut, 2020, s. 124). Bu nedenle, hassas bilgiler yakında tutulma, gizli tutulma veya yalnızca güvenilir sırdaşlara aktarılma eğilimindedir (Ohm, 2014, s. 1171). Bir kişiye, gruba veya kuruma zarar, hasar, utanç ya da itibar kaybına neden olabilecek bilgilerin izinsiz ifşası, erişimi veya kullanımı hassas kabul edilir.

Hassas bilgi kavramı pek çok farklı şekilde tanımlanmıştır. Hassas bilgiler, yanlış ellerde olması durumunda gizliliği ve güvenliği zarara uğratabilecek bilgiler olarak tanımlanmaktadır (Ohm, 2014, s. 1133). Diğer bir tanıma göre kaybolması, tehlikeye

atılması veya izinsiz ifşa edilmesi durumunda, bireylere zarar, utanç, rahatsızlık veya adaletsizlikle sonuçlanabilecek nitelikteki bilgiler hassas olarak kabul edilmektedir (Transportation Security Administration, 2008, s. 1). Bir diğer tanıma göre kayıp, kötüye kullanım, yetkisiz erişim, değişiklik durumlarında ulusal çıkarları olumsuz yönde etkileyebilecek, federal programların yürütülmesini engelleyecek, bireylerin mahremiyetini ihlal edecek bilgiler hassas olarak kabul edilmektedir (Johnson ve diğerleri, 2016, s. 30).

Hassas bilgilerin, maddi veya manevi zararlara yol açabilecek olması, genellikle hassas bilgi tanımlamaları içerisinde öne çıkmaktadır. Bilgi, sahibine ya da ilgili kişilere zarar vermek için kullanılabiliyorsa hassas kabul edilir (Ohm, 2014, s. 1162). Bu bağlamda oluşması muhtemel risk, bilginin kontrolünün kaybedilmesinden kaynaklanmaktadır. Hassas olan bilgi kontrolünün kaybedilmesi, kaybedilme durumunda risk meydana gelmesi hassasiyet oluşumu için temel bir noktadır. Bu durum esasında hassasiyet için belirleyici bir kriter olmasının yanı sıra çok geniş bir hassasiyet anlayışının da oluşabilmesine sebep olmaktadır. Dolayısıyla hassasiyet tespitinde her zaman merkezî bir kesinlik çekirdeği ve onu çevreleyen gri bir alan olacaktır (Sillitoe, 1988, s. 9).

Hassas olarak kabul edilen kategorilerin listesi bir ülkeden diğerine (Henttonen, 2017, s. 286), toplumsal yapı, kültür, inanç (Şişman, 2019, s. 15) ve ahlak anlayışına göre değişkenlik gösterebilmektedir. Verilerin kullanılma amacı ve bağlamı da hassasiyete etki etmektedir. Herhangi bir kişisel veri, işleme amacına veya bağlamına bağlı olarak hassasiyet oluşturabilir (Simitis, 1999, s. 5). Amaç ve bağlam temelli yaklaşımlar/ifadeler düzenlemelerin dilbilimsel özelliklerine yansımıştır. Bu sebeple pek çok ülkede hassasiyet kavramının yerine geçen farklı kavramsal ifadelerin, ifade biçimlerinin ve anlayışlarının tercih edildiği görülmektedir. Hukukî düzenlemelerde "hassas veri" ve "hassas bilgi" terimleri sıklıkla birbirlerinin yerine kullanılmaktadır. Ayrıca benzer bir şekilde "kişisel veri" ya da "kişisel bilgi" kavramları da hukukî düzenlemeler ve bilgi

güvenliğine ilişkin literatürde aynı anlamı işaret ederek birbiri yerine kullanılmaktadır (Henkoğlu, 2015, s. 18). Veri bağlamında düşünüldüğünde hassas veriler (kimlik bilgileri, sosyal güvenlik numaraları vs.) daha çok yapılandırılmış veri formatında bulunan ilişkilendirilmeye ve anlamlandırılmaya gereksinim duyulan verilerdir. Bunun yanı sıra hassas bilgi kavramı (Örneğin kimlik bilgisi ile birlikte hastalık teşhisinin bir arada bulunması) doğrudan kişi veya kurumlar ile ilgili ilişkilendirilmiş ya da yaygın olarak kabul edilen hassasiyetleri ifade etmektedir. Literatürde ve hukukî düzenlemelerde hassas veri *(sensitive data*), hassas bilgi (*sensitive information*), özel veri (*private/special data*), özel kategorideki kişisel veri (*special categories of personal data*) veya özel kişisel veri (*private personal data*) kavramları farklılık olarak kullanılsa da çalışmada, veri-bilgi ilişkisine değinilmeden çatı bir kavram olarak "hassas bilgi" ifadesi tercih edilmektedir. Bununla birlikte "hassas veri" kavramı ifade edilen bağlam esasınca yer yer kullanılmaktadır.

II.3. Mevzuat Düzenlemelerinde Hassas Bilgi

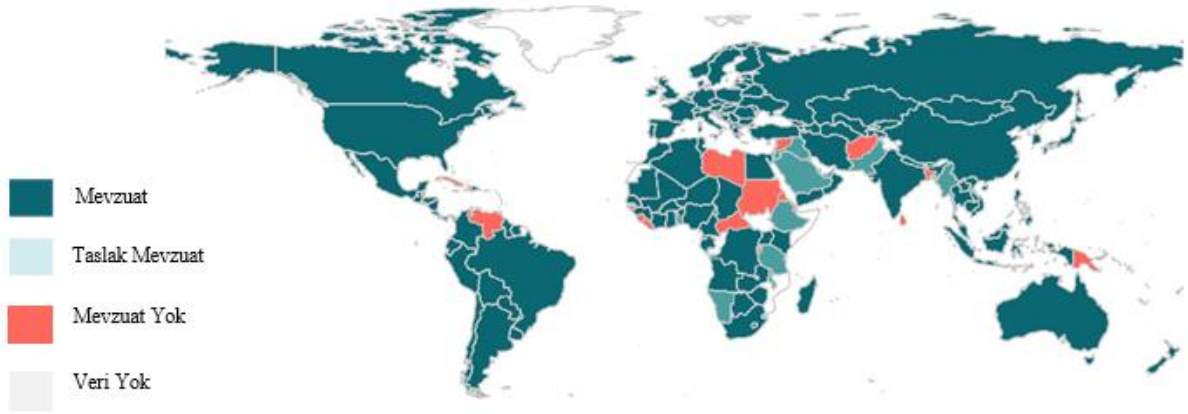
Bilginin hassasiyeti, sadece maddi veya manevi zarar açığa çıkarma olasılığından dolayı kabul edilmeyebilir. Bir yasama organı – veya başka bir kural koyucu kurum – zarar olasılığının yeterince yüksek olduğuna karar verir ve bu durum mevzuat içerisinde yer alırsa meşru bir uygulama zemini kazanır (Ohm, 2014, s. 1168). Mevzuat; kamu ve kişi haklarının korunmasında şeffaflık ve gizlilik dengesi gözetilerek hassas bilgilerin tanımlandığı, işlenme koşullarının düzenlendiği hukukî metinlerdir. Kamunun bilgiye erişim hakkının sağlanması ile tehdit oluşturabilecek veya bireysel mahremiyeti ihlal edebilecek verilerin korunması arasında hassas bir denge kurmak süregelen bir kaygı olmaya devam etmektedir. Hassas bilgiler, savunmasız doğası sebebiyle yasalarca daha yüksek düzeyde korunmaktadır. Dünyanın dört bir yanındaki kanun yapıcılar, özellikle vatandaşlara ait bazı kişisel verilerin diğerleri göre daha özel bir nitelikte olduğuna işaret

ederek bu bilgileri toplama, kullanma ve güvenli bir şekilde saklama konularını düzenlemeler ile korumaktadır. Veri koruma/gizlilik yasalarında hassas bilgi kavramı çeşitli ifadeler ile tanımlamış, belirli veri türlerinin işlenmesinin diğerlerine göre daha sıkı kontrollere tabi tutulması gerektiği ifade edilmiştir (Al-Fedaghi, 2007, s. 165). Hassas bilgi sınıflamaları/kategorileri bir doktrin olarak varlık gösterirken mevzuat, hassas bilgileri belirleme ve işleme süreçlerinin yasal olarak nasıl uygulanacağını belirler ve vatandaşlara bu veriler üzerinde daha fazla hak tanır. Bu tür bilgilerin açığa çıkarılması, özellikle vatandaşlar için bireysel haklar ve mülkiyet güvenliği açısından büyük bir risk oluşturabilir, kurumsal itibara zarar verebilir. Bu nedenle, genel bilgilere kıyasla farklı ele alınmalı ve mevzuatta daha güçlü koruma altına alınmalıdır. Hassas bilgi sınıflamaları, yaygın olarak bazı konular ekseninde mevzuat düzenlemelerinde ortak bir kabul ile yer alırken ilgili ülkenin hukukî ve sosyolojik bağlamı belirleyicidir. Örneğin sendika üyeliğine ilişkin bilgilerin ifşası bazı ülkelerdeki mevzuatta ayrımcılığı ortaya çıkaran mahremiyet riski olarak değerlendirilirken, bazılarında yalnızca siyasî-dinî görüş veya ulusal güvenlik faaliyetleriyle yakından bağlantılı olduğu sürece hassas kabul edilir. Hangi gizlilik veya koruma yasasına tabi olunduğuna bağlı olarak bilginin hassasiyetindeki algı ve anlayış toplumsal normların süzgecinden geçerek normatif hukuk düzenine yansımaktadır. Veri koruma kanunu bulunan tüm ülkeler ve uluslarüstü kuruluşlar bazı verilerin diğerlerine göre daha hassas olduğunu kabul ederek bu konuda düzenlemeler yapmışlardır.

II.3.1. Ulusal ve Uluslarüstü Mevzuat Düzenlemelerinde Hassas Bilgi

Ulusal ve uluslarüstü mevzuat düzenlemelerinde, hassas bilgilerin ele alınması ve korunması, yasal sistemlerin bütünlüğünün ve güvenliğinin korunmasında önemli bir dayanak noktasıdır. Ulusal hükümetler ve uluslarüstü kuruluşlar tarafından hassas bilgilerin ele alınmasında benimsenen yaklaşımlar, kültürel ve sosyal normlara göre

hukukî metinlere yansımaktadır. Hassas bilgilerle ilgili olarak özel düzenlemeler ve gelişmiş koruma sağlayan yasa ve düzenlemeler mevcuttur. Bu düzenlemelerin oluşturulmasındaki tetikleyici gerekçe, kişisel olarak tanımlanabilir bilgilerin varlığıdır. Kişisel bilgilerin ihlal edilme riski büyük ölçüde endişe edilen bir husustur. Bu sebeple hassas bilgi kavramı, bu düzenlemelerde çoğunlukla kişisel bilgilerin bir alt kümesi veya doğrudan kişisel bilgiler olarak yer almıştır. Dünyanın dört bir yanındaki öne çıkan veri gizliliği/koruma yasalarında (Görsel 1) benzer konular işlense bile hassas veri konusunda ortak bir anlayış bulunmamaktadır. Hassas veri kavramı, OECD Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Kılavuz İlkeleri'nde ele alınarak ilk defa uluslararası hukuka dahil edilmiştir (McCullagh, 2007, s. 190). Bu kılavuz ilkelerine göre (2002, s. 28, 40), "evrensel olarak hassas kabul edilen bir dizi verinin tanımlanması mümkün olmadığından" her üye ülkedeki geleneklere ve tutumlara göre hassas verilerin/bilgilerin ayrılması gerektiği ifade edilerek bu konuda bağlamsal bir yaklaşım benimsemektedir. Bu bağlamda etki alanı geniş gizlilik/koruma düzenlemelerinin incelenmesi gerekir.



Görsel 1. Veri Koruma ve Gizlilik Yasaları (Birleşmiş Milletler, 2024a)

Çin Halk Cumhuriyeti Kişisel Bilgileri Koruma Yasası'nda (Personal Information Protection Law/PIPL**),** biyometrik özellikler, dinî inançlar, özel olarak belirlenmiş statü, tıbbî sağlık, malî hesap bilgileri hassas kişisel bilgi olarak yer almaktadır. Ayrıca bireysel konum takibi ve 14 yaşından küçüklerin kişisel bilgileri aynı kapsamda ifade edilmektedir (Personal Information Protection..., 2021, 28).

Rusya Federasyonu, hassas kişisel verileri, özel nitelikli kişisel veriler olarak tanımlanmaktadır. Rusya Kişisel Veriler Kanunu'nda (Law on Personal Data/LPD) ırk veya etnik köken, siyasî görüşler, dinî ve felsefî inançlar, sağlık durumu, mahremiyetle ilgili verileri özel nitelikli kişisel veri kapsamındadır. Listeye dahil edilmemiş olsa da, sabıka kayıtları ve biyometrik verilerin işlenmesi için özel kurallar vardır, bu sebeple bu veriler de hassas olarak değerlendirilebilir (Russian Federation Federal…, 2021, 10/1).

Amerika Birleşik Devletleri'nde (ABD) veri korumaya yönelik tek bir temel mevzuat yoktur. Federal ve eyalet düzeyinde pek çok yasa bulunmaktadır. Gizlilik yasaları konusunda köklü bir geçmişi olan California Gizlilik Hakları Yasası (California Privacy Rights Act/CPRA), hassas kişisel bilgileri; bir tüketicinin sosyal güvenlik, ehliyet, devlet kimlik kartı veya pasaport numarası, hesap oturum açma, finansal hesap, banka kartı veya kredi kartı numarası ile birlikte bir hesaba erişim sağlayan güvenlik veya erişim kodu, şifre veya kimlik bilgileri, kesin coğrafî konumu, ırksal veya etnik kökeni, dinî veya felsefî inançları, sendika üyeliği, alışveriş, e-posta ve metin mesajlarının içeriği, genetik verileri, biyometrik bilgileri, bireyin sağlığı ile ilgili olarak toplanan ve analiz edilen kişisel bilgileri, cinsel yaşamı veya cinsel yönelimi gibi farklı türde çok sayıda veriyi hassas olarak kabul etmiştir (Califonia Privacy…, 2020, 1798,140/L). Virginia Tüketici Verilerini Koruma Yasası'nda (Virginia Consumer Data Protection Act/CDPA), bir kişinin ırksal veya etnik kökeni, dinî inançları, zihinsel veya fiziksel sağlık teşhisi, cinsel yönelimi, vatandaşlık veya göçmenlik durumu, genetik veya biyometrik verileri söz konusu kişiyi benzersiz bir şekilde tanımlamak amacıyla işlenmesi, 13 yaşından

küçük çocuktan toplanan kişisel veriler, kesin coğrafî konum verileri hassas veri olarak nitelendirilmektedir (Virginia Consumer…, 2023). Colorado Gizlilik Yasası'na (Colorado Privacy Act /CPA) göre hassas veri; ırk veya etnik köken, dinî inançlar, zihinsel veya fiziksel bir sağlık durumu ya da teşhisi, cinsel yaşam veya cinsel yönelim, vatandaşlık veya vatandaşlık statüsünü ortaya koyan kişisel veriler, bir bireyin kimliğinin eşsiz olarak belirlenmesi amacıyla işlenebilecek genetik veya biyometrik veriler, bilinen bir çocuğa ait kişisel verilerden oluşmaktadır (Colorado Privacy Act, 2023). Connecticut Veri Gizliliği Yasası'nda (Connecticut Data Privacy Act/CTDPA) hassas veriler kişisel verilerin bir alt kümesi olarak tanımlanmış; ırksal veya etnik köken, dinî inanç, zihinsel veya fiziksel sağlık koşulları veya teşhisleri, cinsel faaliyet veya yönelim, vatandaşlık veya göçmenlik durumunu ortaya koyan her türlü veri, bir bireyi benzersiz bir şekilde tanımlamak için kullanılan genetik veya biyometrik veriler, 13 yaşın altındaki bir çocuğun kişisel verileri ve bir bireyin kesin coğrafî konum verileri bu kapsamda sıralanmıştır (Connecticut Data Privacy Act, 2023).

Meksika Kişisel Verilerin Korunmasına İlişkin Federal Kanun, hassas kişisel verileri; veri sahibinin hayatının en özel alanlarına değinen veya kötüye kullanımı ayrımcılığa yol açabilecek ya da söz konusu veri sahibi için ciddi bir risk içeren kişisel veriler olarak tanımlamaktadır. Özellikle ırksal veya etnik köken, mevcut ve gelecekteki sağlık durumu, genetik bilgiler, dinî, felsefî ve ahlakî inançlar, sendika üyeliği, siyasî görüş, cinsel tercih gibi unsurları ortaya çıkarabilecek veriler hassas veri olarak kabul edilmektedir (Mexico Federal Law, 2010, 3/6).

Arjantin Kişisel Verin Korunması Kanunu'nda (Proteccıon De Los Datos Personales/PDP) hassas veriler; ırk ve etnik köken, siyasî görüşler, dinî, felsefî veya ahlakî kanaatler, sendika üyeliği, sağlık veya cinsel yaşamla ilgili bilgileri ortaya koyan kişisel veriler olarak tanımlanmaktadır (Proteccıon De Los Datos Personales, 2000).

Brezilya Genel Kişisel Verilerin Korunması Kanunu'nda hassas kişisel verileri, (Lei Geral de Proteção de Dados Pessoais /LGPD), bir gerçek kişiyle bağlantılı olduğunda, ırk veya etnik köken, dinî inanç, siyasî görüş, sendika üyeliği, dinî, felsefî veya siyasî örgüt üyeliği, sağlık verileri, cinsel yaşamla ilgili veriler, genetik ve biyometrik veriler olarak listelemektedir (Presidência da República…, 2018, 5/2).

Avustralya Gizlilik Yasası'na (Australia Privacy Act/APA) göre hassas bilgiler kişisel bilgilerin bir alt kümesidir ve bir bireyin ırk veya etnik kökeni, siyasî görüşleri veya bir siyasî derneğe üyeliği, dinî inançları ve bağlılıkları, felsefî inançları, bir meslek, ticaret birliği veya sendikaya üyelik, cinsel yönelim, sabıka kaydı, sağlık bilgileri, genetik bilgiler, otomatik biyometrik doğrulama veya biyometrik tanımlama amacıyla kullanılacak biyometrik bilgiler/şablonlar olarak sayılmıştır (Australia Privacy Act, 1988, Bölüm-2/1).

Kanada Kişisel Bilgilerin Korunması ve Elektronik Belgeler Kanunu'na (Personal Information Protection and Electronic Documents Act/PIPEDA) göre kişisel bilgiler, çoğunlukla hassas olmak ile birlikte hassas kişisel bilgilerin net bir listesi belirtilmemiştir. Yasaya göre bazı bilgiler (örneğin tıbbî kayıtlar ve gelir kayıtları) neredeyse her zaman hassas olarak kabul edilir. Ancak bağlama bağlı olarak herhangi bir bilginin hassas olabileceği özellikle belirtilmektedir. Örneğin, haber dergisi abonelerinin isimleri ve adresleri genellikle hassas olarak değerlendirilmez. Ancak, bazı özel ilgi alanlarına yönelik dergilere abone olanların isim ve adreslerinin hassas olarak değerlendirilebileceği ifade edilmektedir (Personal Information Protection…, 2000).

Birleşik Krallık veri koruma konusunda diğer AB[2] ülkelerinde olduğu gibi çatı bir düzenleme olan Genel Veri Koruma Tüzüğü'ne (GVKT) bağlı olmasının yanı sıra Bilgi Edinme Hakkı Yasası'nda hassasiyeti "Ulusal Güvenlik" "Uluslararası İlişkilere Zarar",

[2] Birleşik Krallık AB üye ülkeleri arasından 31 Ocak 2020 tarihinde ayrılmıştır (Brexit). Ancak hala AB hukukuna tabidir.

"Kişisel Bilgiler" ile "Ticarî Bilgiler" arasında değişen yaklaşık yirmi beş muafiyete (*exemption*) ayırarak belirli temalara göre tanımlamaya çalışmaktadır (Moss ve Gollins, 2017, s. 14; McDonald, 2019, s. 2). GVKT'ye bağlı İtalya, 2003 tarihli Kişisel Verileri Koruma Kodu AB ülkeleri arasında hassas kişisel bilgilerin en ayrıntılı örneklerinin sunulduğu yasal düzenlemedir. Düzenlemeye göre hassas veriler; ırk, etnik köken, dinî, felsefî veya diğer inançlar, siyasî görüşler, parti, sendika, dernek ya da dinî, felsefî, siyasî veya sendikal nitelikteki kuruluşlara üyelik ile sağlık ve cinsel hayatı ifşa eden kişisel verilerdir. Tüm mevzuatta hassas kabul edilen ancak genel olarak soyut bir şekilde ele alınan din ve bu bilgiyi ortaya çıkarabilecek her türlü veri mevzuat kapsamına girmemektedir. Ancak İtalyan Veri Koruma Yasası bir veri sahibinin dinini ortaya çıkarabilecek kişisel bilgi öğelerini listeler ve bu öğeleri hassas olarak kabul eder. Örneğin dinî bayramlarda izin veya kantin hizmetlerinden yararlanmaya ilişkin her türlü bilgi mevzuatta yer alan maddelerden bazılarıdır. Aynı zamanda siyasî görüşler, sendika üyelikleri ve diğer ülke kanunlarından farklı olarak yargılamaya ait veriler hassas olarak düzenlenmiştir (Italian Personal Data…, 2003; Kaya, 2011, s. 320; Belen-Sağlam, Nurse ve Hodges, 2022b, s. 8).

1981 yılında Avrupa Konseyi tarafından çıkarılan, Türkiye'nin[3] de imzacı olduğu 108 sayılı "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karsısında Şahısların Korunmasına Dair Sözleşme" kişisel verilerin korunması konusundaki bağlayıcı olan ilk belgedir (Kılınç, 2012, s. 1114). Pek çok hukukî düzenlemeye ilham olan bu sözleşmenin 6. maddesinde hassas bilgiler özel veri kategorileri olarak nitelendirilmiştir. Anılan maddeye göre ırksal kökeni, siyasî görüşleri, dinî ya da diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayata ilişkin kişisel veriler, iç hukukta uygun güvenceler sağlanmadıkça otomatik olarak işlenemez (Council of European, 1981, 6).

[3] 17 Mart 2016 tarihli ve 29656 sayılı Resmî Gazete'de yayımlanarak yürürlük kazanmıştır

1995 yılında Avrupa Parlementosu (AP) ve Konseyi tarafından 95/46 sayılı[4] "Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiğine İlişkin Direktif" hassas verileri; ırk veya etnik köken, siyasî görüşler, dinî veya felsefî inançlar, sendika üyeliği, sağlık veya cinsel yaşam, suçlar, ceza mahkumiyet ve güvenlik tedbirleri ile ilgili verilerin işlenmesini ortaya koyan kişisel verileri, özel kategoride nitelendirerek işlenmesini yasaklamıştır (European Parliament…, 1995, 8/1, 8/5).

2018 yılında yürürlük kazanan Avrupa'da veri koruma konusunda kapsayıcı bir çerçeve oluşturan son düzenleme, üye ülkeleri bağlayan Genel Veri Koruma Tüzüğü (General Data Protection Regulation/GDPR), hassas kişisel verileri işleme, denetleme, koruma ve hukukî süreçleri içermesi bakımından çoğu yasal düzenlemeye rehberlik etmektedir. Tüzükte hassas veriler özel kategorideki kişisel veriler olarak ifade edilmiştir. Doğası gereği, temel hak ve özgürlüklerle ilgili olarak özellikle hassas olan kişisel veriler, işlenmeleri bağlamında temel hak ve özgürlükler açısından önemli riskler yaratabileceğinden, özel korumayı hak etmektedir Bu kapsamda ırk veya etnik köken, siyasî görüş, dinî veya felsefî inanç, sendika üyeliğini ortaya koyan kişisel verilerin işlenmesi, genetik verilerin, bir gerçek kişiyi benzersiz bir şekilde tanımlamak amacıyla biyometrik verilerin, sağlıkla ilgili verilerin veya bir gerçek kişinin cinsel yaşamı ya da cinsel yönelimi ile ilgili verilerin işlenmesi yasaklanmıştır (European Parliament, 2016, 51, 56, 4/13, 4/14, 9/1). AB ülkelerinin ve diğer[5] ülkelerin kendi veri koruma yasaları bulunmasına karşın çoğu konuda bu tüzüğe atıfta bulunulmaktadır. Örneğin üye ülke olmayan İzlanda, GVKT'den uyarlamalar ile kendi Kişisel Verilerin Korunması ve İşlenmesi Hakkında Kanunu'nu (Act on Data Protection and the Processing of Personal Data/ADPPPD) oluşturmuştur. Bu düzenlemede, kişisel hassas veriler; ırk veya etnik

[4] 25 Mayıs 2018 tarihi itibarıyla Avrupa Birliği Genel Veri Koruma Tüzüğü hükümleri geçerli olmuştur.
[5] Örneğin AB üyesi ülke olmamasına rağmen Norveç, GVKT'yı kişisel verilerin korunması konusunda kendi yasalarına dahil etmektedir.

köken, siyasî görüş, dinî veya felsefî inanç, sendika üyeliği, sağlık verileri (fiziksel veya zihinsel sağlık), cinsel yaşam veya yönelim, genetik ve biyometrik veriler olarak kabul edilmektedir (Act on Data Protection…, 2018). Üye ülke olmayan ve GVKT'ye uyumu gözeten bir diğer ülke İsviçre'dir. İsviçre Federal Veri Koruma Kanunu (Federal Act on Data Protection/FADP), hassas kişisel bilgileri; dinî, ideolojik, siyasî veya sendika ile ilgili görüşler/faaliyetler, sağlık verileri, mahrem alan, ırksal köken, sosyal güvenlik önlemleri, idarî veya cezaî kovuşturma ve yaptırımlar olarak ele almaktadır. GVKT ile uyum kapsamında bu listeye genetik ve biyometrik veriler de eklenmiştir (Federal Act on Data Protection, 2023).

NATO (North Atlantic Treaty Organization / Kuzey Atlantik Antlaşması Örgütü) Kişisel Bilgilerin ve Gizliliğin Korunması Kanunu'nda hassas kişisel bilgiler ve özel kategorideki kişisel bilgiler olmak üzere iki kavramsal farklılık bulunmaktadır. Düzenlemeye göre hassas kişisel bilgiler, bir kişinin iş yerindeki performansı, disiplini, fiziksel veya ruhsal sağlığı, malî işleri veya özel hayatı hakkında açıklanmasının kişiyi fiziksel olarak tehlikeye atması, kariyerine veya itibarına zarar vermesi makul olarak beklenebilecek her türlü gerçek/görüş olarak ifade edilmiştir. Bu direktifin amaçları doğrultusunda, kişisel bilgiler veya kişisel veriler, gerçek bir kişinin kimliğini ayırt etmek veya izlemek için kullanılabilecek her türlü bilgiyi hassas olarak nitelendirmiştir. Bununla birlikte özel kategorideki kişisel bilgiler; ırk veya etnik köken, cinsel yönelim, siyasî, felsefî, dinî görüşler veya faaliyetlerle ilgili kişisel bilgilerin yanı sıra genetik, biyometrik veriler ve sağlıkla ilgili bilgiler olarak tanımlanmıştır (NATO Act Personal Information…, 2022, 1/3, 5/5). İki ayrı tanım olarak ifade edilen kavramlar arasında bazı farklılık olmasına rağmen aynı kapsamda değerlendirilebilir. Her iki kavramın odağında kişilere yönelik hassasiyetler bulunmaktadır.

Birleşmiş Milletler (BM) tarafından yayınlanan "Veri Gizliliği, Etiği ve Korunması" başlıklı kılavuzda hassas veriler; ırk veya etnik köken, siyasî görüşler,

sendikal örgütlenme, dinî inançlar veya benzer nitelikteki diğer inançlar, fiziksel/zihinsel sağlık veya durum (veya herhangi bir genetik veri) ile ilgili veriler, cinsel yönelim ve diğer ilgili faaliyetler, herhangi bir suçun işlenmesi veya işlendiği iddiası, adlî işlemlere ilişkin her türlü bilgi, her türlü malî veri, çocuklar ve herhangi bir zarar riskiyle karşı karşıya olan birey(ler) veya birey(ler) grubu (Örneğin fiziksel, duygusal, ekonomik) olarak tanımlanmıştır[6] (Birleşmiş Milletler Geliştirme Grubu, 2017, s. 11). Kılavuzda ayrıca hassas olmayan verileri kullanılan bağlam (örneğin kültürel, coğrafî, dinî, siyasî koşullar vb.) esasınca hassas verilere dönüştürebileceği, açıkça kişisel veya hassas olmasa bile veri analizinin bir birey veya bireyler grubu üzerinde etkili olabileceği ifade edilmektedir (Birleşmiş Milletler Geliştirme Grubu, 2017, s. 5).

II.3.2. Türkiye'deki Mevzuat Düzenlemelerinde Hassas Bilgi

Türkiye'de kişisel verilerin korunması meselesi, normlar hiyerarşisinin en üst noktasında bulunan anayasaya "özel hayatın gizliliği" başlığıyla 2010 yılında yapılan 5982 sayılı "Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun" ile bir hak olarak girmiştir. Yapılan düzenlemeyle Anayasa'nın 20. maddesine göre;

> Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler,

[6] BM tarafından kabul edilen hassasiyetler, diğer düzenlemelerde olduğu gibi belirli konular eksenin örtüşmektedir. Ancak ifade edilenin dışında BM "Bilgi Hassasiyeti, Sınıflandırma ve İşleme" başlıklı bültende bazı belgelerin hassasiyetine ilişkin durumları sıralamaktadır. 1-Gizlilik beklentisi olan, üçüncü taraflardan alınan veya gönderilen belgeler, 2-Açıklanması herhangi bir bireyin güvenliğini, hakkını ve mahremiyetini ihlal eden belgeler, 3-Açıklanması üye devletlerin güvenliğini tehlikeye atması ve BM'nin herhangi bir operasyonunun veya güvenliğine zarar verecek belgeler, 4-Yasal ayrıcalık kapsamındaki iç soruşturma belgeleri, 5-Açıklanması BM'nin mali çıkarlarına zarar verecek ticarî belgeler, 6-Oluşturulma ve iletilme koşulları sebebiyle gizli kabul edilmesi gereken diğer bilgileri hassas olarak sınıflandırılmaktadır (Birleşmiş Milletler Genel Sekreterlik Bülteni, 2007/6, 1/2).

ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir (T.C. Anayasası, 1982).

Benzer bir şekilde Türk Medeni Kanunu'nun (2001) 24. maddesi[7] ile Türk Borçlar Kanunu'nun 49. maddesi[8] özel yaşama dair kişi haklarının korunmasına genel bir dayanak oluşturmuştur. Anayasanın 20. maddesinde belirtilen kanunî düzenleme, hem kişisel verilerin korunması hem de hassas verilerin ele alınması bakımından münhasır bir niteliği olan Kişisel Verilerin Korunması Kanunu'dur.[9]

Türk mevzuat düzenlemelerinde hassas bilgi kavramı, "özel nitelikli kişisel veri (*sensitive personal data*)" olarak ifade edilerek, kişisel bilgi odaklı hassasiyetleri kapsamaktadır. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) 6. maddesinin 1. fıkrasında "kişilerin ırkı, etnik kökeni, siyasî düşüncesi, felsefî inancı, dinî, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı[10], cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri[11] özel nitelikli kişisel veridir*"* ifadesiyle tanımlanmıştır. Bu maddeye ilişkin gerekçe "sayılan kişisel verilerin, başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden

[7] Madde-24 "hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir. Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır."

[8] Madde-49 "Kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür."

[9] KVKK öncesi özel nitelikli kişiler verilerin korunmasına dayanak oluşturacak anayasanın Madde-2 "Hukuk Devleti" ilkesi, Madde-12 "Temel Hak ve Hürriyetlerin Niteliği", Madde-17 "Kişi Dokunulmazlığı, Kişinin Maddi ve Manevi Varlığını Koruma ve Geliştirme Hakkı", Madde-19 "Kişi Hürriyeti ve Güvenliği", Madde-21 "Konut Dokunulmazlığı" Madde 20-21 "Özel Hayatın Gizliliğinin Korunması Hakkı" ve "Haberleşme Hakkı", Madde-24 "Din ve Vicdan Hürriyeti", Madde-25 "Düşünce ve Kanaat Hürriyeti" maddeleri örnek olarak gösterilebilir (Bulut, 2020, s. 119).

[10] 5502 sayılı Sosyal Güvenlik Kurumu Kanunu'nun 35. Maddesi gereği "kurumca genel sağlık sigortalılarının, bireysel veri ve haklarından oluşan toplu veri ve hakları ile işletmelerin ticarî sırları satılamaz ve paylaşılamaz" denilerek sağlık verileri özel koruma altına alınmıştır.

[11] Genetik verilere ilişkin Ceza Muhakemesi Kanunu'nun 75, 76 ve 78 75, 76 ve 78 inci madde hükümlerine göre alınan örnekler (vücuttan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak, cinsel organlar ve anüs bölgesinde yapılan muayene sonuçları) üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz.

olabilecek nitelikte veriler olmaları dikkate alınmakta ve bu sebeple bu türden veriler özel nitelikli (hassas) veri olarak kabul edilmektedir" şeklinde açıklanmıştır (Kişisel Verileri Koruma Kurumu, 2019). Sayılan verilerden bazıları 25611 sayılı Türk Ceza Kanunu'nun (TCK) 135. maddesinin 2. fıkrasında "kişisel verinin, kişilerin siyasî, felsefî veya dinî görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlakî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra[12] uyarınca verilecek ceza yarı oranında artırılır*"* olarak ifade edilmiştir (Türk Ceza Kanunu, 2004). Ancak bazı farklılıklar bulunmaktadır. KVKK'da hassas olarak sayılan "etnik köken", "mezhep veya diğer inançlar", "kılık kıyafet", "vakıf ya da dernek üyeliği", "ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler" ve "biyometrik veriler" TCK'da yer almayarak cezai artırım hükmüne bağlanmamıştır. Benzer bir şekilde TCK'da sayılan kişilerin "ahlaki eğilimleri" KVKK'da yer almamaktadır. Bazı verilerin işlenmesi sonucu ceza artırımı uygulanırken bazıları için söz konusu değildir. İki kanunî düzenleme arasında uyuşmazlık bulunmaktadır (Özkan, 2020, s. 247). Bu durumda ortaya çıkan farklılıkların giderilmesi gerekmektedir.

Hâlihazırda anılan ulusal ve uluslarüstü düzenlemelerde, hassas veri kategorileri belirli temalarda benzerlik gösterse de farklı şekilde tanımlanmakta, açıklık ve bireysel katılımı sağlama araçları farklılık göstermektedir. Hukuk sistemleri arasındaki mevcut geleneksel farklılıklar, hem yasal yaklaşımlar hem de kişisel verilerin korunmasına yönelik düzenleyici çerçeve açısından bir eşitsizlik nedenidir (OECD 2002, s. 25). Siyasî görüş, Amerika Birleşik Devletleri'nde kanunen hassas bilgi olarak kabul edilmemekle birlikte, özellikle İngiltere'de ve genel olarak Avrupa Birliği'nde (AB) hassas bilgi olarak kabul edilmektedir. Bazı hukukî düzenlemelerde belirli yaşın altındaki bireylere ait tanımlayıcı veriler, kesin coğrafî konum bilgileri, vatandaşlık ve göçmenlik bilgisi, alkol,

[12] TCK, Madde 135- (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

tıbbî ilaç ve uyuşturucu kullanımı sosyal görüşler, sosyal refahı, destek ve yardımları[13], hassas olarak ele alınmıştır. Farklılıklar coğrafya, kültür, inanç ve sosyal yaşam unsurlarının bir yansımasıdır. Örneğin coğrafî bölge bakımından yakın eyaletleri olan federal bir devlet yapılanmasına sahip ABD'de çeşitli münferit düzenlemeler uygulanmaktadır. Bu durum benzer kültürler arasındaki görüş farklılıklarının aynı çatı altındaki yönetimlerde bile ayrıştığını göstermektedir. Bunun dışında diğer düzenlemelerden farklı olarak ABD eyaletlerinde vatandaşlık statüsü hassas bir veri türü olarak yer almıştır. Bölgenin yasal ve yasa dışı göç hareketlerine maruz kalması ve bu durumun vatandaşlar arasındaki ayrıma sebebiyet vermesi bölgeye özgü bir hassasiyet olarak değerlendirilebilir.

İncelenen düzenlemeler doğrultusunda listelenen (Tablo-2) herhangi bir veri türü üzerinde mutabık bir anlayış yoktur. Tarihsel olarak da hangi tür verilerin hassas olarak kabul edileceği ve mevzuatta nasıl ifade edilmesi gerektiği konusunda fikir birliği bulunmamaktadır (Quinn ve Malgieri, 2021, s. 1587). Irk veya etnik köken, dinî, ahlakî, felsefî inanç ve faaliyetleri, sağlık verileri, genetik veya biyometrik veriler düzenlemelerinde çoğunda yer alan unsurlardır. Bunun dışında bazı düzenlemelerde (PIPEDA, BM) hassasiyet oluşumunun büyük ölçüde bağlama bağlı olduğu örnekler ile açıklanmıştır. Bu durum, konu-kelime odaklı listeleme yapmanın hassasiyet çerçevesini oluşturmak için yeterli olmayacağına[14] işaret edebilmektedir.

Türkiye'de yürürlükte olan düzenlemeler arasında farklılıklar bulunmasına rağmen AB GVKT ile uyumludur. Ancak hassas veri türlerinin yalnızca kişiler odaklı olması, çeşitlenmemesi ve düzenlemelerde yeterli düzeyde açıklanmadığı görülmektedir.

[13] Anılan düzenlemelerin dışında farklılık olarak alkol, tıbbî ilaç ve uyuşturucu kullanımı (İzlanda), sosyal görüşler (Finlandiya), sosyal refah, destek ve yardımlar (Finlandiya) bazı ülkelerde hassas olarak değerlendirilmektedir (Kaya, 2010, s. 319). Ayrıca web arama geçmişleri ve satın alma/alışveriş verileri dijitalleşmenin getirmiş olduğu yeni hassasiyetler olarak görülmektedir.

[14] III.2.1 Bağlam ve İlişki Kurma bölümünde belge içeriğine bağlı olarak bağlamsal hassasiyetlerin oluşabileceği, ilişkili veya ilişkisiz verilerin bir araya getirildiğinde hasssasiyet açığa çıkabileceği belirtilmektedir.

Bu durum anılan düzenlemelerin genelinde mevcuttur. İncelenen düzenlemelerdeki veri türlerinden farklı olarak kişilerin kılık ve kıyafeti özel bir nitelik bildirdiğinden Türkiye özelinde hassas olarak kabul edilmektedir.

Tablo 2. Ulusal Düzenlemelerde Hassas Bilgi

Mevzuat / **Veri Türü**	**Türkiye** KVKK	**Çin** PIPL	**Meksika** MFL-PPDHI	**Avustralya** APA	**Kanada** PIPEDA	**Virginia (ABD)** CDPA	**California (ABD)** CPRA	**Colorado (ABD)** CPA	**Connecticut (ABD)** CTDPA	**Rusya** LPD	**Arjantin** PDP	**Brezilya** LGPD	**İzlanda** **ADPPPD**	**İsviçre** **FADP**
Cinsel hayat veya yönelim	✓		✓	✓		✓	✓	✓	✓		✓	✓	✓	
Sağlık verileri		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Genetik veya biyometrik veri	✓	✓	✓	✓		✓		✓	✓	✓		✓	✓	
Sendika-dernek-vakıf üyeliği	✓		✓	✓			✓				✓	✓	✓	✓
Dinî - felsefî - iahlakî inançları ve faaliyetleri	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Kılık kıyafet	✓													
Siyasî görüş	✓		✓	✓						✓	✓	✓	✓	✓
SGK, ehliyet, kimlik, pasaport numaraları			✓	✓		✓	✓							
Irk veya etnik köken	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Finansal veriler, gelir (kartı numarası/ güvenlik/hesap erişim kodu vb.)		✓			✓		✓							
Kesin Coğrafî Konum						✓	✓							
Belirli yaşın altındaki çocuklara ait veri	✓					✓			✓					
Vatandaşık Statüsü (göçmenlik vs.)						✓		✓	✓					
Bilinen bir çocuğa ait veri								✓						
Sabık kaydı -suç geçmişi veya iddiası	✓			✓						✓				✓
Özel hayat, mahrem alan ve sosyal güvenlik										✓				✓

Uluslarüstü kurumlara ait düzenlemeler (Tablo 3), küresel düzeyde iş birliği ve etkileşimi düzenleyen kurallardır. Bu yapılara üye ülkeler coğrafî, ekonomik, askerî ve ulusal güvenlik gibi gerekçeler ile katılmaktadır. AB (27 üye), NATO (32 üye) ve BM (193 üye) hassas veriler konusunda yaygın bir etkiye sahiptir. AB GVKT'nin hassas veri tanımı çoğu ülke ve bölge hassas verilerini veya özel kişisel veri kategorilerini şekillendirmektedir (Wang ve Jiang, 2017, s. 11). Yayınlanan düzenlemelerde hassas verilerin rolü, genellikle güvenlik, gizlilik ve bilgi paylaşımı açısından geçerlilik ve kapsama alanını oluşturmaktadır. Ulusal düzenlemelerde listelenen çoğu veri türü bu düzenlemelerde de yer almaktadır.

Tablo 3. Uluslarüstü Düzenlemelerde Hassas Bilgi

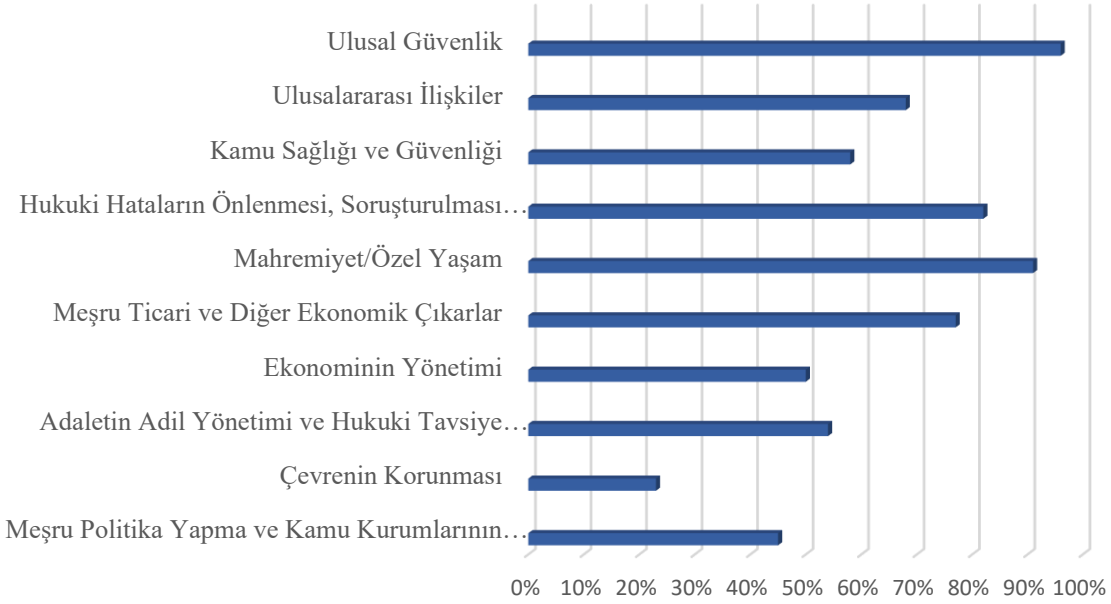
Mevzuat / **Veri Türü**[15]	**AB**	**NATO**	**BM**[16]
Cinsel hayat veya yönelim	✓		✓
Sağlık verileri	✓	✓	✓
Genetik veya biyometrik veri	✓		
Sendika-dernek-vakıf üyeliği	✓		✓
Dinî - felsefî - ahlakî inançlar	✓		✓
Siyasî görüş	✓		✓
SGK, ehliyet, kimlik, pasaport numaraları		✓	
Irk veya etnik köken	✓		✓
Finansal veriler, gelir (kartı numarası/ güvenlik/hesap erişim kodu vb.)		✓	
Zarar riski olan birey veya gruplar			✓
İşyeri performansı ve disiplin		✓	

[15] Tablo 2 ve Tablo 3'de yer alan veri türleri, incelenen düzenlemeler esas alınarak sadeleştirilerek kullanılmıştır. Hassas bilgi bağlamında kullanılan veri türleri sadece listelenen sayıda değildir.
[16] Tablo 2'de yer alan BM kapsamındaki hassas veri türleri, Veri Gizliliği, Etiği ve Korunması kılavuzu dikkate alınarak oluşturulmuştur. 2007/6 tarihli BM Genel Bülteni'nde ifade edilen hassasiyetler kavram odağı dışında belge odaklı olduğundan dahil edilmemiştir.

Özel hayat		✓	
Açıklanması kişiye zarar verecek her türlü gerçek veya görüş		✓	

Gerek ulusal gerekse uluslarüstü düzenlemelerde listelenen hassas bilgilerin listesini genişletmek mümkündür. Ancak bilgi hassasiyetinin doğrudan sayılamayacağı veya hassasiyet oluşumunun belirli kelimeler ile sınırlandırılamayacağı durumlar bulunmaktadır. Hukukî düzenlemelerde doğrudan hassas bilgilerin listesini oluşturmak çoğu zaman yetersizdir. Bu konuda "dolaylı hassas veri" kavramını geliştirerek ilk defa veri koruma mevzuatında yer veren – GVKT'ye tabi bir ülke olan – Belçika, oluşabilecek karışıklıkların önüne geçerek perspektifi genişletmiştir. Dolaylı hassas veriler, listelenen hassas bilgilerden herhangi birine işaret edebilecek veriler olarak ifade edilmektedir (Kindt, 2016, s. 127). Bu durum, dolaylı olarak ifade edilen hassas verilerin aynı zamanda bağlama bağlı oluşumlarına da dikkat çekmektedir. Hangi veri koruma ve gizlilik düzenlemesi olursa olsun listelenen hassasiyetler ile ilişkili verilerin de bu bağlamda değerlendirilmesi gerekmektedir.

Hassas bilgi mevzuatında yer alan veri/bilgi türleri çoğunlukla kişisel verileri kapsamaktadır. Kişilere bağlı hassasiyetlerin dışında yer alan türler genellikle Bilgi Edinme Hakkı kanunlarında muafiyet veya istisnai durumlar olarak ifade edilmektedir. UNESCO 2022 Kamuya Açık Bilgi Raporu'na göre (UNESCO, 2023, s. 16) 114 ülkede yürürlükte olan BEHK muaf olarak listelenen bilgi kategorileri (Grafik 1) belirlenmiştir.



Grafik 1. 114 Ülkenin Bilgi Edinme Muafiyetleri (UNESCO, 2023, s. 16)

Grafikte sunulan bilgi türleri değerlendirildiğinde, anılan hukukî düzenlemelerde tanımlanan özel nitelikli/hassas bilgilerde olduğu gibi potansiyel zarar oluşturma riski açısından ortak noktalar bulunduğu görülmektedir. Bu tür bilgiler, kişilere bağlı hassas bilgiler gibi, özel bir yönetim ve koruma yaklaşımını gerektirmektedir. Nitekim uluslarüstü düzenlemelerde bu konulara daha geniş bir çerçeveden yaklaşıldığı görülmektedir. Bu sebeple, söz konusu bilgilerin hassas yönetimi, hem bireylerin haklarının korunması hem de kamu yararının sağlanması açısından önemlidir. Çoğunlukla kişisel verilerden oluşan hassas bilgi türleri, Bilgi Edinme Hakkı Kanunlarında yer alan muafiyetler (*exemption*) aracılığıyla kapsamının genişletilmesine olanak tanımaktadır.

II.3.3. Hassas Bilgilerin İşlenmesi

Kurumlarda hassas bilgilerin işlenmesi, kurumsal itibarın zarar görmemesi, bireylerin mahremiyetini koruma ve güvenliklerini sağlama açısından büyük bir sorumluluktur.

Tüm kişisel bilgilerin aynı düzeyde korunamayacağı ve hassas olanların işleme (toplamak, kullanmak, analiz etmek, manipüle etmek vs.) koşullarının daha fazla önlem içermesi beklenir. Veri koruma/gizlilik yasalarında kişisel verilerin işlenmesi çeşitli şartlara bağlanırken hassas bilgi işleme konusu daha dikkat edilmesi gereken ve genellikle bazı istisnai ve özel durumlara bağlanmıştır.

Çin Kişisel Bilgileri Koruma Yasası'na göre kişisel bilgi işleyicileri, yalnızca belirli bir amaç ve yerine getirilmesi gereken bir ihtiyaç olduğunda, sıkı koruma önlemleri altında hassas kişisel bilgileri işleyebilir. Hassas kişisel bilgilerin işlenebilmesi için kişilerden rıza alınması gerektiği, kanunların veya idarî düzenlemelerin hassas kişisel bilgilerin işlenmesi için yazılı onay alınmasını öngördüğü durumlarda, bu hükümlere uyulacağı ifade edilmektedir. Ayrıca 14 yaşından küçüklerin kişisel bilgilerini işlediği durumlarda, özel kişisel bilgi işleme kurallarının formüle edileceği belirtilmiştir (Personal Information Protection..., 2021).

Rusya Kişisel Veriler Kanunu'nda hassas kişisel verilerin işlenmesi; veri sahibinin yazılı olarak açık rızasını göstermiş olması, veri sahibi tarafından kamuya açıklanmış olması, Rusya Federasyonu'nun geri kabule ilişkin uluslararası anlaşmalarını uygulaması için gerekli olması ve bazı mevzuat (sosyal hizmet, çalışma ve emeklilik) hükümlerine uygun olarak gerçekleştirilmesi gerekir (Russian Federation Federal…, 2021).

California Gizlilik Hakları Kanunu'nda hassas kişisel bilgilerin işlenmesi bazı durumlar ile sınırlandırılmıştır. İlk olarak işletmeler, mal veya hizmetleri gerçekleştirmek amacıyla tüketiciden makul olarak beklediği faydayı sağlamak için gerekliyse hassas bilgileri işleyebilmektedir. İkinci olarak işletmeler, belirtilen hizmetlerin (hesap bakımı, müşteri hizmetleri, sipariş işlemi, bilgi doğrulama, hizmet veya cihazı iyileştirmek vs.) yürütülmesi için hassas kişisel bilgileri kullanabilir. Son olarak işletmeler CPRA uyumluluğu gözetildiği sürece hassas kişisel bilgileri herhangi bir amaç için

kullanılabilir. İşletmeler hassas kişisel bilgileri toplaması durumunda, bu bilgileri hangi amaçlarla toplama, kullanma, satın alma veya paylaşma hususlarına ilişkin bildirimde bulunmadan kullanamayacaktır. Düzenlemede tüketiciler yüksek bir zarar riski yaratan hassas kişisel bilgilerinin yetkisiz kullanım veya ifşası durumunda kullanım sınırlaması yapılabileceği, makul önlemler almayan işletmeleri sorumlu tutabileceği ifade edilmektedir. Ayrıca işletmenin hassas kişisel bilgileri saklamayı amaçladığı süreyi belirtmesi gerekmektedir (Califonia Privacy…, 2020). Virginia Tüketici Verilerini Koruma Yasası'nda hassas veriler, kişisel veri olarak kabul edilir ve bu verilerin işlenmesi tek bir koşula bağlanmıştır. Kontrolörler bir tüketici ile ilgili hassas verileri tüketicinin rızasını almadan işleyemez (Virginia Consumer…, 2023). Benzer bir açıklı Colorado Gizlilik Yasası'nda da yer almaktadır. Bir kontrolör tüketicinin hassas verilerini önce tüketicinin rızasını almadan veya bilinen bir çocuğa ilişkin kişisel verilerin işlenmesi durumunda önce çocuğun ebeveyninin veya yasal vasisinin rızasını almadan işlemeyecektir (Colorado Privacy Act, 2023). Connecticut Veri Gizliliği Yasası da hassas verileri işlemek için bir tüketicinin rızasına ihtiyaç olduğunu ifade etmektedir (Connecticut Data Privacy Act, 2023).

Meksika Kişisel Verilerin Korunmasına İlişkin Federal Kanun'a göre hassas kişisel veriler söz konusu olduğunda, veri sorumlusu, veri sahibinin imzası – elektronik imzası veya bu amaçla oluşturulmuş herhangi bir kimlik doğrulama mekanizması – aracılığıyla veri sahibinden işleme için açık yazılı onay almalıdır. Ayrıca düzenlemede hassas kişisel veri içeren veri tabanları, meşru, somut ve düzenlemeye tabi tarafça izlenen açık hedefler veya faaliyetlerle tutarlı amaçlar gerekçelendirilmeksizin oluşturulamaz (Mexico Federal Law, 2010).

Arjantin Kişisel Verin Korunması Kanunu'na göre hiç kimse hassas verileri sağlamaya zorlanamaz. Hassas kişisel veriler, veri sahiplerinin kimliğinin belirlenemediği durumlarda istatistiksel veya bilimsel amaçlarla işlenebilir. Bunun

dışında adlî sicil kayıtları veya suçlara ilişkin veriler, ilgili kanun ve yönetmelikler çerçevesinde yalnızca yetkili kamu makamları tarafından işlenebilir. Doğrudan veya dolaylı olarak hassas verileri açığa çıkaran bilgileri depolayan dosyaların, bankaların veya kayıtların oluşturulması yasaktır. Ancak istisnai olarak Katolik Kilisesi, dinî dernekler ve siyasî ve sendikal örgütler üyelerinin kaydını tutabileceği ifade edilmektedir (Proteccıon De Los Datos Personales, 2000).

Brezilya Genel Kişisel Verilerin Korunması Kanunu'nda hassas kişisel verilerin işlenmesi iki hususta açıklanmıştır. İlk olarak veri sahibinin veya yasal vasisinin belirli amaçlar doğrultusunda belirli ve müstakil bir şekilde rıza göstermesi halinde verilerinin işlenebileceği belirtilmiştir. İkinci olarak veri sahibinin rızası olmaksızın, veri işlemenin zorunlu olduğu durumlar listelenmiştir. Düzenlemeye göre zorunlu haller şu şekildedir:

a) Yasal veya düzenleyici bir yükümlülüğün yerine getirilmesi,
b) Kamu idaresinin kanun veya yönetmeliklerle belirlenen politikalarını uygulayabilmesi için gerekli olan verilerin paylaşılarak işlenmesi,
c) Mümkün olduğunda hassas kişisel verilerin anonimleştirilmesi garanti altına alınarak bir araştırma kuruluşu tarafından çalışmaların yürütülmesi,
d) 23 Eylül 1996 tarihli ve 9.307 sayılı Kanun (Tahkim Kanunu) hükümleri uyarınca sözleşmeler, adlî, idarî ve tahkim yargılamaları dahil olmak üzere hakların düzenli olarak kullanılması,
e) Veri sahibinin veya üçüncü bir tarafın hayatının ya da fiziksel güvenliğinin korunması,
f) Münhasıran sağlık profesyonelleri, sağlık hizmetleri veya sağlık makamları tarafından yürütülen işlemlerde sağlığın korunması,
g) Bu Kanunun 9 uncu maddesinde belirtilen hakları koruyarak ve kişisel verilerin korunmasını gerektiren temel hak ve özgürlüklerin üstün olduğu durumlar hariç olmak üzere, elektronik sistemlerde kayıt tanımlama ve kimlik doğrulama

süreçlerinde sahteciliğin önlenmesini ve veri sahibinin güvenliğini garanti altına almak,

Amaçlarıyla hassas kişisel bilgilerin zorunlu haller kapsamında işlenmesi uygun bulunmuştur. Verilerin hassasiyeti, veri sahiplerinin zarar görme olasılığı ve ciddiyeti dikkate alınarak işlenebileceği belirtilmiştir (Presidência da República…, 2018, 11/1, 11/2).

Avustralya Gizlilik Yasası'na göre, bir devlet dairesinin veya kuruluşun hassas kişisel bilgileri toplayabilmek için bireylerden izin alması gerekir. Ancak bu durum, devlet dairesinin veya kuruluşun bir ya da daha fazla işlevi/faaliyeti için gerekli olmalıdır. Bunun dışında bilgilerin toplanması için bir Avustralya kanunu veya mahkeme kararı bulunması, devlet dairesi veya kuruluş tarafından toplanması ile ilgili izin verilen genel bir durum olması, izin verilen bir sağlık durumunun bulunması gerekmektedir. Ayrıca bir veya daha fazla uygulama faaliyet için makul ölçüde gerekliliği bulunan Göçmenlik Dairesi gibi devlet daireleri ve kâr amacı gütmeyen kuruluşların yalnızca kuruluşun üyeleri veya faaliyetleri ile bağlantılı, düzenli teması olan bireylerin verilerinin işlenmesi bu kapsamdadır. Bireyler bilgilerini bu amaçla kullanılmasına veya ifşa edilmesine rıza göstermişse, kurumlar doğrudan pazarlama amacıyla kullanabilir veya ifşa edebilir (Australia Privacy Act, 1988, 7/2, 7/3, 7/4).

Kanada Kişisel Bilgilerin Korunması ve Elektronik Belgeler Kanunu'na göre bilgilerin hassas olarak değerlendirilmesi muhtemel olduğunda işlenebilmesi için bir kurum genellikle açık rıza aramalıdır. Bilginin daha az hassas olması durumunda ise zımni rıza genellikle uygun olacaktır. Rıza, yasal vasi veya vekaletnameye sahip yetkili bir temsilci tarafından da verilebilir (Personal Information Protection…, 2000, 4.3.6)

Uluslarüstü düzenlemelerde hassas bilgilerin işlenme hususu AB odaklı kronolojik olarak incelendiğinde, 108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karsısında Şahısların Korunmasına Dair Sözleşme kapsamında daha önce

ifade edildiği gibi hassas kişisel verilerin işlenme koşulu, iç hukuka uygun güvenceler sağlanmaktır. Diğer bir düzenleme 95/46 sayılı "Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiğine İlişkin Direktif" hassas bilgilerin işlenebilmesi için veri sahibinin açık rıza vermiş olması gerektiğini belirtmektedir. Açık rızanın aranmadığı durumlar, düzenlemede şu şekilde açıklanmıştır:

a) Yeterli güvenceler sağlayan ulusal hukuk tarafından yetkilendirildiği ölçüde, kontrolörün iş hukuku alanındaki yükümlülüklerinin ve belirli haklarının yerine getirilmesi amacıyla işleme faaliyetinin gerekli olması,
b) Veri sahibinin fiziksel ve yasal olarak rıza gösteremeyecek durumda olması, veri sahibinin bir kişinin hayati çıkarlarını korumak için işlemenin gerekli olması,
c) İşleme faaliyetinin bir vakıf, dernek, siyasî, felsefî, dinî, sendikal amacı olan ve kâr amacı gütmeyen başka bir yapı tarafından uygun garantilerle meşru faaliyetleri sırasında işlenebilir. İşleme faaliyeti, yalnızca üyeleri veya amaçlarıyla bağlantılı olarak düzenli temas halinde olan kişilerle ilgili olması ve veri sahiplerinin rızası olmadan üçüncü bir tarafa ifşa edilmemesi koşuluyla gerçekleştirilmesi,
d) İşlemenin veri sahibi tarafından açıkça kamuya açıklanan verilerle ilgili olması veya yasal taleplerin oluşturulması, uygulanması ve savunulması için gerekli olması,

hassas verilerin işleme koşullarını oluşturmaktadır. Ayrıca verilerin işlenmesi, koruyucu hekimlik, tıbbî teşhis, bakım, tedavi sağlama veya sağlık hizmetlerinin yönetim amaçları için gereklilik ve bu verilerin ulusal hukuk veya ulusal yetkili organlar tarafından oluşturulan kurallar uyarınca mesleki gizlilik yükümlülüğüne tabi olan bir sağlık mesleği mensubu ya da eşdeğer bir gizlilik yükümlülüğüne tabi olan başka bir kişi tarafından işlendiği hallerde uygulanmaz. Direktif'e göre uygun güvencelerin sağlanmasına bağlı

olarak üye devletler, önemli kamu yararı gerekçeleriyle, ulusal hukuk veya denetim makamının kararı ile ek muafiyetler belirleyebilir (European Parliament…, 1995, 8/2, 8/2, 8/4).

Avrupa Konseyi tarafından 2001 yılında "181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol" kabul edilmiştir. Bu kapsamda hassas kişisel verileri de içine alan kişisel verilerin korunması alanında tam bağımsız görev yapan herhangi bir kişi tarafından kişisel verilerin işlenmesiyle ilgili olarak haklarının ve temel özgürlüklerinin korunmasına ilişkin yapılan talepleri kabul eden denetleyici bir kurul oluşturulacağı şart koşulmuştur (Council of European, 2001, 1/1, 1/2.a, 1/2.b, 1/3; Bulut, 2020, s. 117).

AB GVKT, hassas kişisel verilerin işlenmesini[17] yasaklamıştır. Ancak bazı durumlarda işlenebileceğine dair örneklemelerde bulunmuştur. Tüzüğe göre bu durumlar şu şekildedir:

a) Veri sahibinin söz konusu hassas verilerini belirtilen bir veya daha fazla amaç doğrultusunda işlenmesine açık rıza göstermiş olması,
b) Bir toplu sözleşme, kontrolörün veya veri sahibinin iş, sosyal güvenlik veya sosyal koruma için gerekli olduğunu belirtiyorsa ve bu sözleşme, birlik veya üye devletin yasalarına uygun olarak yetkilendirilmişse, kişisel verilerin işlenmesi gerekebilir. Bu durumda, belirli yasal yükümlülüklerin yerine getirilmesi veya belirli hakların kullanılabilmesi,

[17] 2018 yılında GVKT'ya dayalı olarak Avrupa Arşiv Grubu tarafından "Arşiv Hizmetleri İçin Veri Koruma Rehberi" hazırlanmıştır. Rehberde veri işlemenin bir yönü olan arşivlerde hassas bilgi işleme konusunda arşivcilerin, yasaları uygulama konusunda uzun ve başarılı bir deneyime sahip olduğu; arşiv hizmetlerinde veri sahiplerinin hak ve özgürlüklerine karşı risk değerlendirmesinin gerekliliği; kişisel veriler tutan topluluk arşivlerinde veri koruma memurunun görevlendirilmesi gerektiği; hassas kişisel veri içeren arşiv fornları işlenirken veri koruma etki değerlendirmesi hakkında kılavuzların kullanılması gerektiği ifade edilmektedir (European Archives Group, 2018, s. 27, 32).

c) Veri sahibinin fiziksel ve yasal olarak rıza gösteremeyecek durumda olması, veri sahibinin bir kişinin hayati çıkarlarını korumak için işlemenin gerekli olması,

d) İşleme faaliyetinin bir vakıf, dernek, siyasî, felsefî, dinî, sendikal amacı olan ve kâr amacı gütmeyen başka bir yapı tarafından uygun garantilerle meşru faaliyetleri sırasında işlenebilir. İşleme faaliyeti, yalnızca üyeleri veya amaçlarıyla bağlantılı olarak düzenli temas halinde olan kişilerle ilgili olması ve veri sahiplerinin rızası olmadan üçüncü bir tarafa ifşa edilmemesi koşuluyla gerçekleştirilmesi,

e) İşlemenin veri sahibi tarafından açıkça kamuya açıklanan verilerle ilgili olması,

f) İşleme faaliyetinin yasal hak taleplerinin oluşturulması, uygulanması veya savunulması için mahkemelerin adlî sıfatıyla hareket ettiği durumlarda gerekli olması,

g) İşleme faaliyetinin, birlik veya üye devlet hukuku temelinde, izlenen amaçla orantılı olarak veri koruma hakkının özüne saygı gösterecek, veri sahibinin temel haklarını ve menfaatlerini korumak için uygun ve özel tedbirler sağlayacak önemli kamu yararı sebebiyle gerekli olması,

h) İşlemenin koruyucu hekimlik, mesleki hekimlik, çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbî teşhis, sağlık, sosyal bakım, tedavi sağlanması ya da sağlık-sosyal bakım sistemlerinin ve hizmetlerinin birlik veya üye devlet hukuku temelinde veya bir sağlık profesyoneli ile yapılan sözleşme uyarınca yönetilmesi amaçlarıyla gerekli olması,

i) İşleme faaliyetinin birlik veya üye devlet hukuku temelinde özellikle mesleki gizlilik olmak üzere veri sahibinin hak ve özgürlüklerini korumak, sağlığa yönelik sınır ötesi tehditlere karşı koruma veya sağlık hizmetleri ile tıbbî ürün-

tıbbî cihazların yüksek kalite ve güvenlik standartlarının sağlanması gibi kamu sağlığı[18] alanında kamu yararı gerekçeleriyle gerekli olması,

j) Kamu yararına arşivleme, bilimsel veya tarihi araştırma amaçları ya da istatistiksel amaçlar doğrultusunda, izlenen amaçla orantılı olarak veri koruma hakkının özüne saygı gösterecek ve veri sahibinin temel haklarını ve menfaatlerini korumak için uygun tedbirler sağlayacak birlik veya üye Devlet hukukuna dayalı olarak işleme faaliyetinin gerekli olması,

hassas verilerin işlenme koşullarını oluşturmaktadır (European Parliament, 2016, 9/1, 9/2). AB üyesi olmayan İzlanda, Kişisel Verilerin Korunması ve İşlenmesi Hakkında Kanunu'nda GVKT'de ifade edilen işleme koşullarını doğrudan kendi düzenlemesine dahil etmiştir (Act on Data Protection…, 2018, 11). GVKT'den farklı olarak hassas kişisel veriler ve cezai suçlara ilişkin veriler de dahil olmak üzere, ses ve görüntü gibi elektronik izleme sırasında üretilen materyallerin toplanması konusu düzenlenmiştir[19]. AB üyesi olmayan bir diğer kıta ülkesi İsviçre, Federal Veri Koruma Kanunu'nda hassas kişisel verilerin veya kişilik profillerinin işlenmesini, resmî bir düzenlemenin açıkça öngörmesi halinde veya istisna olarak işlenebileceği haller belirlenmiştir. Verilerin işlenmesi, resmî bir yasada açıkça tanımlanan bir görev için gerekliyse, Federal Konsey veri sahibinin hakları tehlikeye atılmadığı bireysel bir durumda işlemeye izin veriyorsa, veri sahibi bireysel bir durumda rızasını vermiş veya verilerini genel olarak erişilebilir hale getirmiş ve işlenmesini açıkça yasaklamamışsa işlenebilir. Bu tür verileri işleyen

[18] Avrupa Parlamentosu ve Konseyi'nin 1338/2008 sayılı (EC) Tüzüğünde (1) tanımlandığı şekilde, hastalık ve engellilik de dahil olmak üzere sağlık durumu, bu sağlık durumu üzerinde etkili olan belirleyiciler, sağlık bakımı ihtiyaçları, sağlık bakımına ayrılan kaynaklar, sağlık bakımının sağlanması, sağlık bakımına evrensel erişimin yanı sıra sağlık bakımı harcamaları ve finansmanı, ölüm nedenleri gibi sağlıkla ilgili tüm unsurlar olarak yorumlanmaktadır. Sağlıkla ilgili verilerin kamu yararı amacıyla bu şekilde işlenmesi, kişisel verilerin işverenler veya sigorta ve bankacılık şirketleri gibi üçüncü taraflarca başka amaçlarla işlenmesine yol açmaması gerektiği belirtilmektedir (European Parliament, 2016, 54).

[19] Belitilen hassas bilgi içeren materyallerin anılan düzenlemede bazı şartlar doğrultusunda toplanabileceği ifade edilmektedir. Buna göre gözetim gereklidir, güvenlik ve mülkiyetin korunmasına ilişkin nedenlerle gerçekleştirilir. Gözetim yoluyla toplanan materyal, ilgili kişinin rızası veya kurallarda belirtilen yetkilere dayanarak ancak, materyalin bilgi ile birlikte polise iletilmesine izin verilir. Bu durumda materyalin diğer tüm kopyaları silinmelidir. Ayrıca gözetim yoluyla toplanan materyal, saklanması için nesnel gerekçeler kalmadığında silinecektir (Act on Data Protection …, 2018, 14/1, 14/2, 14/3).

özel kişiler, veri dosyalarını beyan etmek zorundadır. Federal Konsey, yetkili kimseye/komisyon üyesine danıştıktan sonra ve resmî bir kanun yürürlüğe girmeden önce, bazı durumlarda hassas kişisel verilerin veya kişilik profillerinin otomatik olarak işlenmesini onaylayabilir. Bu durumlar; veri işleme görevinin resmî bir düzenlemede bulunması, mahremiyet ihlallerinin önlemek için yeterli önlemler alınması, resmî düzenlemenin yürürlüğe girmeden önce test edilme aşaması olarak sıralanmıştır. Düzenlemeye göre test aşamasının zorunlu olduğu durumlar bulunmaktadır. İşleme, hassas kişisel verilerin veya kişilik profillerinin çevrimiçi olarak kanton[20] yetkililerine iletilmesini gerektiriyorsa zorunlu olarak test aşamasına tabi tutulur. Anılan kanunda ifade edilen bir diğer husus çevrimiçi erişimdir. Hassas kişisel veriler ve kişilik profilleri yalnızca resmî bir düzenlemede açıkça belirtilmişse çevrimiçi olarak erişilebilir hale getirilebilir (Federal Act on Data Protection, 2023, 4/5, 11/3, 11/3.a, 17/2, 17a/1, 17a/2, 19/3).

NATO, özel kategorideki kişisel bilgi ve hassas kişisel bilgi kavramlarını ayrı olarak tanımlasa da işlenme koşullarını özel kategorideki kişisel bilgilerin altında düzenlemiştir. Düzenlemeye göre özel kategorideki kişisel bilgilerin işlenme şartları şu şekildedir:

a) Bilgi sahibi, kişisel bilgilerin bir veya daha fazla özel amaç için işlenmesine açık rıza gösteriyorsa,
b) İşleme, bilgi sahibinin veya başka bir kişinin hayati çıkarlarının korunması için gerekliyse,
c) İşleme, NATO güvenlik politikasının ve istihbarata karşı koymanın gözetilmesi ve ayrıca yükümlülüklerin yerine getirilmesi, iş ve sosyal güvenlik alanındaki hakların kullanılması için gerekliyse,
d) İşleme, yasal taleplerin uygulanması veya savunulması için gerekliyse,

[20] Türk Dil Kurumu Çevrimiçi Sözlüğü'ne göre kanton, İsviçre Konfederasyonu'nu oluşturan devletlerden her biri anlamına gelmektedir. Bkz. https://sozluk.gov.tr/

e) İşleme, kamu yararına arşivleme amaçları, bilimsel, tarihi ve istatistiksel amaçlar için gerekliyse,

f) İşleme, kamu sağlığı alanında kamu yararı, çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbî teşhis ve sağlık veya sosyal bakım sağlanması nedenleriyle gerekliyse,

verilerin işlenmesi meşru bir zemin kazanır (NATO Act Personal Information…, 2022, 5/5). Uluslarüstü düzenlemeler arasında BM'nin hassas bilgilerin işlenmesine yönelik bir düzenlemesine ulaşılamamıştır.

Türkiye'de hassas bilgilerin/özel nitelikli kişisel verilerin işlenmesi, KVKK'nın 6. maddesinde düzenlenmiştir. Düzenlemeye göre (6/2), "özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır". Ancak "sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir" (6/3). 12 Mart 2024 tarihli 32487 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'da KVKK'nın 6. maddesinin anılan 2. fıkrası yürürlükten kaldırılmış, açık rıza şartı 3. fıkraya eklenerek bu fıkranın kapsamı genişletilmiştir. Son düzenleme ile birlikte KVKK'da özel nitelikli kişisel verilerin işlenme şartları (6/3) şu şekildedir:

a) İlgili kişinin açık rızasının olması,

b) Kanunlarda açıkça öngörülmesi,

c) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukukî geçerlilik tanınmayan kişinin, kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,

ç) İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,

d) Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,

e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,

f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukukî yükümlülüklerin yerine getirilmesi için zorunlu olması,

g) Siyasî, felsefî, dinî veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması

halinde mümkündür (Ceza Muhakemesi Kanunu…, 2024, 33). Bu durum hassas bilgilerin işlenme koşullarının anılan diğer ulusal ve uluslarüstü düzenlemelerde olduğu gibi geniş kapsamda değerlendirildiğini göstermektedir. Yapılan değişiklikler ile sağlık ve cinsel hayata ilişkin verilerin işlenmesi açık rıza şartına bağlıyken bu gereklilik artık kalmamıştır. Anılan nitelikte tüm veri işleme faaliyetlerinin tamamı kanunlarda ön görülmesi esasınca yürütülecektir.

Veri işleme hususu, Türk Ceza Kanunu'nun 135. maddesinin 1. fıkrasında "Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir" olarak yer almıştır. Daha önce ifade edildiği üzere 135. maddenin 2. fıkrası kapsamında sayılan hassas kişisel verilerin hukuka aykırı işlenme cezası yarı oranda artmaktadır. Hassas kişisel verilerin işlenmesine yönelik cezai müeyyide kişisel verilere

göre daha ağır önlemlere tabidir. Son düzenleme değişiklileri ile birlikte KVKK'da hassas kişisel verilerin işlenmesi şartları genişletilmiş, AB GVKT'ye büyük ölçüde uyumlu hale getirilmiştir.

KVKK'da hassas verileri konu edinen bir diğer değişiklik kişisel verilerin yurt dışına aktarılması hususunu inceleyen 9. maddede yapılmıştır. Bazı hususların geçerlilik süresi[21] devam etmek ile birlikte 7499 sayılı kanundaki (Ceza Muhakemesi Kanunu…, 2024, 34) güncel madde şu şekildedir:

1) Kişisel veriler, 5 inci ve 6 ncı maddelerde belirtilen şartlardan birinin varlığı ve aktarımın yapılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar hakkında yeterlilik kararı bulunması halinde, veri sorumluları ve veri işleyenler tarafından yurt dışına aktarılabilir.
2) Yeterlilik kararı, Kurul tarafından verilir ve Resmî Gazete'de yayımlanır. Kurul, ihtiyaç duyması halinde ilgili kurum ve kuruluşların görüşünü alır. Yeterlilik kararı, en geç dört yılda bir değerlendirilir. Kurul, değerlendirme sonucunda veya gerekli gördüğü diğer hallerde, yeterlilik kararını ileriye etkili olmak üzere değiştirebilir, askıya alabilir veya kaldırabilir.
3) Yeterlilik kararı verilirken öncelikle aşağıdaki hususlar dikkate alınır:
    a) Kişisel verilerin aktarılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar ile Türkiye arasında kişisel veri aktarımına ilişkin karşılıklılık durumu.
    b) Kişisel verilerin aktarılacağı ülkenin ilgili mevzuatı ve uygulaması ile kişisel verilerin aktarılacağı uluslararası kuruluşun tâbi olduğu kurallar.

[21] 7499 sayılı kanunun 36. maddesine 6698 sayılı kanuna geçici maddeler eklenmiştir. GEÇİCİ MADDE 3- (1) 9 uncu maddenin bu maddeyi ihdas eden Kanunla değiştirilmeden önceki birinci fıkrası, maddenin yürürlüğe giren değişik haliyle birlikte 1/9/2024 tarihine kadar uygulanmaya devam olunur.
(2) 1/6/2024 tarihi itibarıyla sulh ceza hâkimliklerinde görülmekte olan başvurular, bu hâkimliklerce görülmeye devam olunur.

c) Kişisel verilerin aktarılacağı ülkede veya uluslararası kuruluşun tâbi olduğu bağımsız ve etkin bir veri koruma kurumunun varlığı ile idarî ve adlî başvuru yollarının bulunması.

ç) Kişisel verilerin aktarılacağı ülkenin veya uluslararası kuruluşun, kişisel verilerin korunmasıyla ilgili uluslararası sözleşmelere taraf veya uluslararası kuruluşlara üye olma durumu.

d) Kişisel verilerin aktarılacağı ülkenin veya uluslararası kuruluşun, Türkiye'nin üye olduğu küresel veya bölgesel kuruluşlara üye olma durumu.

e) Türkiye'nin taraf olduğu uluslararası sözleşmeler.

4) Kişisel veriler, yeterlilik kararının bulunmaması durumunda, 5 inci ve 6 ncı maddelerde belirtilen şartlardan birinin varlığı, ilgili kişinin aktarımın yapılacağı ülkede de haklarını kullanma ve etkili kanun yollarına başvurma imkânının bulunması kaydıyla, aşağıda belirtilen uygun güvencelerden birinin taraflarca sağlanması halinde veri sorumluları ve veri işleyenler tarafından yurt dışına aktarılabilir:

a) Yurt dışındaki kamu kurum ve kuruluşları veya uluslararası kuruluşlar ile Türkiye'deki kamu kurum ve kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşları arasında yapılan uluslararası sözleşme niteliğinde olmayan anlaşmanın varlığı ve Kurul tarafından aktarıma izin verilmesi.

b) Ortak ekonomik faaliyette bulunan teşebbüs grubu bünyesindeki şirketlerin uymakla yükümlü oldukları kişisel verilerin korunmasına ilişkin hükümler ihtiva eden ve Kurul tarafından onaylanan bağlayıcı şirket kurallarının varlığı.

c) Kurul tarafından ilan edilen, veri kategorileri, veri aktarımının amaçları, alıcı ve alıcı grupları, veri alıcısı tarafından alınacak teknik ve idarî tedbirler, özel nitelikli kişisel veriler için alınan ek önlemler gibi hususları ihtiva eden standart sözleşmenin varlığı.

ç) Yeterli korumayı sağlayacak hükümlerin yer aldığı yazılı bir taahhütnamenin varlığı ve Kurul tarafından aktarıma izin verilmesi.

5) Standart sözleşme, imzalanmasından itibaren beş iş günü içinde veri sorumlusu veya veri işleyen tarafından kuruma bildirilir.

6) Veri sorumluları ve veri işleyenler, yeterlilik kararının bulunmaması ve dördüncü fıkrada öngörülen uygun güvencelerden herhangi birinin sağlanamaması durumunda, arızi olmak kaydıyla sadece aşağıdaki hallerden birinin varlığı halinde yurt dışına kişisel veri aktarabilir:

a) İlgili kişinin, muhtemel riskler hakkında bilgilendirilmesi kaydıyla, aktarıma açık rıza vermesi.

b) Aktarımın, ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için zorunlu olması.

c) Aktarımın, ilgili kişi yararına veri sorumlusu ve diğer bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin kurulması veya ifası için zorunlu olması.

ç) Aktarımın üstün bir kamu yararı için zorunlu olması.

d) Bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin aktarılmasının zorunlu olması.

e) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukukî geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin aktarılmasının zorunlu olması.

f) Kamuya veya meşru menfaati bulunan kişilere açık olan bir sicilden, ilgili mevzuatta sicile erişmek için gereken şartların sağlanması ve meşru menfaati olan kişinin talep etmesi kaydıyla aktarım yapılması.

7) Altıncı fıkranın (a), (b) ve (c) bentleri, kamu kurum ve kuruluşlarının kamu hukukuna tâbi faaliyetlerine uygulanmaz.
8) Veri sorumlusu ve veri işleyenler tarafından, yurt dışına aktarılan kişisel verilerin sonraki aktarımları ve uluslararası kuruluşlara aktarımlar bakımından da bu Kanunda yer alan güvenceler sağlanır ve bu madde hükümleri uygulanır.
9) Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak kurulun izniyle yurt dışına aktarılabilir.
10) Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır
11) Bu maddenin uygulanmasına ilişkin usul ve esaslar yönetmelikle düzenlenir.

Hassas kişisel bilgilerin/özel nitelikli kişisel verilerin, hem yurt içinde hem de yurt dışında işlenme koşulları, yapılan değişiklikler ile birlikte açıklanmıştır. Bu durumda yurtdışına veri aktarımı için açık rıza şartı yeterli olmayarak kaldırılmıştır. Önceki düzenlemeye göre veri aktarımının yapılacağı ülkelere, sektörlere veya kuruluşlara yönelik yeterlikleri belirlenmesi ve artık veri işleyenlerin de veri sorumluları ile eş değer tutulması,[22] kabahatlere[23] tabi olması yenilikler arasındadır. Dikkat çeken bir diğer değişiklik ile KVVK'nın 6/2 fıkrasında belirtilen sağlık ve cinsel hayata ilişkin veriler ile diğer özel nitelikli veriler arasındaki işleme ayrımı kaldırılmıştır.

Anılan düzenlemelerde hassas bilgilerin işlenmesine yönelik çeşitli yönlerden yaklaşımlar ortaya konulmuştur. Açık rıza şartı hemen hemen tüm düzenlemelerde temel

[22] Bu hususta KVKK'nın 18'inci maddesine ek olarak "(2) Birinci fıkranın (a), (b), (c) ve (ç) bentlerinde öngörülen idarî para cezaları veri sorumlusu, (d) bendinde öngörülen idarî para cezası veri sorumlusu veya veri işleyen gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır." maddesi eklenerek verim sorumlusu ve veri işleyen benzer yükümlülüklere tabi tutulmuştur.
[23] 7499 sayılı kanunda yapılan değişikliler ile "d) 9 uncu maddenin beşinci fıkrasında öngörülen bildirim yükümlülüğünü yerine getirmeyenler hakkında 50.000 Türk lirasından 1.000.000 Türk lirasına kadar," fıkrası eklenerek hem veri sorulusuna hem de veri işleyene uygulanacaktır (Ceza Muhakemesi Kanunu…, 2024, 35).

işleme gerekçesi olarak bulunmaktadır. Yasal yükümlülüğün yerine getirilmesi amacıyla kanunî düzenlemeye uyumluluk, kamu sağlığı ve hayatî çıkarların korunması hususları da genellikle yer edinmiştir. Bazı düzenlemeler, belirli yaşın altındaki bireylere yönelik özel durumlar (PIPL), ticarî hususlar (CPRA), güvenlik ve istihbarat (NATO), kamu yararına arşivleme (GVKT, NATO) konularını işleme gerekçesi olarak sunması ile farklılık oluşturmaktadır.

Bir diğer husus kamuya açık bilgilerdir. Kamuya açık bilgiler, bireylerin erişime izin verdiği bilgiler ve kamuyu ilgilendiren bilgiler genellikle hassas bilgi olarak kabul edilmez. Bu bilgiler hâlihazırda kamu malı olduğundan bağlam ve içerik açısından hassas olmamaktadır (Photopoulos, 2011, s. 21). Ancak bir kişi kendisine ait tıbbî kayıtları sosyal ortamlarda paylaşması kendi mahremiyetini ihlal etmesi anlamına gelirken kamu kurumları için aynı durum geçerli olmamaktadır. Bu konuda temel ölçüt kamunun herhangi bir üyesinin bu bilgilere erişip erişemeyeceğidir. Özel veya sınırlı bir kitleye sunulan hassas bilgileri kimin açıkladığı, hangi bağlamda açıklandığı, kasten veya kazara mı açıklandığı, bireylerin bu bilgileri kamu malı haline getirdiğinin farkında olup olmadığı önemlidir. Hassas bilgilerin kamuya açıklanması kurumların şeffaflık konusundaki yükümlülüklerini/sınırlılıklarını etkilememektedir (Information Commissioner's Office, 2022). Kamuya açık hassas bilgilerin kurumlar tarafından işlenmesi ile erişime sunulması ve yaygınlaştırılması farklıdır. Dolayısıyla bilginin kamuya açık bir belge içeriğinde yer alması mahremiyet ve gizlilik hakkının elden alınması anlamına gelmemektedir.

Hassas bilgi tanımlaması ve işlenmesi hususundaki yaklaşımlar çeşitli faktörlere göre mevzuata yansımıştır. Anılan sınırlı düzenleme bu konuda geniş ve muğlak bir durumun olduğunu göstermektedir. Nitekim daha geniş kapsamlı bir araştırma 92 ülkedeki veri koruma yasasında ve uluslarüstü düzenlemelerdeki hassas veri tanımını inceleyerek yürütülmüştür (Wang ve Jiang, 2017). Elde edilen bulgular benzer

niteliktedir[24]. Mevzuat odaklı hassas bilgi saymaları/listelemeleri salt kişisel bilgilere odaklı bir tutumdadır. Bu bağlamda çalışma kapsamında araştırma konusuna bağlı olarak bir sınıflamanın yapılması, yasal olarak ifade edilenlere ek olarak yasal olmayan hassasiyet varlığına ilişkin bakış açısının oluşturulması, kişisel bilgilere bağlı odak hassasiyet sınıflaması ile birlikte yeni bir yaklaşımın ortaya konulması gerekmektedir. Ancak yeni bir hassas bilgi sınıflamasının yapılması zorlu bir süreçtir. Verilerin işlenme ve kullanım koşulları ile değişen toplumsal, ekonomik ve kültürel konjonktür dikkate alındığında mutlak sınıflandırma yaklaşımının yanı sıra bir görecelilik durumunun varlığının kabul edilmesi makul bir seçenek olarak ortaya çıkmaktadır (Bulut, 2020, s. 124). Bu noktada bağlam faktörü verileri/bilgileri potansiyel olarak hassas kılacağından (McCullagh, 2007, s. 198) sınırlama veya çerçevenin mevzuat göz ardı edilmeksizin ilgili alana göre şekillenmesi gerekir.

II.4. Hassas Bilgi Türleri

Hassas bilgileri korumanın ilk adımı, tanımlamak ve sınıflandırmaktır. Bu durum risk düzeyini ve uygulanması gereken güvenlik önlemlerinin yürütülmesine yardımcı olacaktır. Hukukî düzenlemelerde hassas bilgiler çeşitli türlerde sayılarak listelenmiştir. Ancak etkili bir sınıflandırmanın/kategorizasyonun yapılması, mevzuat sınırlarını aşarak uygulamada görülebilecek hassasiyetlerin sınıflandırılması gerekir. Bu durumda hangi verilerin hassas olduğunu belirginleştirmek zordur (Bulut, 2020, s. 124). Mevzuat liste olarak bir çerçeve ortaya koymaktadır. Sınıflama yapmanın ve hassas verilere yönelik tanımsal bir yaklaşımın yeterli olmadığı, genellikle mevzuatta yer alan listelemelerin tamamen örnek niteliğinde olması gerektiği (Simitis, 1999) görüşleri de bulunmaktadır.

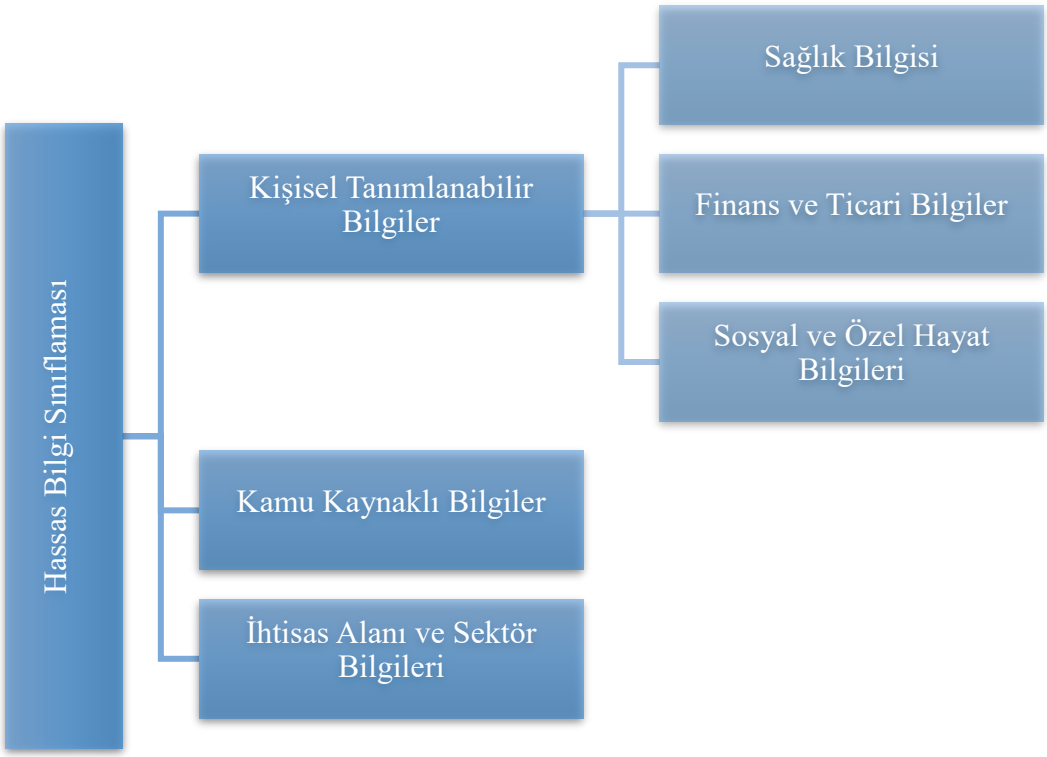
[24] 92 ülke üzerine yapılan araştırmada, bu çalışma kapsamında belirtilen hassas bilgi türlerinin dışında; kişisel alışkanlıklar, vergi borçları, telefon numarası, yaş, evlat edinme, aile içi şiddet, noter işlemi, eğitim, ev adresi/kayıtlı ikametgâh, kişisel veya tanıdık miras, sosyal statü, öğrenci verileri gibi bazı veri/bilgi türleri incelenen mevzuat düzenlemelerinde yer almıştır. Bu hususların birçoğu benzer ilişkiler kurularak çalışma kapsamında vurgulanmıştır.

Bu konuda genel bir yaklaşımın yanı sıra odak alana yönelik bir sınıflamanın geliştirilmesi belirsizliği ortadan kaldırabilir. Kurumların bilgi varlıklarını bu tür sınıflamalara göre kategorize etmesi hassasiyetlerini ve gizliliklerini tanımlamasına yardımcı olacaktır (Photopoulos, 2011, s. 44).

Hassas bilgi sınıflandırması yapılırken genellikle konulara göre bir sınıflandırmanın yaygın olarak kullanıldığı görülmektedir (Ohm, 2014; The National Archives, 2019a). Fakat bu durum belirsiz ve tartışmaya açıktır (Belen-Sağlam, Nurse ve Hodges, 2022a, s. 2). Tüm hassas bilgilerin aynı düzeyde olmayacağı görüşü (Photopoulos, 2011, s. 5), derecesine/seviyesine göre yüksek, orta ve düşük olarak sınıflandırıldığı taksonomiler de mevcuttur. Örneğin tıbbî geçmiş, cinsel yaşam bilgileri yüksek hassasiyet; sendika üyeliği orta hassasiyet; isim, adres bilgileri düşük hassasiyet olarak değerlendirilmektedir. Bir bireyin sosyal güvenlik veya finansal hesap numarasının genellikle telefon numarasından veya posta kodundan daha hassas olduğunu ifade etmek mümkündür. Örnek bir hassasiyet derecelendirme yaklaşımı BM Arşiv ve Belge Yönetimi Bölümü tarafından geliştirilmiştir. BM çalışmalarına büyük zararlar vererek yürütülmesini engelleyebilecek bilgiler çok gizli (*strictly confidential*); zarar vermesi beklenen bilgiler gizli (*confidential*); herhangi bir zarar oluşturmayan bilgiler ise gizli olmayan (*unclassified*) olarak üç kısma ayrılmıştır (Birleşmiş Milletler, 2024b).

Kişiler hakkındaki herhangi bir hassas bilgi, onların mahremiyetini ihlal etme potansiyelini taşırken stratejik görev ve meslek durumu, kamusal tanınırlık gibi unsurlara göre az ya da çok hassasiyet oluşturabilir. Bu durumda hassasiyet yargısının bireyler özelinde değişkenlik göstereceği ifade edilebilir (Sillitoe, 1988, s. 9). Hassasiyet derecelendirme yaklaşımı, konu odaklı sınıflamaya göre daha dar bir çerçeve sunmaktadır. Mevzuat ve araştırmalarda konu odaklı bir yaklaşım yaygın olarak benimsenmektedir. Finans, sağlık, kişisel, ticarî, uluslararası ilişkiler vb. pek çok konu sınıflandırması kullanılmaktadır. Neredeyse tüm bilgi gizliliği yasaları sağlık, cinsiyet

veya finansal bilgiler gibi belirli "hassas bilgi" kategorileri için özel koruma sağlamaktadır. Bu yaklaşım yaygın olsa da hassas bilgi kavramı yeterince teorize edilmemiştir (Ohm, 2014, s. 1125). Bu sınıflandırmalar genellikle gerçek kişiler ile ilgili olan hassasiyet konuları ve diğer konulardan oluşmaktadır. Kişisel bilgiler altında pek çok konu ile ilgisi olan hassas bilgiler yer alabilmektedir. Bir kişinin finans ve sağlık konularında hassas bilgileri olabileceği gibi bu alanların kendi özelinde barındırmış oldukları hassas bilgiler de mevcuttur. Kişilerin kamu kurumlarında yaptığı işlemlerden dolayı hassas bilgileri paylaşılırken kurumların da hassas bilgilere sahip olduğu bilinmektedir. Diplomatik ziyaretler, yazışmalar, kamuya kapalı görüşmeler, yine kişilerden bağımsız bir hassasiyet oluşturmaktadır. Dolayısıyla hassas bilgiler kategorize edilirken doğrudan kişileri ilgilendiren bilgiler ve kişilere bağlı olmayan hassas bilgiler olarak bir sınıflandırma (Şema 2) yapılması mümkündür.



Şema 2. Hassas Bilgi Sınıflaması

II.4.1. Kişisel Tanımlanabilir Bilgiler

Hassas bilgi tanımlaması ve sınıflandırılması yapılırken genellikle kişisel bilgiler, öne çıkan tanımlama argümanı olarak ifade edilmektedir. Çünkü kişisel ve hassas bilgiler arasındaki farklar çok incedir. Hassas bilgilerin çoğunlukla kişisel bilgilerden oluşması bu durumu desteklemektedir. Her iki veri türünün de kazara ifşa edilmesi korku ve rahatsızlığa neden olsa da, ifşa edilen hassas verilerden kaynaklanan etkiler özellikle çok daha ciddidir. Kişisel verilere ise makul ölçüde koruma önlemleri uygulanmalıdır (Birleşmiş Milletler Geliştirme Grubu, 2017, s. 5). Kişisel verilerin de hassasiyet oluşturma ihtimali vardır. Fakat her kişisel bilginin tek başına veya bir arada hassasiyet içermediği durumlar da bulunmaktadır. Bir kişiye ait sadece ad-soyad bilgisi, telefon numarası veya e-posta adresi hassasiyet için yeterli midir? Kişisel Verilerin Korunması Kanunu'nda (2016) kişisel veri ve özel nitelikli kişisel veri kavramları bir ayrım olarak açıklanmıştır. Kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanırken özel nitelikli kişisel veri, "kişilerin ırkı, etnik kökeni, siyasî düşüncesi, felsefî inancı, dinî, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler" olarak ifade edilmektedir. Bu tanımlamalar hassasiyetin yalnızca sayılan özel nitelikli kişisel veriler çerçevesinde daraltılması anlamına gelmemektedir. Bilgi parçalarını birbiri ile tamamlayıp bir bireyi tanımlayacak şekle dönüştürünce bağlama bağlı olarak hassasiyet durumu ortaya çıkabilir veya çıkmayabilir. Kişisel tanımlanabilir bilgiler, hassas olabilir veya olmayabilir; yalnızca belirli koşullar altında hassas kabul edilebilir; veya bir birey hakkındaki diğer verilerle birleştirildiğinde hassasiyet açığa çıkabilir. Örneğin, adlar, telefon numaraları veya herkese açık olarak yaygın olarak bulunabilecek kişisel bilgiler genellikle (belirli bağlamlarda olabilir) hassas kabul edilmez. Bundan dolayı kişisel bilgilerin başlı başına hassas bilgi olarak kabul edilemeyeceği durumlar da bulunmaktadır. Nitekim bazı

durumlarda kişinin görevli olduğu kurumsal yapı, tanınırlık ve görev bilgisi sebebiyle ad soyad bilgisi dahi hassasiyet olarak düşünülebilir. Bir ev adresi veya telefon numarası kişisel tanımlayıcı bilgi olması sebebiyle bağlamına bağlı olarak "hassas" olabilir. Bunun aksine, çalışanların bir kartviziti veya umumi telefon rehberi kişisel tanımlayıcı bilgi içerir ancak hassas değildir (Transportation Security Administration, 2008, s. 2). Kişisel bilginin yer aldığı bağlam çoğu zaman hassasiyet durumunu değiştirebilmektedir. Hassas bilgi sınıflamasının büyük bir bölümünü oluşturan kişisel bilgiler, doğası gereği gerçek kişilere doğrudan etki etmesi sebebiyle diğer bilgilerden daha savunmasızdır. Dolayısıyla hassasiyet oluşturabilecek noktalarının doğru anlaşılması gerekmektedir.

Kişisel bilgiler doğası gereği kritiktir. Niteliği itibarıyla temel hak ve özgürlüklere yönelik önemli riskler oluşturabilmesi sebebiyle özel korumayı gerektirir. Bu durum, riske maruz kalma düzeyinin daha yüksek olmasından dolayıdır. Bu tür verilerin kötüye kullanılması veya uygunsuz bir şekilde değerlendirilmesi, istenmeye sonuçlara yol açabilir. Kişisel bilgiler, bir kişiyi tanımlamak için kullanılan herhangi bir veriyi ifade eder. Doğrudan ya da dolaylı olarak, tek başına veya diğer bilgilerle birlikte kimliği belirli veya belirlenebilir bir gerçek kişiyle ilgili her türlü bilgi kişisel bilgi kapsamındadır (Entrikin, 2020, s. 895). Bir adres, bir araç kaydı veya dinamik bir IP adresi bir bireyle güçlü bir şekilde ilişkilendirilebilir, bu nedenle bunlar hakkındaki veriler dolaylı olarak o birey hakkındaki verilerdir (Rumbold ve Pierscionek, 2018, s. 54). Ad-soyad, medeni durum, adres, sosyal güvenlik numaraları, ehliyet numaraları, banka hesap numaraları ve tıbbî kayıtlar gibi doğrudan ilişkili bilgilerden oluşabilir. Bazı kişisel bilgiler (fotoğraflar, sesler, veya teyp kayıtları) hiç kelime içermez. Örneğin bir telekomünikasyon şirketi, telefon görüşmelerini kaydeder. Bireyin sesini içeren bir çağrının kaydedilmesi, kaydedilen kişinin tanımlanabileceği kişisel bilgileri olabilir. Bu kayıtlar müşterinin dosyasında yer alan kişisel bilgileri oluşturur. Bu bilgiler genellikle gizlilik düzenlemelerine tabidir ve özel koruma gerektirir.

Kişisel bilgiler, bireyle ilgili olan; bu sebeple mahrem veya hassas olarak kabul edilen; toplanılması veya kullanılması hususunda kısıtlama veya engelleme istenmesi makul olan gerçekler, iletişimler veya görüşlerden oluşmaktadır (Wacks, 1989, s. 26). Fakat her kişisel bilginin mahrem veya hassas olduğunu ifade etmek güçtür. Kişisel bilgilerin güvenlik açığı, maddi veya manevi zarar, utanç ve ayrımcılık gibi mağduriyetlere sebep verebilme ihtimalinin bulunması, ekstra güvenlik ve özel işlenme gereksinimleri hassas bir nitelik taşıdığını gösterir. Hassas kişisel bilgileri, kamuya açık hale getirildiği takdirde makul bir kişide önemli sorunlara sebep olacak bilgiler olarak tanımlanmaktadır (Sillitoe, 1988, s. 9). Bu bilgiler bir kez sızdırıldığında, insan onuru ve mülkiyet güvenliği açısından büyük bir risk oluşturabilir ve bu nedenle genel kişisel bilgilerden daha sıkı bir koruma sağlanması gerekmektedir. Niteliği itibarıyla temel hak ve özgürlükler açısından hassas olan kişisel veriler, işlendikleri bağlama yönelik önemli riskler oluşturabilmesi nedeniyle özel korumayı hak etmektedir.

Kişiler ile ilgili pek çok bilgi hassas olarak değerlendirilebilir. Örneğin çalışanların kâr amacı gütmeyen topluluklara veya meslek örgütlerine olan üyeliği, göğüs kanseri olan bir çalışanın hastane kayıtları, kişinin ırkı, dinî, cinsel tercihi, siyasî görüşü, düzenli kullanılan ilaçları ve hastalıkları, mahkûmiyet geçmişi, zihinsel ve fiziksel sağlık vb. bilgiler hassas nitelikteki kişisel bilgilerdir. Kişi hakkında herhangi bir görüş ifadesi bu kişiyle ilgili niyetin bir göstergesini içerir ve bu nedenle, ilgili herhangi bir bağlamsal bilgi de hassas kişisel bilgilerin bir parçasıdır (McDonald, 2019, s. 38). Bu tür hassas kişisel bilgiler, özel nitelikli kişisel bilgi statüsüne sahip olup bireyler veya topluluklar tarafından ihlal edilmeye açıktır. Bununla birlikte genetik veriler, fotoğraf ve görüntüler [25]de hassas olarak değerlendirilebilir. Bir kişinin sesinin veya görüntüsünün kullanılması,

[25] Hollanda'daki kanun yapıcılar kişilere ait resimlerin/fotoğrafların işlenmesinin temelde bir kişinin ırkının belirleyebileceğinden hassas verilerin işlenmesi olarak değerlendirilmesi gerektiğini belirtmişlerdir (Kindt, 2016, s. 137).

çeşitli uygulamalar ile manipüle edilerek utanç verici durumlara sebebiyet vererek maddi zararlara uğratabilecek niteliktedir. Kişilerin sosyal hayatına zarar verebileceği gibi bankacılık uygulamalarındaki doğrulama süreçlerinde kullanılması bakımından da risk oluşturmaktadır.

Hassas nitelikteki kişisel bilgiler, bireylerin gündelik faaliyetleri ve etkileşimde bulundukları alanlara göre farklı tür ve niteliklere sahip olabilmektedir. Özel bir uzmanlık alanını kapsayan bilgiler, bireyler ile ilgili olabildiği gibi kendi içerisinde de hassas bilgiler barındırmaktadır. Örneğin bir kişiye ait mobil bankacılık parolası hassas finansal bilgi olmasının yanında, tüzel bir finans kuruluşunun müşteri bilgileri veya borsa işlem planlamaları da finansal hassas bilgilerdir. Bu bağlamda kişiler etrafındaki hassasiyet sınıflandırmasının doğru anlaşılması gerekmektedir.

II.4.1.1. Sağlık Bilgisi

Sağlık bilgisi, sağlık hizmetlerinin sağlanması da dahil olmak üzere kişilerin fiziksel veya zihinsel sağlığına ilişkin kişisel verileri anlamına gelmektedir. Bu veriler, kişisel bir nitelikte olup açığa çıkması durumunda bireylerin mahremiyetini ilgilendiren fiziksel, zihinsel, ekonomik, kültürel veya sosyal kimliğe zarar verebilecek etkidedir. Hassas sağlık bilgileri genetik, biyometrik, genomik ve aile tıbbî geçmişi dahil olmak üzere geçmiş, mevcut veya gelecekteki potansiyel sağlık veya tıbbî koşullar, tedaviler hakkında kesin bilgiler olarak tanımlanmaktadır Kişilerin genetik bilgisi, sağlık sigortası, test ve laboratuvar sonuçları, cinsel sağlığı, ilaç kullanımları, fiziksel ve zihinsel sağlığı, geçirmiş olduğu hastalıklar gibi çeşitli tedavi ve sonuçları içeren tıbbî geçmişleri hassas içerikli kişisel sağlık bilgisi kapsamındadır. Sağlık bilgisi, birçok farklı paydaş tarafından ele alınır ve işlenir, bu da verilerin gizliliği ve güvenliği açısından önemli sorumluluklar gerektirir. Sağlık hizmeti sunan hastaneler, eczaneler, yaşam ve tıp merkezleri sağlık ağında tedavi, bakım veya hizmet alan her hasta için kişisel hassas bilgiler tutmaktadır.

II.4.1.2. Finansal ve Ticarî Bilgiler

Yaygın olarak tanınan bir diğer hassas bilgi kategorisi finansal bilgilerdir. Finansal bilgiler ölçülebilir ekonomik zararlara kolayca maruz kalma eğilimindedir, bu da onları korumayı gerekli kılar. Bir bilginin finansal veya ticarî olarak gizli kabul edilmesi için ekonomik bir değere sahip olması, nüfusun çoğunluğu tarafından bilinmemesi ve sahibinin bilgiyi gizli tutmak için gösterdiği çabalar nedeniyle keşfedilebilecek bir bilgi olmaması gerekir (American Board…, 2016, s. 11). Bazı malî olmayan bilgi türleri bile, kimlik hırsızlığı gibi malî zarar potansiyeli nedeniyle korunmaktadır. Örneğin, sosyal güvenlik numaraları gibi benzersiz devlet tanımlayıcıları, yeni kimlik kartları almak ve kredi hatları açmak için kolayca kullanılabileceğinden genellikle korunmaktadır (Ohm, 2014, s. 1155). Finans kategorisindeki uygulamalar, çevrimiçi bankacılık kimlik bilgileri, yatırımlar, bütçeler, maaşlar veya kullanıcılarının sahip olduğu varlıklar gibi son derece hassas verileri işler (Belen-Sağlam, Nurse ve Hodges, 2022b, s. 10). Hassas finansal ve ticarî bilgiler, bireylerin ekonomik faaliyetleriyle ilgili kişisel verilerini kapsamaktadır. Kişisel sağlık bilgilerinde olduğu gibi uygunsuz şekilde ifşa edilmesi durumunda bireylerin ekonomik, kültürel veya sosyal kimliğini etkileme potansiyeline sahiptir. Özellikle ekonomik bakımdan finansal ve ticarî hassas bilgiler maddi zararlar oluşturabilmektedir. Kişisel finansal ve ticarî bilgiler, finansal işlem kayıtları, mobil bankacılık ve kredi kartı şifreleri, vergi bilgileri, yatırım portföyleri, iş sözleşmeleri gibi çeşitli hassas bilgileri içermektedir. Bunlara ek olarak bireylerin fikri mülkiyet hakkı kapsamındaki patent, yazılım ve telif hakkı ürünleri de finansal ve ticarî hassasiyet oluşturmaktadır. Finansal ve ticarî bilgiler finans kuruluşları, devlet kurumları, vergi yetkilileri ve ticarî kuruluşlar tarafından ele alınmaya ve incelenmeye tabidir. Bu hassas verilerin gizliliğini ve güvenliğini koruma sorumluluğu, yetkisiz erişim veya veri ihlali risklerini azaltmak için sıkı koruma önlemleri ve düzenlemeler gerektirir.

II.4.1.3. Sosyal ve Özel Hayat Bilgileri

Hassas sosyal ve özel yaşam bilgileri, bireylerin kişilerarası ilişkileri, aile bağları, özel deneyimleri, mahrem alanları ile ilgili kişisel bilgileri kapsamaktadır. Bu bilgiler özel hayatın gizliliğine etki edecek niteliktedir. Bireylere ilişkin medeni durum, boşanma, vesayet hakları, bilinen ve bilinmeyen genetik akrabalarının tanımlanması, aile sırlarını açığa çıkarılması veya aile ilişkilerinin etkilenmesine yol açan toplumsal yaşamda dışlanmışlığa, ayrımcılığa sebebiyet verecek bilgiler hassastır. Sosyal ve özel hayat bilgilerinin gizliliği, bireylerin temel insan haklarını korumak ve kişisel mahremiyetlerini güvence altına almak için kritik bir öneme sahiptir.

Sosyal/kültürel alandaki hassas bilgiler, bireyin bir sosyal organizasyon hakkında veya o sosyal grubun üyelerinden edindiği ve bireyin sosyal organizasyon dışında bilinmemesi gerektiğini düşündüğü bilgileri içerir. Ailede hassas bilgi, aile birimi dışında bilinmeyen bilgi olarak kavramsallaştırılmaktadır. Bu bazen aile sırrı terimiyle karakterize edilebilir. Bilginin ifşa edilmesinin sonucu, öncelikle grup veya kuruluş içindeki ilişkilerin bozulması veya kuruluşun daha yakından, hoş karşılanmayan incelemeye maruz kalmasıdır. Bu bazen güvene ihanet olarak nitelendirilir. Özellikle aile gruplarında sonuçlar, gruptaki diğer kişileri etkileyecek utanç veya damgalanma olabilir. Aile sırları bu açıdan hassas bilgilerin başlıca örneğidir (Thompson ve Kaarst-Brown, 2005, s. 253). Açıklanması yaşayan kişiler veya onların soyundan gelenler için sorun veya tehlikeye neden olacak, bireyler hakkında bilgi içeren belgeler (Andrews, 1998, s. 20) de bu kapsamda değerlendirilmektedir.

II.4.2. Kamu Kaynaklı Bilgiler

Kamu düzenini ve stratejik çıkarları koruyabilmek adına belirli bilgiler saklı tutulmalıdır. Kamuya ait hassas bilgiler, devletin güvenliği, egemenliği, ekonomik ve hukukî yönetim süreçleri, ulusal güvenlik politikaları ve diplomatik ilişkilerine dair kritik verileri

içerebilir. Bu bilgilerin sınıflandırılması ve korunması, başta Bilgi Edinme Hakkı Kanunu ve ilgili kurumların mevzuatı çerçevesinde düzenlenmektedir. Bilgi Edinme Hakkı Kanunu, vatandaşlara şeffaflık sağlarken, kamuya ait belirli bilgilerinin gizliliğini korumaya yönelik istisnalar da getirmektedir. Bu bağlamda kamuya özgü hassas bilgi içerikli belgeler kurumların faaliyet gösterdikleri alanlarda rutin işleyişleri sırasında doğal olarak üretilmektedir.

Diplomatik ve Uluslararası İlişkiler: Uluslararası ilişkilere, kanun ve düzenin korunması dahil olmak üzere ulusal güvenliğe veya ekonomik çıkarlara zarar vermesi nedeniyle ifşa edilmesi kamu yararına olmayacak olan bilgilerdir (Andrews, 1998, s. 20). Uluslararası ilişkiler; egemen devletler, uluslararası örgütler, sivil toplum kuruluşları ve küresel sistemdeki diğer aktörler arasındaki diplomatik ilişkilere, etkileşimlere odaklanmaktadır. Bir ülkenin uluslararası çıkarlarına zarar verebilecek tüm bilgiler, hassas olarak kabul edilebilir. Bilgi edinme hakkı kanunlarında muaf/sınırlı tutulması gereken bir konu olarak işlenmektedir. Diplomatik müzakereler, stratejik müttefiklikler ve uluslararası anlaşmaların gizliliği, devletin uluslararası alanda etkili bir şekilde konumlanmasına ve ulusal çıkarlarını korumasına hizmet eder. Hassas bilgi içeren veya fonksiyonu itibarıyla bütünü hassas olarak kabul edilen istihbarat raporları, askerî planlar önemli toplantıların tutanakları, tarihi bir değeri olan hükümet belgeleri, kamuya açık olması halinde uluslararası ilişkilere zarar verebilecek bilgiler içerebilir. Ayrıca kamu soruşturmaları, genellikle ifşası durumunda ulusal güvenliği, gizliliği veya veri koruma ilkelerini ihlal edecek bilgiler gibi hassas nitelikteki bilgilerle ilgilenir (The National Archives, 2023). Uluslararası ilişkiler hassasiyetleri, genellikle kimin kim hakkında ne söylediğinin bir ürünüdür (McDonald, 2017, s. 451). Diplomatik yazışmalarda kullanılan dil ve içerik de hassas bilgilerin korunması açısından kritiktir. Bir ülkenin diğerine yönelik eleştirel bir dil kullanarak diplomatik bir nota göndermesi veya bir uluslararası toplantılarda iç politikaların sert bir şekilde eleştirilmesi, gizli

bilgilerin ifşa edilmesine veya diplomatik ilişkilerin bozulmasına yol açabilir. Örneğin, ülke liderlerinin birbirlerine yönelik yaptığı açıklamalar, gönderilen mektuplar veya çeşitli yazışmalar uluslararası ilişkilerdeki hassasiyetleri önemli ölçüde etkileyebilir. Yakın dönemde ABD başkanı (45. ve 47. dönem) Donald Trump tarafından yapılan mektup ifşaatı, uluslararası ilişkileri etkileyen ve hükümetlerin uluslararası alandaki itibarına etki eden, yönünü tayin eden bir durum olarak ifade edilebilir. Benzer bir şekilde yabancı hükümetler, AB, NATO veya BM gibi uluslararası kuruluşlar hakkında raporlar veya bunlarla bilgi alışverişi; vatandaşların veya şirketlerinin yurtdışındaki konsolosluk veya ticarî faaliyetlerine ilişkin bilgiler; diplomatik ve siyasî alışverişler sırasında sağlanan diğer devletlerin görüşleri veya niyetleri hakkında bilgiler; devlet ziyaretleri ile bakanlar ve yetkililer tarafından yapılan ziyaretlerin detayları; uluslararası bir mahkeme önündeki mevcut veya potansiyel davalarla ilgili bilgiler (McDonald, 2019, s. 33) gizli ve korunması gereken hassas bilgilerdendir. Ayrıca, merkezi ve yerel yönetimler başta olmak üzere, üst düzey yöneticiler arasındaki yazışmalar ve diplomatik görüşmeler de bu kapsamda değerlendirilmektedir. Bu konuda, ABD'de WikiLeaks tarafından diplomatik yazışmaların sızdırılması ve İran'da nükleer anlaşma müzakerelerinin detaylarının ifşa edilmesi örnek olarak gösterilebilir.

Ulusal Güvenlik ve Savunma: Açıklanması ulusal güvenlik veya diğer gerekçelerle kamu çıkarına aykırı olabilecek bilgiler hassastır. Ulusal güvenlik ve savunmaya dair bilgiler, devletlerin varlığını, toprak bütünlüğünü ve egemenliğini korumak amacıyla kullandığı stratejik, operasyonel ve taktiksel bilgileri kapsamaktadır. Bu bilgiler, devletin askeri kapasitesini, savunma planlarını, kritik altyapılarını, siber güvenlik önlemlerini ve olası tehditlere karşı geliştirdiği savunma mekanizmalarını içermektedir. Özellikle askerî harekât planları, istihbarat raporları ve savunma sanayi projeleri gibi bilgiler, yetkisiz kişilerin kontrolüne geçmesi durumunda devletin güvenlik açıklarını ortaya çıkarabilir veya olası terör örgütleri tarafından istismar edilebilir.

Bununla birlikte, ulusal güvenlik ve savunma bilgileri devletin uluslararası ilişkilerdeki konumunu doğrudan etkilemektedir. 2013 yılında, ABD Ulusal Güvenlik Ajansı'nın (*National Security Agency*) küresel dinleme ve gözetleme faaliyetlerine dair belgelerin bir çalışanı tarafından ifşa edilmesi buna örnek olarak gösterilebilir.[26] Bu tür bilgilerin sızdırılması, ittifakların zedelenmesine ve diplomatik krizlere yol açabilmektedir. Bu sebeple, bu bilgilerin hassasiyetle korunması, devletin güvenlik politikalarının etkin bir şekilde uygulanabilmesi açısından gereklidir.

Hukukî ve Yönetsel: Hukukî ve yönetsel bilgiler, devletin hukuk sisteminin işleyişi, yargı süreçleri, idarî kararlar ve kamu kurumlarının iç işleyişine dair kritik bilgileri kapsayan geniş bir alanı ifade etmektedir. Bu bilgiler, mahkeme kararları, savcılık soruşturmaları, yasal düzenlemeler, idarî yargı süreçleri, kamu ihale süreçleri ve devlet kurumlarının iç denetim mekanizmaları gibi konuları içermektedir. Hukukî bilgiler, adaletin sağlanması ve hukuk devletinin işleyişi açısından büyük önem taşırken, yönetsel bilgiler ise kamu kurumlarının şeffaf, etkin ve hesap verebilir bir şekilde yönetilmesini sağlamaktadır. Ancak, bu bilgilerin yetkisiz kişilerin eline geçmesi veya zamanından önce ifşa edilmesi, ciddi sonuçlar doğurabilmektedir. Örneğin, devam eden bir yargı sürecine ilişkin bilgilerin sızdırılması, adil yargılanma hakkını ihlal edebilir, tanıkların güvenliğini tehlikeye atabilir veya delillerin manipüle edilmesine yol açabilir. Benzer şekilde, kamu ihale süreçlerine dair hassas bilgilerin ifşası, haksız rekabete, yolsuzluklara veya kamu kaynaklarının kötüye kullanılmasına yol açabilir. Ayrıca, devlet kurumlarının iç denetim raporları ve idarî kararlar, kurumların işleyişine dair stratejik bilgiler içerir ve bu bilgilerin sızdırılması, kurumların itibarını zedeleyebilir ve kamu düzenini bozabilir. Bu sebeple, hukukî ve yönetsel bilgilerin korunması, hem hukuk

[26] ABD Ulusal Güvenlik Ajansı çalışanlarından Edward Snowden tarafından yapılan ifşaata ilişkin bkz. BBC Türkçe (2025, Şubat 9). https://www.bbc.com/turkce/articles/cgr608rdd42o

devletinin sağlıklı işleyişi hem de kamu yönetiminin etkinliği açısından büyük önem taşımaktadır.

Ekonomik ve Ticarî: Ekonomik ve ticarî bilgiler, devletin ekonomik istikrarını, büyüme dinamiklerini ve uluslararası rekabet gücünü doğrudan etkileyen stratejik verileri içermektedir. Bu bilgiler, hükümetin ekonomi politikalarına ilişkin kararları, kamu kaynaklarının dağılımı, vergi sistemine dair detaylar, dış ticaret verileri, yatırım projeleri, finansal piyasalara yönelik düzenlemeler ve devlet destekli ekonomik girişimler gibi geniş bir yelpazeyi içermektedir. Ekonomik ve ticarî bilgilerin korunması, devletin ekonomik egemenliğini sürdürmesi ve piyasa istikrarını sağlaması açısından kritik öneme sahiptir. Özellikle, henüz kamuoyuna açıklanmamış ekonomik politika kararları veya finansal düzenlemeler, erken ifşa edildiğinde piyasalarda spekülasyonlara, sermaye kaçışına veya ekonomik istikrarsızlığa yol açabilmektedir. Benzer bir şekilde, devletin yatırım projelerine veya stratejik sektörlere dair detaylar, rakip ülkeler veya uluslararası şirketler tarafından kullanılarak ülkenin rekabet gücü zayıflatılabilir. Ticarî sırlar ve patent bilgileri gibi ekonomik veriler de, devletin himayesi altında korunması gereken bilgiler arasındadır; zira bu bilgilerin sızdırılması, şirketlerin rekabet avantajını kaybetmesine ve ulusal ekonominin zarar görmesine yol açabilir. Ayrıca, uluslararası ticaret anlaşmaları ve müzakerelere dair bilgiler, zamanından önce veya usulsüz olarak ifşa edildiğinde ülkenin pazarlık gücünü zayıflatabilir ve diplomatik ilişkileri olumsuz etkileyebilir. Bu sebeple, ekonomik ve ticarî bilgilerin korunması, hem devletin ekonomik çıkarlarını korumak hem de piyasa güvenini sağlamak açısından faydalı olacaktır.

II.4.3. İhtisas Alanı ve Sektör Bilgileri

Bilginin hassasiyeti belirli bir uzmanlık alanına bağlı olarak değişebilir. İhtisas alanı bilgisi, genel veya temel bilginin ötesine geçen belirli bir alan, konu veya etki alanı

hakkında derin ve ayrıntılı bir anlayış anlamına gelir. Yalnızca bir kuruluş veya ihtisas alanı içinde kullanılması amaçlanan bilgileri kapsamaktadır.

Bilginin hassasiyetine ilişkin yargılar, bilginin değerine dayanmaktadır. Ekonomik araştırmalar ekonomik temelli bir bilgi görüşünün anlaşılmasını sağlamıştır. Bu bakış açısına göre hassas bilgi, bu bilgiyi kontrol eden kişi, grup veya kuruluş için olumlu bir sonuç olasılığını artırmak veya gelecekteki eylem veya karar seçeneklerini korumak veya artırmak için korunan bilgidir (Thompson ve Kaarst-Brown, 2005, s. 251). Bu bilgi her ihtisas alanında ve faaliyet gösterilen sektöre göre değişkenlik göstermektedir. Bilimsel araştırma faaliyeti gösteren eğitim kurumlarında öğrenci dosyaları, devam eden araştırmaların verileri; kurumsal ticarî işletmelerde ticarî sırlar, fikri mülkiyet, pazar ve satış bilgileri, yeni ürün stratejisi, formüller, terkipler, tedarik bilgileri, güvenlik açığı raporları, işyeri soruşturmaları, disiplin işlemleri veya çalışan ilişkileri hakkında bilgiler; imalat ve mühendislik çalışmalarında ürünler, üretim süreçleri için hazırlanan plan ve tasarımlar; pazarlama ve reklamcılık alanında müşteri verileri, pazarlama stratejileri; tıp ve sağlık alanında hasta kayıtları, halk sağlığı verileri ve stratejileri, ar-ge verileri (ilaç formülasyonları, klinik denemeler vs.) çeşitli ihtisas alanı ve sektörlerdeki hassas bilgilerden bazılarıdır. Bu örnekler çoğaltılabilir olmak ile birlikte zamanla farklı hassasiyetlerin ortaya çıkması da muhtemeldir. Daha önce belirtildiği üzere hassasiyet yargısının verilebilmesi için bir risk durumunun ortaya çıkma ihtimalinin var olması gerekmektedir. Risk değerlendirmesinin tespiti ve kararı bazı alanlar veya tematik soyutlamalar için sınırları çizilebilir bir durumdur. Fakat her alan için bu mümkün değildir.

Bir ticarî işletmedeki gizli bilgilerin gizliliğinin korunması, işletmelerin rakiplerine karşı avantaj elde edebilmeleri ve bunun sonucunda daha yüksek kar elde edebilmeleri için önemlidir (American Board…, 2016, s. 11). Kuruluşlar tarafından kullanılan ve paylaşılan hassas bilgiler, iş akışlarının etkinliğini güçlendirir. Üretim

maliyetleri, yeni bir ürün serisinin başlatılması gibi gelecek pazar stratejisi, yeni bir sermaye ekipmanı satın alınması gibi büyük üretim değişiklikleri hakkında bilgiler hassastır (Kleiner ve Bouillon, 1991, s. 484). Bu bilgiler, firmaların satın alma ve alışveriş alışkanlıklarına uygun ürün ve hizmetleri uyarlayarak müşterilerine daha fazla kolaylık sağlamalarına olanak tanırken işletmeler için en hassas konular arasında yer almaktadır. İşletmelerdeki yeni ürünlere ilişkin verilerin ifşa edilmesinin, firma stratejisi ve politikasının bu önemli alanında rakiplere avantaj sağlayabilme ihtimali yüksektir.

Hassas bilgi teorisine dair belirtilen bilgi türleri, hassas bilgi sınıflaması yaklaşımlarının kapsamını ve sınırlılığını belirlemede kesin yeterlik iddiası taşımamaktadır. Bu çalışma kapsamında kamu ve özel yapıdaki kurumların üretmiş olduğu belgelerde yer alması muhtemel hassas bilgi türlerine odaklı bir bakış açısı ile bu sınıflandırmaya başvurulmuştur. Sayılan türlerin dışında da farklı hassasiyetler, teknolojik gelişmeler ve sosyal hayattaki yenilikler doğrultusunda her geçen gün artış göster-mektedir/ecektir. Örneğin kesin konum (coğrafî) bilgileri, iletişim üst verileri (web taraması, tarama geçmişi, IP adresi vb.), teknolojik gelişmelerin ortaya çıkarmış olduğu yeni hassasiyetlerdendir. Teknolojinin sunmuş olduğu imkânlar, hassas ve gizli tutulması gereken bilgilere olan bakışı da değiştirmiştir. Bir IP adresini web aramaları gibi diğer bilgilerle ilişkilendirerek bir bireyi tanımlamak mümkün olduğunda, belirli bağlamlarda kişisel veri olarak kabul edilmesi lehine bir argüman vardır. Web aramalarından elde edilen bilgiler, bir bireyin uygulamaları, tercihleri ve inançları hakkında son derece hassas bilgileri ortaya çıkarabilir (OECD, 2013, s. 97). Bu konudaki en dikkat çekici örneklerden biri, dijital ortamda mahremiyet ve gizlilikle ilgili artan kaygılar sonucunda ortaya çıkan "unutulma hakkı" kavramıdır. Çünkü bireylerin, üçüncü taraflara kendi başına kişisel olabilen veya başka verilerle birleştirilip analiz edildiğinde hassas kişisel bilgileri açığa çıkarabilecek veriler sağlamadan dijital ortama katılması artık mümkün değildir (OECD, 2021, s. 20). Bu bağlamda, bir İspanyol vatandaşının kişisel bilgilerinin korunmasıyla

ilgili alınan dönüm noktası niteliğindeki bir karar dikkat çekicidir. Söz konusu kişi, 1998 yılında gazetede yayımlanan ve sosyal güvenlik borçlarını kapatmak amacıyla hacizli evinin açık artırma ilanını içeren bir haberin Google arama sonuçlarında listelenmeye devam ettiğini fark etmiştir. Ancak, ilgili işlemler yıllar önce tamamlandığından ve haberin güncelliğini yitirdiğinden, bu durumun gizlilik haklarını ihlal ettiğini belirterek şikâyette bulunmuştur. Gazetede kişisel verilerinin görünmemesi için sayfaların kaldırmasını veya değiştirmesini, Google'dan da arama sonuçlarında artık görünmemesi için kişisel verilerini kaldırmasını talep etmiştir. Konu çeşitli yargı süreçlerinden geçtikten sonra AB Adalet Divanı Google'ın İspanyol vatandaş tarafından ilgisiz görülen bilgilere erişimi silmesini gerektirdi, ancak temel gazete arşivinin içeriğinin veri koruma adına değiştirilmesi gerektiğine hükmetmemiştir (European Commission, 2014). Gazetenin ilgili haberi kurumun arşivinin bir parçasını oluşturmaktadır. Dolayısıyla veriler üzerinde oynama, silme, değiştirme vb. tahribat ve tahrifat işlemlerinin yapılması uygun değildir.

Gizlilik ve hassasiyet, gelişmelere bağlı olarak değişkenlik gösterirken hangi bilgilerin hassas olarak kabul edildiği genellikle mevzuat düzenlemelerinde sayılma yoluyla yer almaktadır. Fakat bir kanun uyarınca hassas olarak kabul edilen bilginin, başka bir düzenlemede hassas bilgilere örnek olmadığı veya tersinin de geçerli olduğu durumlar olabilmektedir. Özellikle bu farklılık, sosyal kültürel normlar çerçevesinde toplumlara göre değişmektedir. Mevzuat – hangi gizlilik yasası incelendiğine bağlı olarak – genellikle endişe duyulan bilgileri hassas olarak kabul ederek toplumdaki hassas bilginin kapsamını ve sınırlarını belirlemektedir.

III. BÖLÜM: HASSAS BİLGİ İÇERİKLİ KAMU BELGELERİ

A Glossary of Archival and Records Terminology'e göre (Pearce-Moses, 2005, s. 357) "potansiyel olarak utanç verici olan, bireylerin gizli tutulmasını bekleyebileceği, kamu denetiminden korunması gereken yasal, malî veya kişisel nedenlerden dolayı gizlilik içeren bilgiler" hassas olarak ifade edilmektedir. *Dictionary of Archives Terminology*'e göre kamu incelemesinden/denetiminden korunması gereken kişisel veya gizli ya da kişilerin özel tutulmasını bekleyebileceği, potansiyel olarak utandırıcı bilgiler hassas olarak tanımlanmaktadır (Society of American Archivists, 2024). Hassas kavramı, gizlilik (*classified*) kapsamına giren çoğunlukla aynı durumu karşılayan bir terim olarak kullanılmaktadır. Gizlilik, "belirli bilgi veya belgelere yüklenen ve böylece onlara erişimi sınırlayan veya özel hayata saygı gerektiren durum ya da hükümet tarafından devlet güvenliğinin korunması amacıyla belirli belgelere, içeriklerine ve kullanımına getirilen kısıtlama" olarak ifade edilmektedir (Belge Yönetimi ve Arşiv Terimleri Sözlüğü, 2009, s. 23). Bir diğer gizlilik tanıma göre "hukukî, idarî, ticarî veya özel hayata ilişkin nedenler veya olağanüstü hallerde içerdiği bilgi/ veri nedeniyle belge/materyal, yayın, kayıt ortamı veya belge grubuna erişimi sınırlayan durum, mahremiyet" olarak ifade edilmektedir (Arşiv Terimleri, 2023, s. 65). Birçok kamu belgesi çeşitli niteliklerde gizli veya hassas bilgiler içermektedir. Bireylerin kamu kurumları ile etkileşimleri, toplumsal yaşamın ayrılmaz bir parçasını oluştururken, bu etkileşimler sıklıkla kamu kurumları tarafından üretilen belgelerin içeriğine de yansımaktadır. Kamu kurumları, doğal faaliyetlerini yürütürken işlevlerinin ve hizmetlerinin niteliğine bağlı olarak çeşitli hassas bilgiler içeren belgeler üretebilir veya bu bilgileri kullanabilir. Örneğin, vatandaşların kamu hizmetlerine başvuruları, vergi ödemeleri, kurum içi-kurum dışı resmî yazışmalar ve diğer çeşitli talepler, kamu kurumlarının ürettiği belgeler aracılığıyla şekillenir. Bu belgeler, bireylerin özel hayatına dair çeşitli bilgiler içerebilir ve bu nedenle hassas bilgi içerikli belge varlığı, mahremiyet haklarının korunması, hukukî süreçlerin izlenmesi ve

kamu kurumlarının şeffaflığı açısından kritik bir öneme sahiptir. Mahremiyet, kişisel bilgi içeren belgelere erişim menfaatini korumayı amaçlarken, şeffaflık hükümet bürokrasisini kamu denetimine açma çabasını içerir.

Kamu kurumları ve devlet arşivleri, kendi gözetimleri altında bulunan hassas bilgilere erişim hizmeti sağlamakla ve aynı zamanda hassasiyet oluşturan kişisel bilgilerin haksız yere ifşa edilmesini önlemek zorundadır (Whorley, 2006, s. 12). Kamu belgelerinin genellikle hassas içerikli bilgiler içermesi yaygın olarak kabul edilir. (Ohm, 2014, s. 1160). Bir kişi ehliyet aldığında, trafik cezası aldığında, oy kullanmak için kayıt yaptırdığında veya evlendiğinde ya da boşandığında resmî bir belge düzenlenmektedir. Benzer şekilde, bir kolluk kuvveti, istihdam amacıyla veya gizli bir pozisyonda görevlendirilecek bir aday hakkında güvenlik soruşturması yürütebilir. Bu tür işlemler, hukukî sorumluluklar, haklar ve yükümlülükler doğurduğundan, kamu kurumları belirli belgeleri incelemekte ve muhafaza etmektedir. Örneğin, adlî makamlar suç geçmişi, tutuklama ve mahkeme kayıtlarını saklarken, eğitim kurumları bireylerin akademik geçmişine ilişkin belgeleri arşivlemektedir. Sosyal yardım hizmeti sunan kuruluşlar, yardım alanlar ve bağışçılar hakkında veri toplarken, sağlık kurumları hastaların tıbbî geçmişlerini ve genetik bilgilerini teşhis ve tedavi süreçlerinde kullanmaktadır. Güvenlik birimleri, kimlik doğrulama ve suç önleme amacıyla biyometrik verileri işlerken, vergi daireleri mükelleflerin finansal kayıtlarını denetim ve tahsilat için analiz etmektedir. Öte yandan, aile toplumun en özel birimi olmasına rağmen, aile bireyleri arasındaki bazı hukukî işlemler de resmî kayıtlara geçmektedir. Tüm bu süreçler, bireylerin doğal faaliyetleri sonucunda hassas verilerin kamu kurumlarıyla paylaşılmasını gerektirmekte ve bu durum, mahremiyet hakları ile kamu yararı arasındaki dengenin titizlikle korunmasını zorunlu kılmaktadır.

Kişilerin kamu kurumları ile olan etkileşimlerinin yanı sıra kurumlar da hassasiyet içeren faaliyetlerde bulunmaktadır. Kamu kurumları – özellikle savunma ve güvenlikle

ilgili olanlar – ulusal güvenlik plan ve stratejilerinin geliştirilmesinde, potansiyel risk ve tehditlerin oluşturulmasında yer alırlar. Kurumsal yapı gereği Dışişleri Bakanlığı gibi bir kamu kurumu, ulusal güvenlik, dış ilişkiler, diplomatik faaliyetler ve uluslararası iş birliği gibi konularda faaliyet gösterdiğinden çeşitli hassas içerikli bilgiler ve belgeler tutabilir.

Kamudaki belge üretimi – kayıt ortamı fark etmeksizin – kurumsal bilgi yönetiminin sürdürülebilmesi için devam etmektedir. Bu süreçte hassas bilgi içerikli belgelerin üretilmesi, kullanılması ve muhafaza edilmesi kaçınılmaz bir gerçekliktir. Kamu belgeleri güncel ve yarı güncel kullanım zamanlarını doldurduktan sonra arşivsel değer ölçütlerini taşıması durumunda arşiv belgesi olarak korunmaktadır. Son işlem tarihi üzerinden yirmi yıl geçmiş veya üzerinden on beş yıl geçtikten sonra kesin sonuca bağlanan, çeşitli arşiv değerine sahip belgeler, arşiv belgesi vasfını kazanmaktadır (Devlet Arşiv Hizmetleri…, 2019, 4/1.a). Bu süre çoğu Avrupa ülkesinde 20 yıl olarak belirlenmiştir. Arşiv belgesi ile ifade edilmek istenen sadece fiziksel ortamda üretilen kurumların en çok kullandığı kâğıt belgeler değildir. Hassas bilginin varlığı sadece yazılı belgelerde yer alan sözcüklerin taşımış olduğu hassasiyet için geçerli değildir. Belge niteliğinde olan fotoğrafik, kartografik, film görüntüsü ve ses kaydı gibi elektronik ve fiziksel ortamda yer alan her türlü bilgi taşıyıcıları da hassasiyet unsuru içerebilmektedir. Özellikle hassas bilgi içeren görsel-işitsel materyallerin değerlendirilmesi zorlayıcı olabilmektedir. Görsel-işitsel materyallerin analiz edilmesi genellikle daha fazla personel zamanı ve çaba gerektireceğinden – transkribe edilen bir metin olmadığından dolayı – değerlendiricilerin içeriği izlemesi/dinlemesi gerekmektedir (Whyte ve Walsh, 2024, s. 13). Bununla birlikte fotoğraf, resim, harita ve planların da dikkate alınması gerekir. Bir fotoğraf, altyazılarla veya üst veriler ile etiketlenmemiş olsa bile, bireyin kimliğinin tespit edilmesine yardımcı olabilir. Her durumda, görüntülerinin kullanıma sunulmasının insanlar üzerindeki olası etkisi dikkate alınmalıdır. Fotoğrafların genellikle özel kişisel veri kategorilerine dahil edildiği unutulmamalıdır. Tıbbî tedavi gören kişiler, tutuklanan

kişiler, sendika gösterilerine katılanlar fotoğraflarda yer alabilmektedir. Fotoğraflar dışında ilk bakışta kişisel verileri içermeyecek belgelere de dikkat edilmelidir. Örneğin haritalar ve planlar bilirkişinin veya mimarın adını içerebilir (The National Archives, 2018, s. 34). Bunun dışında ses örneklerinin de ırksal veya etnik kökeni ortaya çıkarması muhtemeldir. Irk veya etnik kökeni ortaya çıkaran biyometrik verilerin toplanması ve işlenmesi, etnik ve dinî gerilimlerin hüküm sürdüğü bölgelerde özellikle hassas olmaktadır (Kindt, 2016, s. 322).

Arşiv belgeleri, insanların kamusal ve özel yaşamları hakkında bilgiler içermektedir. Geçmiş yıllarda bazı arşivler, araştırmacıların kullanımına sunulan belgelerin hassas bilgi içermediğinden – ve bu bilgileri kullanmalarına engel olmak – emin olmak amacıyla araştırmacıların [kullanım sonrası] notlarını incelemeyi tercih etmiştir. Kullanıcılar hassas bilgileri not etmeseler bile hatırlayabileceğinden bu yöntem çözüm olmamıştır. Belgelerin taranması ve hassas bölümlerinin araştırmaya kapatılması, daha güvenilir bir yöntem olmuştur (Pugh, 1992, s. 58). Bu durumda kamu belgelerini yönetme ve arşivlemenin amacı öncelikle bu bilgileri, bireyler ve kurumlar üzerindeki potansiyel etkinin düşük olduğu veya hiç olmadığı çok uzun vadeli kullanım için tutmaktır. Hassas bilgi içeren belgeler süreli veya süresiz saklama kararları esasınca kurum arşivinde veya ulusal arşivde muhafaza edilmektedir. Bir arşiv kurumunun üstlendiği iki temel görev vardır: koruma ve erişilebilirlik. Arşiv belgelerinin muhafazası geçmişin korunmasını sağlarken, erişilebilirlik de kullanıcıların bu geçmişi hatırlanmasını sağlamaktır. Arşivcilik hizmet ve faaliyetleri arasında kişisel bilgilerin gizliliğini korumak, arşiv belgelerinin gizlilik derecelerini belirleyerek bilgi ve belge güvenliğini sağlamak yer almaktadır (Rukancı, Anameriç ve Başar, 2021, s. 34). Arşivler ve arşivciler belgeleri oluşturan veya belgelere konu olan kişi ve toplulukların mahremiyetine saygı duymalıdır (Association of Canadian Archivists, 2017, s. 3). Ancak, kurumlar ve çoğu zaman ulusal arşivler belgeye erişim hizmeti sunarken gizlilik hususu

bir engel olarak ortaya çıkmaktadır. Kamuoyu tarafından bilinmemesi gereken hassas içerikli belgeler erişime açıldığında ne olur? Bu durum, kamuyu olası yasal işlemlere kadar uzanan maddi ve manevi sonuçlara/sorunlara maruz bırakarak kurumları zor durumlar ile karşı karşıya getirebilir. Sonuçlar ne kadar ciddi olursa olsun, hem gizliliği korumanın hem de erişilebilirlik misyonuna sadık kalmanın kolay bir yolu hassasiyet temelli olarak zor bir süreçtir. Bu konuda IFLA (International Federation of Library Associations) ve ICA (International Council on Archives) hükümetlere ve karar vericilere ortak bir bildirimde bulunarak arşiv belgelerine hâlihazırda erişimin teşvik edilmesi gerektiği, ancak kişisel mahremiyeti, gizliliği, kültürel hassasiyetleri korumak veya meşru güvenlik kaygılarını gidermek için gerektiğinde istisnaların uygulanmasına izin verilebileceği tavsiyesinde bulunmuştur (IFLA-ICA Statement…, 2020).

Güncel ve hassas materyallere erişimde bazı kısıtlamaların olmaması bireylere zarar verebilir (Pugh, 1992, s. 56). Kamu belgeleri, kişisel veya kamusal mahremiyet-gizlilik ilkeleri esasınca hem güncel hem de arşiv belgesi vasfı kazandığı dönemde hassasiyet değerlendirmesinden geçmesi gerekmektedir. "Belge yönetimi aşamasında yapılan değerlendirmede belgeler aktif halde olduğundan üretim ve kullanım amaçları, yasal dayanakları değerlendirilebilir, birim personeli ve uzman görüşleri alınabilir" (Rukancı, Anameriç ve Başar, 2021, s. 46). Bu sebeple değerlendirme işlemi, arşivsel bir süreç olan "değerlendirme" safhasına göre sadece güncelliğini kaybetmiş arşivlik malzemeler için değil, ayrıca üretim süreciyle birlikte dolaşımda bulunan güncel ve yarı güncel durumdaki belgeler için de uygulanarak bütüncül bir yaklaşım benimsenecektir.

III.1. Hassasiyet Değerlendirmesi Yöntem ve Süreci

Belge yönetimi ve arşivcilik terminolojisine göre değerlendirme (*appraisal*), diğer tüm işlevlerin bağlı olduğu, birincil arşiv işlevidir ve bu nedenle dikkatli düşünmeyi gerektirir (Johns, 2017, s. 32). Erişim eşittir değerlendirme (Reed, 2014, s. 127) olarak ifade

edilmektedir. Doğru yürütülen değerlendirme süreci, kamu ve kişi hakları gözetilerek gerekli kısıtlamalar veya kapatma kararları dikkate alınarak erişim öncelik esasına dayalı olarak gerçekleştirilir. Değerlendirme, belgelerin üretilmesi ve güncel kullanım sürecindeki görevini tamamlamasıyla birlikte başlamaktadır. Bu süreç tekrar kullanım değerine sahip, arşiv değer ölçütlerini karşılayan belgelerin arşivlenmesi sürecidir. Değerlendirme, ayıklama ve imha işlemleri, belge üretici kurum ve kuruluş yetkilileri ile arşivcilerin birlikte yönettikleri belki de arşivcilikte sorumluluk düzeyinin en yüksek ve kritik olduğu faaliyettir. Zira bu faaliyette gizlilik, erişim ve saklama sürelerini negatif yönde etkileyecek yanlış kararlar, telafisi mümkün olmayacak sonuçlar doğurabilir (Rukancı, Anameriç ve Başar, 2021, s. 45). Değerlendirme yaklaşımları, tüm belgeler için geçerli olmakla birlikte, kabul edilmelidir ki kişisel bilgi içeren veya çeşitli sebeplerden ötürü hassasiyet oluşturan belgeler/dosyalar bir araya getirildiğinde [ayrı bir sorundur] ve özel muamele gerektirir (Cook, 1991, s. 6). Dolayısıyla hassas bilgi içeren bu tür belgelerin değerlendirilmesi, "değerlendirme" sürecinin bir parçası olmakla birlikte ayrı bir odak noktasını oluşturmaktadır. Bu işleme, hassasiyet değerlendirmesi (*sensitivity review*) veya incelemesi süreci denilmektedir. Hassasiyet değerlendirmesi, Kamu belgelerinin, kamuya veya bireylere yönelik itibar, mahremiyet ve güvenlik gibi potansiyel risklerini belirleme, analiz etme ve bu riskleri etkili bir şekilde değerlendirme sürecidir. Belgenin entelektüel içeriği ile ilgilenen bir yön olması sebebiyle değerlendirme ve hassasiyet değerlendirmesinin birlikte yapılması önerilmektedir (Sloyan, 2016, s. 31). Hassasiyet değerlendirmesinin ayrı bir iş olarak yürütülmesi arşivsel değere sahip belgelere uygulanacak saklama sürelerine doğrudan etki edecektir. Bu sebeple hassasiyet değerlendirmesi arşivsel değerlendirme süreçleri içerisinde yapılandırılmış bir faaliyet olarak düşünülmektedir. Kurumların ulusal arşive belge transferi öncesinde kurum içi istişarede bulunarak hassasiyet değerlendirmesi yapması gerekmektedir. Hassasiyet değerlendirmesinin amaçları aşağıdaki gibidir:

a) Bilgi ve belgelerin arşiv hizmetine sunulmadan kurumda/birimde tutulup tutulmayacağını değerlendirmek,
b) Birden fazla Bilgi Edinme Hakkı muafiyetinin geçerli olduğu durumlarda belgelerin transfer sürecinde kapatılıp kapatılmayacağını değerlendirmek,
c) Bilgi muafiyeti bulunan belgenin kamu yararına açıklanması gerekip gerekmediğini değerlendirmek ve
d) Bilgi Edinme Hakkı muafiyeti olmayan bilgi ve belgeleri teyit etmektir (The National Archives, 2015, s. 18).

Hassasiyet değerlendirmesi sürecindeki ilk adım, ulusal arşive devredilmeden/transfer edilmeden önce potansiyel olarak hassas bilgi içeren belge ve belge gruplarının tespit edilmesidir. Bu süreci daha geriye götürmek gerekirse belge yönetimi safhasında gizlilik derecesinin verilmesi ile başlamaktadır. Hassas bilgi içeren belgelerin belge yönetimi döneminde gizlilik derecesinin doğru seçilmesi, süreçlerin verimli ve şeffaf bir şekilde yürütülmesini, hesap verilebilirliği artırmayı ve bilgi taleplerinin düzgün bir şekilde karşılanmasını sağlar. Yanlış gizlilik derecelendirmesi ise süreçlerde gecikmelere, artan maliyetlere ve güvenlik ile hak ihlallerine neden olabilir (Kaymak ve Külcü, 2024, s. 22). Ancak hassasiyet değerlendirmesi, gizlilik derecesi[27] verilen belgelerin transfer sürecinde ve arşiv döneminde uygulanan bir işlem olduğundan öncesinde yapılan işlemler etkili olmak ile birlikte temel işlemler transfer ve devam eden süreçte uygulanmaktadır. Hassas bilgiler, edinim/transfer ve işleme sürecinde tanımlanarak ayrılmalıdır (Pugh, 1992, s. 64). Bu süreç belge, dosya, seri, fon düzeyinde hassas bilgi taşıma riskinin değerlendirilmesini içerebilir. Bazı durumlarda, risk düşük olacaktır ve kurum, bu yargıyı doğrulamak için biraz örnekleme ile ayrıntılı sayfa sayfa

[27] Hassas bilgi/veri içeren belgelerin yönetimi gizlilik yönetiminin bir parçası olduğundan gizlilik derecesine sahip belgelerde olduğu gibi bir yönetim [gönderme-kayıt-erişim-imha-devir] ile yürütülmektedir. Ancak bu işlemler bilginin kayıtlı olduğunu ortama göre farklılık göstermektedir.

incelemenin gerekli olmadığına karar verebilir (Allan, 2014, s. 14). Bazı durumlarda fonun tamamen kapalı olacağı yargısına varılabileceği gibi belge ve dosya düzeyinde kısıtlamalara da gidilebilir. Örneğin belirli belgenin veya belge grubunun tamamı, hassas olduğu kabul edilene kadar saklanabilir veya kapatılabilir (McDonald, 2019, s. 2). Hassasiyet değerlendirmesi yapılamayan herhangi bir belgenin ihtiyati kapatmaya tabi olması muhtemeldir, yani hassas bilgilerin ihmalkârlığa yol açma ve potansiyel olarak yasa dışı olabilme ihtimalinin bulunması sebebiyle kamuya açıklanmayacaktır. Ayrıca, hassas bilgi içeren incelenmemiş belgelerin ve bu bilgilerin kamuya açıklanması yoluyla zarara yol açma riski çok fazladır (Sloyan, 2016, s. 30; McDonald, 2019, s. 52). Hassas veya gizli belgeler içeren birçok arşiv kurumu, bu belgelerin potansiyel yayılma endişesi nedeniyle erişimi tamamen kısıtlama seçeneğini tercih etmektedir (Jaillant, 2022b, s. 427). Fakat bekleme süresinin uzaması ve ihtiyatlı kapatmaların artması belge grubunu atıl duruma getirerek erişim misyonuna zarar verecektir. Bu sebeple hassasiyet değerlendirmesi, hızla yürütülmesi gereken bir süreçtir.

Bazı kurumlarda hassas bilgi türlerini içeren az sayıda belge vardır ve bu nedenle hassasiyet değerlendirmesine sınırlı olarak ihtiyaç duyulmaktadır. Dolayısıyla bu kurumlarda yapılacak hassasiyet değerlendirmesi, kümülatif birikimin oluştuğu süreçte daha çok uygulanacaktır. Böylelikle belge üreticileri hassas bilgi içeren belgeleri transfer öncesi düzenleyerek söz konusu belge grubuna erişim hususundaki potansiyel riski azaltacaktır (Jaillant ve Rees, 2023 s. 576).

Hassasiyet değerlendirmesi, yoğun emek, deneyim ve muhakeme gerektiren bir süreçtir. Bu sebeple hataların meydana gelmesi kaçınılmazdır. Değerlendirme süreci boyunca değerlendiricilere (arşivci, belge yöneticisi), birimlerin veya kurumun çıkarlarıyla ilgili dikkat edilmesi gereken konular hakkında ayrıntılı rehberlik sağlanması gerekebilir. Değerlendiriciler belgeleri hassasiyet açısından incelerken hem birim içinde hem de hassasiyet incelemesi kararından etkilenebilecek diğer birimlerle (Örneğin,

bilgiyi ilk olarak sağlayan veya konunun uzmanı olan birimler) yeterli istişarenin yapıldığından emin olmalıdır (The National Archives, 2021a, s. 4). Değerlendiricinin belge içeriğinde denk geldiği sorun başka bir birimle ilgili olması durumunda, diğer birime danışılır ve incelenmesi için dosyalar gönderilir (Allan, 2014, s. 15). Değerlendirme sürecinde, hem kurum hem de ulusal arşivdeki değerlendiricilerin uzmanlık alanlarına ve tercihlerine uygun olarak belgelerin atanması, hassas bilgilerin daha kolay tespit edilmesine olanak tanır. Bu yaklaşım, gözden geçirenlerin hangi bilgilerin hassas kabul edilmesi gerektiği konusunda daha bilinçli kararlar vermelerini sağlayabilir (Narvala, 2024, s. 6). Bu kapsamda ulusal arşivlerde ihtiyaç duyulması halinde kurumlar ile hassasiyet konusunda fikir alışverişi yapan, otorite bir danışma kurulunun oluşturulması gerekli olabilir. Bazı ulusal arşivlerde[28] bu tarz yapılanmalar mevcuttur. Belge içeriği konusunda uzman bilgisi olan araştırma personeli hassasiyetler konusunda tavsiyelerde bulunabilir ve inceleme sırasında bu personele danışılması gerekir. Hassasiyetin tespit edildiği durumlarda, personel hangi bilgilerin düzeltileceğini, hangi hassasiyetlerin uygulanacağını ve bilgilerin kapatılması muhtemel olduğu süreyi belgelemelidir (The National Archives, 2023).

Hassas olduğuna karar verilen bir belge veya belge grubu ile ilgili; tespit edilen hassasiyet kategorisi, hassasiyetin hangi bölümlerde (Örneğin cümleler veya paragraflar) yer aldığı; bilgilerin neden hassas olduğu ve bu nedenle kapatılması gerektiğine dair açıklama veya gerekçenin (McDonald, 2019, s. 2) ifade edilmesi beklenmektedir. Hassasiyeti gözden geçiren kişinin bir belgeyi incelerken, belge içerisindeki tüm hassas bilgilere açıklama eklemelidir. Ancak açıklamaların da hassasiyet ihlaline sebebiyet vermemesi gerekir. Örneğin belgede yer alan bir isim hassas olmakla birlikte dosyanın seçilme nedeninin merkezinde yer alıyorsa ve açıklamada yer alması gerekiyorsa, belge

[28] İngiltere, ABD, Avustralya, İrlanda vb. pek çok ulusal arşivde danışma konseyi (*advisory council*), danışma kurulu (*advisory board*) veya danışma komitesi (*advisory committee*) gibi çeşitli uzmanlık alanından kişilerin yer aldığı birimler oluşturulmaktadır. Bu yapılar gizlilik ve hassasiyet konularında tavsiyelerde bulunmaktadır.

kapalıyken açıklama saklanmalı veya redakte edilmelidir. İsmin açıklamaya dahil edilmesi gerekmiyorsa ve açıklamanın yayınlanmaması için başka bir neden yoksa, açıklama herkese açık olabilir. Hassas dosyaya ilişkin açıklama yaparken; dosyanın kamuya açık-kapalı olma durumu, bilgilerin yayınlanmasına ilişkin yasal kısıtlamaların olup olmadığı, açıklamada kişisel bilgilerin yayınlanmasının gerekliliği ve veri sahibine sorun oluşturma veya zarar verme ihtimali gözetilmelidir. Eğer ilgili kişi kendisiyle ilgili bilgiyi kamu malı[29] haline getirmişse, arşiv hizmetlerinin bu bilgiyi ifşa etme konusunda haklı olma ihtimali yüksektir. Ancak, bilginin bir zamanlar kamuya açık olması – örneğin yerel bir alanda ve bunun bir süre önce gerçekleşmiş olması – daha fazla dağıtım adil olmayabileceğinden arşiv tarafından ifşa edilmesi için tek başına bir gerekçe değildir. Bu sebeple bir risk değerlendirmesi yararlıdır (The National Archives, 2018, s. 30-31).

Hassas bir belgenin değerlendirme işlemi çok sayıda açıklama içerebilir. Açıklamaların boyutu tek bir terim ile belgedeki tüm terimler arasında değişkenlik gösterir. Tek bir belgenin emsal olarak kabul edilerek dosya ve ilişkili serilerin etkilenmesi de olağandır. Tek bir terimden veya kişiden dolayı belge veya belge grubu yüksek derece hassasiyet taşıyabilir. Bu süreçte hassasiyet kategorilerine dair sınıflama veya kodlama numaralarının oluşturulması kullanım kolaylığı ve hızlı üst veri bilgisi sağlamak amacıyla gerekli olabilir. Ayrıca hassasiyetin derecelere ayrılması (Örneğin: düşük, orta, yüksek veya 1,2,…,5), belge üzerinde redaksiyon, maskeleme ve kapatma kararlarının uygulanmasını kolaylaştıracaktır. Gizlilik veya hassasiyet dereceleri-kategorileri hangi düzeyde olursa olsun arşivlerde üzerinde titizlik ve hassasiyet

[29] Kişilerin kendilerine ait verileri kamuya açık hale getirmesi/alenileştirmesi KVKK'nın 5/2-d bendinde "İlgili kişinin kendisi tarafından alenileştirilmiş olması" kaydıyla işlenebileceği ifade edilmektedir. Örneğin veri sahipleri kitle iletişim araçlarında, sosyal çevresi ile kurduğu iletişimlerde veya kayıtlı kamu belgelerinde dinî tercihini, cinsel yönelimini ya da sağlık durumuna ilişkin açıklamalarını paylaşabilir. Ancak bu bilgilerin alenileştirilmiş olması ilgili mevzuat kapsamında işlenme gerekliliğe bakılmadan işlenebileceği anlamına gelmemektedir. Nitekim 32487 sayılı 12 Mart 2024 tarihli "Ceza Muhakemesi Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun" un 33/3-ç bendinde "İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması" şartıyla özel nitelikli verilerin işlenebileceği belirtilerek bu durum mevzuat ile garanti altına alınmıştır.

gösterilmesi gereken bir konudur. Nitekim kamu hafızasını oluşturan arşivler, bilgi hizmetlerini sunarken devletin, milletin ve bireylerin mahremiyetine ve çıkarlarına saygı göstermek durumundadır (Rukancı, Anameriç ve Başar, 2021, s. 18).

Amerikan Kütüphane ve Bilgi Kaynakları Konseyi (Council on Library and Information Resources /CLIR) tarafından yayınlanan rehber (Born Digital: Guidance for Donors, Dealers and Archival Repositories/ Dijital Doğan: Bağışçılar, Satıcılar ve Arşiv Depoları için Rehber), hassas içerik tespit edilmesi durumunda yapılması gereken işlemleri üç safhada incelemektedir: Belgeyi açık tutmak, tamamen kaldırmak ya da kısıtlama getirmek (Redwine ve diğerler, 2013, s. 8). Hassas bilgi içeren bir belgeyi veya belge grubunu erişime açık tutmak en iyi ihtimalle ihmalkârlık, en kötü ihtimalle de yasa dışı bir durum olduğu ifade edilmektedir. Sadece hassas bilgi içerdiği için belgeleri tamamen erişime kapatmak, temel arşivcilik ilkelerine aykırıdır. Belgeler üzerinde mümkün olabildiğince – birincil yaklaşım – kapatma kararının alınmamasıdır. Tam veya kısıtlı erişim amacı güdülmelidir. Erişim kısıtlaması hassas içerik tespit edildiğinde yapılmalıdır. Ancak belge içeriğinde hassas bilginin artış göstermesi değerlendiricileri önlem olarak çok sayıda kaydı kapatmaya teşvik ederek bir tehlike oluşturmaktadır. (Sloyan, 2016, s. 30). Bu durum açık devlet anlayışının kabul edildiği demokratik toplumlarda şeffaflık ve hesap verilebilirlik anlayışlarına aykırı olarak ahlakî, etik ya da siyasî açıdan kabul edilebilir değildir. Öte yandan, belgelerin erişime kapatılma uygulamasının çok ileri bir boyutu olan arşivler de mahremiyeti korumak için belgelerin yok edildiği durumlar (İsveç'te, yüksek soylu aile skandallarıyla ilgili belgeler 1860'larda imha edilmiştir) da meydana gelmiştir (Henttonen, 2017, s. 298). Mahremiyet, ulusal güvenlik veya bireysel gizlilik kaygıları, kapatma veya imha yolu ile giderilmeye çalışılmıştır. Mümkün olan yerlerde bir dosya içindeki belgeler yeniden düzenlenmelidir. Yalnızca bunun mümkün olmadığı durumlarda kapatma uygulamasına başvurulmalıdır. Gizliliğin korunmasında bir veya birden fazla verinin silinmesi her zaman son çare

olmalıdır (Naugler, 1984, s. 87), imha seçenekler arasında düşünülmemelidir. Amerikan Arşivciler Derneği'nin hazırlamış olduğu Etik Kurallar rehberinde kısıtlamaları en aza indirmeye ve erişim kolaylığını en üst düzeye çıkarmaya çalışırken belgelere açık ve adil erişimi aktif olarak teşvik edilmesi gerektiği ifade edilmektedir (Society of American Archivists, 2020). Bu bağlamda "hassas içerikli bir belge veya belge grubu arşivlenmeden önce yeniden düzenlenmeli mi ya da bilgilerin hassaslığı ortadan kalkana kadar kapatılmalı mı?" sorusu sorulabilir. Kapalı tutma süreci, bir belge üzerinde uygulanacak kısıtlamaların o belgenin bütünlüğünün anlaşılmasına zarar vermesi durumunda makul bir seçenek olarak değerlendirmelidir. Ancak erişim, kısıtlı olsa da sağlanması öncelikli yaklaşımdır. Bu hususta hassasiyetin zamanla azalan bir yönünün bulunması, kısıtlamanın ne kadar süre olacağı konusunu öne çıkarmaktadır (Peterson, 2007, s. 7).

Arşivciler erişimi yasaklayan/sınırlandıran mevzuat hükümlerinin kontrolünü sağlamak için belgeleri tek tek inceledikten sonra anonimleştirerek, redakte ederek veya "sterilize" versiyonlar [hassasiyetten arındırılmış kopya] oluşturarak belgelere tam veya kısmi erişim sağlanıp sağlanamayacağını belirlemelidir (Lemieux, 2024, s. 3). Belge üzerinde sınırlamalara dair alanlar, çeşitli üst veri standartlarında yer bulmuştur. ISAD(G)[30] ve RAD[31] gibi arşiv belgelerinin/materyalinin tanımlanmasına ilişkin üstveri standartlarında "kısıtlama" ve "sınırlama" ifadeleri geçmektedir. Bu niteleme alanlarının olması belgelerin içerek özelliklerine göre bir bakış açısı olması gerektiğini, değerlendiricilerin bu özelliklere göre belgeye/materyale varsa mevzuat yoksa da tecrübe ve ahlakî olarak kısıtlama ve/veya sınırlama koyabileceğini göstermektedir. RAD standardına göre (1.8B16a. *Restrictions on access*), erişim sınırlamalarına ilişkin açıklamada kısıtlamanın ayrıntıları, kaldırılacağı tarih, erişimi düzenleyen mevzuat (eğer varsa), kısıtlamaları uygulayan veya denetleyen kişi ya da kurum ile itirazların

[30] International Standard Archival Description (General): Uluslararası Standart Arşivsel Tanımlama (Genel)
[31] Rules for Archival Description: Arşiv Tanımlama Kuralları

yönlendirilebileceği merci gibi unsurların yer alması gerekmektedir (Rules for…, 2008). ISAD(G) standardına göre (3.4.1 *Conditions governing access*), erişimi kısıtlayan veya etkileyen hukukî durumlar ya da diğer düzenlemeler hakkında bilgi sağlanmalıdır. Erişimi etkileyen yasa, hukukî statü, sözleşme, yönetmelik veya politika belirtilmelidir. Uygun olduğu durumlarda, kapanma süresinin kapsamı ve materyalin erişime açılacağı tarih de belirtilmelidir. Buna dair standartta bazı örnekler sunulmuştur. Örneğin Fransa Arşiv Yönetmeliği (3 Ocak 1979 tarihli 79-18 sayılı yasa, Madde 7) uyarınca belgeler, oluşturulma tarihinden itibaren 60 yıl boyunca erişime kapalıdır (International Council on Archives, 1999).

Tanımlama standartlarına göre, ilgili üst veri alanlarında varsa sınırlamaların belirtilmesi gerekmektedir. Bu üst veri alanları, hassas veya gizli belgelerin erişim yönetimini belirler. Değerlendiricinin erişime ilişkin kararını bu alanlara işlemesi gerekir. Daha sonra, hassas bilgi içeren belgeler için bu süreç; belge üzerinde sınırlama (anonimleştirme, maskeleme, redaksiyon), kapatma ve erişime sunma işlemleri şeklinde yürütülmektedir.

III.1.1. Anonimleştirme-Maskeleme

Anonimleştirme, bir veri setinde kişisel olarak tanımlanabilir veriler gibi hassas bilgilerin çıkarılması veya değiştirilmesi işlemidir. Anonimleştirme ile verilerin analiz, araştırma, arşivleme veya diğer amaçlar için kullanılmasına izin verilirken gizliliği korumak esas amacı oluşturmaktadır. Anonimleştirme, yetkisiz erişimi veya ifşayı önlemek için hassas bilgiler söz konusu olduğunda özellikle önemlidir. Belgeler üzerinde anonimleştirmenin uygulanması, belge temizleme (*document sanitation*) olarak da ifade edilmektedir. Belge temizleme, belgenin gizliliği korunan bir sürümünü üretmeyi içermektedir. Belge temizleme işlemi hassas verilerin tespiti ve gizlenmesi olarak ifade edilmektedir (Nettleton ve Abril, 2014, s. 155). Bu sebeple belge temizleme işlemi için tek tek terimler

veya terim dizileri sınıflandırılmalıdır (McDonald, 2019, s. 67). Hassas verilerin mümkün olduğunca anonimleştirilerek orijinal kopyalarının anonimleştirilmiş şekilde sunulması gerekmektedir (Čtvrtník, 2021, s. 324). Değerlendiricinin böyle bir durumla karşı karşıya kalması durumunda, belge üretici kurumla yüksek hassasiyete sahip veri dosyalarının anonimleştirilmesine yönelik bir prosedür üzerinde çalışması gerekli olabilir (Naugler, 1984, s. 83). Anonimleştirmenin uygulandığı durumlarda, veri deposunda biri ham diğeri ise kamu kullanımına açık formattaki verileri içeren iki dosya bulunur. Bu işlem hassas içeriğe sahip her belge üzerinde uygulanan düzenlemelerde yaygınlıkla kullanılmaktadır. Temel amaç orijinal belgenin korunmasıdır.

Anonimleştirme gizliliği artırarak kullanımı azaltmak anlamına gelir. Bu sebeple değerlendirme sürecinde verilerin anonimleştirilmesi önerilmemektedir. Ancak, bu aşamada arşivcinin verileri anonimleştirmesinin değeri ve sonuçları hakkında bir ön değerlendirme yapması ve ayrıca gerekli olacak kişi/zaman, teknolojik donanım ve iş gücü maliyetlerinin bir tahmininin yapılması gerekebilir. Anonimleştirme, bir maliyet/fayda analizi gerektirir: yarar, gizliliğin korunmasıdır, maliyet ise sonuçta ortaya çıkan bilgi kaybı derecesidir (Naugler, 1984, s. 84; Henttonen, 2017, s. 293).

Çeşitli anonimleştirme (maskeleme, genelleştirme, rastgeleleştirme vb.) teknikleri bulunmaktadır. Ancak kamu belgeleri üzerinde uygulanacak anonimleştirme işlemi, belgenin provenansı, aidiyeti ve bağlamı üzerinde negatif etkiler oluşturacak tercihte olmaması gerekir. Bir anonimleştirme tekniği olan genelleştirmenin uygulanmasıyla belirli değerlerin daha genel veya daha az kesin değerlerle değiştirilmesi sağlanabilir. Örneğin belge içeriğinde hassas bir bilgi olan kesin coğrafî konum bilgisinin daha geniş bölgeler olarak, kişilere ait yaş bilgisinin kesin olmayan, gelir bilgisinin yaklaşık ifadelerle genelleştirilebilir. Fakat bu uygulamalar, belgenin özgünlüğüne ve bütünlüğüne zarar verecektir. Dolayısıyla bütünlüğe zarar vermeyecek şekilde anonimleştirilmenin

uygulanması beklenmektedir. Bu noktada maskeleme tekniği belge anonimleştirme için uygun bir seçenek olarak öne çıkmaktadır.

Tablo 4. Veri Maskeleme İşlemi

Veri Türü	Maskelenmemiş Veri	Maskelenmiş Veri
Ad Soyad	John Sensitive	J*** S********
Kimlik Numarası	12345678901	12345*******01
Sosyal Güvenlik Numarası	123-45-6789	*--6789
Kredi Kartı Numarası	1234 5678 9012 3456	**** **** **** 3456
Adres	123 Main St, City	123 **** St, City
Biyometrik Veri	Retina tarama sonucu	Görüntü değeri yerine "Biyometrik Veri"
DNA Dizilimi	AGCTTACG...	AGCT****...

Maskeleme, belirli karakterleri veya ögeleri semboller, yer tutucular veya rastgele değerlerle değiştirerek hassas bilgileri korumak için kullanılan belge bütünlüğüne zarar vermeyen bir tekniktir. Çeşitli maskeleme teknikleri/türleri (şifreleme, yer değiştirme, karıştırma vs.) var olsa da bütünlüğün garanti altına alınması ve manipülatif sonuçların yaşanmaması için sayı/harf/sembol kullanılarak maskelemenin[32] yapılması uygun bir seçenektir. Verilerin genel yapısını ve biçimini koruyacak şekilde belirli ayrıntıları gizlemek ve aynı zamanda bilgilerin tanımlanmasını veya kötüye kullanılmasını daha zor hale getirmeyi amaçlamaktadır. Maskeleme, gizliliği koruma ihtiyacı ile dengelemeyi amaçlayan bir veri anonimleştirme yöntemidir. Bu teknik genellikle kişisel olarak tanımlanabilir bilgiler veya hassas ayrıntılar içeren veri kümelerine (Tablo 4) uygulanır. Örneğin isimler, adresler, doğum tarihleri, sosyal güvenlik numaraları, finansal hesap

[32] Maskelemenin çeşitli türleri olmak ile birlikte başlı başına sayı, harf ve sembol kullanılarak uygulanan bir teknik olduğu bilinmektedir. Bkz. Ajayi, O. O., & Adebiyi, T. O. (2014). Application of data masking in achieving information privacy. *IOSR Journal of Engineering*, *4*(2), 13-21.

bilgileri maskelenebilecek yapılandırılmış türdeki verilerdir. Maskeleme tekniği belge içerisindeki yapılandırılmış veri türleri için daha uygun bir seçenektir. Ayrıca bu durum verinin yer aldığı formatın düzenlenebilir niteliğine de bağlıdır. Örneğin dijitalleştirilmiş belgelerde maskeleme işleminden ziyade redaksiyon yöntemi yoğunlukla kullanılabilir. Bununla birlikte yapılandırılmamış veri ögelerindeki bağlamsal hassasiyetlerin anonimleştirilmesi için doğru bir tercih olmayacaktır. Örneğin siyasî veya dinî inanç, suç geçmişi, hastalık bilgileri belirli bir kalıpta olmayan (yapılandırılmamış) bağlama bağlı olarak çıkarılması gereken ifadelerdir. Dolayısıyla belge içeriğinde maskelemenin yapılamayacağı bağlama bağlı hassasiyetler için terim veya cümle düzeyinde düzenlemelere ihtiyaç duyulacaktır. Bu düzenlemeler erişimin daha geri planda kalacağı hassasiyetin yüksek olduğu kamu belgelerinde uygulanacak redaksiyon işlemleri ile mümkün hale gelecektir. Bunun dışında maskeleme, gerektiğinde üst veri alanlarında[33] da etkili bir şekilde kullanılabilir.

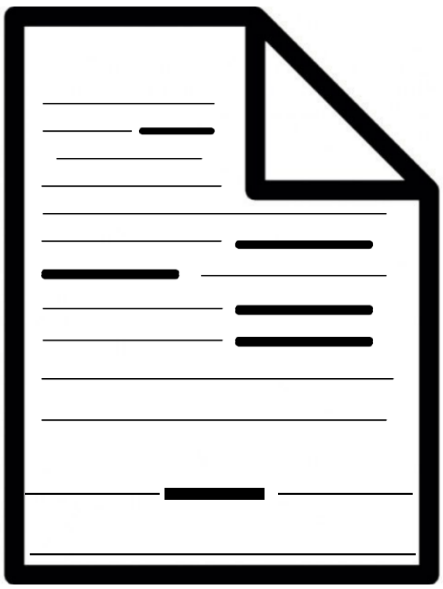
III.1.2. Redaksiyon

"Redaksiyon, bireyin mahremiyetini korumak, gizli bilgilerin tehlikeye atılmasını engellemek amacıyla belgedeki hassas bilgilerin, genel kullanıma veya görme yetkisi olmayan birine sunulmadan önce maskeleme veya kaldırma işlemidir" (Pearce-Moses, 2005, s. 336; Association of Records…, 2007). Redaksiyon işlemi, anonimleştirmeyi kapsayan bir kavram olmasının yanı sıra farklı olarak belgenin yayınlanmadan önce tek tek kelimelerin, cümlelerin veya paragrafların karartılması ya da sayfaların veya bölümlerin görünmez hale getirilmesi olarak uygulanmaktadır. (The National Archives, 2022, s. 2). Bu işlem bir anlamda tashih etmek olarak da düşünülebilir. Anonimleştirilmesi zor belgelerde redaksiyon kararının alınması, erişim kaybının yüksek

[33] Belge başlığının maskelenmesine dair örnek uygulama IV.6 İsviçre (Swiss Federal Archives) başlıklı bölümde "Anonimleştirilmiş Belge" isimli 10. görselde yer almaktadır.

olacağına işaret etmektedir. Kurumlar, hassas bilgilerin redakte edilmesi halinde belgelerin bazı bölümlerinin yayınlanıp yayınlanamayacağını değerlendirmesini yapacaktır. Bu sebeple redaksiyon için harcanan zaman, bir belgenin tarihi değeri ve mevcut kaynaklarla orantılı olmalıdır. (The National Archives, 2019b, s. 3; The National Archives, 2021a, s. 4).

Redaksiyon işlemi, kâğıt veya elektronik belgenin her zaman bir kopyası üzerinde gerçekleştirilmelidir. Orijinal belgeye daha sonra erişim sağlanabilmesi için redaksiyon işleminde kullanılmamalıdır. Redaksiyon, hiçbir zaman metnin veya bilginin bir belgeden tamamen çıkarılmasıyla sonuçlanmamalıdır. Belgede bir ya da iki kelimenin, bir cümlenin ya da paragrafın, bir ismin, adresin ya da imzanın çıkarılması gerektiğinde muaf tutulan ayrıntıları düzenlemek için kullanılır. Birkaç cümlede veya sınırlı sayıda sayfada hassas bilgiler içeriyorsa, bu bilgiler gizlenir ve öğenin geri kalanı genel erişim için serbest bırakılır. Ancak redaksiyon talep edilen öğe veya dosya yanıltıcı veya anlaşılmaz hale geliyorsa bir belgenin anlamsız hale gelmesine neden olacak kadar çok bilginin redakte edilmesi gerekiyorsa – belgenin üçten birinden fazlası çıkarılması gerekiyorsa –, belgenin tamamı erişime kapalı olarak muhafaza edilmelidir (International Council on Archives, 2012, s. 11; The National Archives, 2015, s. 29; The National Archives, 2022, s. 3).



Şekil 1. Redaksiyon İşlemi

Hassas bilgi içeren kâğıt belgelerde orijinal belgenin ya da ana kopyanın fotokopisi çekilerek gizlenecek veriler kalemle veya siyah bant çekilerek (Şekil 1) redakte edilir.[34] Redaksiyon tamamlandıktan sonra kopyanın kendisi fotokopi haline getirilir ve ardından imha edilir. Kalem kullanılarak redakte edilen bilgiler ışığa tutulduğunda okunabileceğinden tekrar fotokopi çekilmesi gereklidir. Bu kopya, orijinal belgenin yerini alan erişim kopyasıdır. Orijinal belge, erişim yetkisi bulunan personel dışında kimsenin erişemeyeceği kontrol dosyalarının yer aldığı dolaplarında tutulur. Bu yöntem yoğun emek gerektirir, ancak arşiv malzemesini muhafaza etmenin, içerdiği hassas bilgileri korumanın ve belgeyi aynı anda kullanıcıların erişimine sunmanın etkili bir yoludur (Stein, 2021, s. 8; The National Archives, 2022, s. 9). Elektronik belgelerde bu işlem yazılım araçları ile sağlanmaktadır. Bununla birlikte elektronik belgenin basılı hale getirilerek geleneksel redaksiyon işlemlerine tabi tutulduktan sonra tekrar elektronik ortama aktarılması da mümkündür. Ancak bu genellikle tercih edilen, işler ve yararlı bir seçenek değildir. Elektronik bir belge, bilgi silme ve farklı bir formata dönüştürme

[34] Redaksiyon işlemine dair gerçek örnek IV.7.Kanada (Library and Archives Canada) başlığı altında yer alan. "1960-1985 Alberta Üniversitesi Siyasî Faaliyetler" isimli 11. görselde yer almaktadır.

işlemlerinin bir kombinasyonu yoluyla redakte edilebilir (The National Archives, 2022, s. 11). Örneğin orijinali PDF formatında olan bir belgenin öncelikle düzenlenebilir metin formatına dönüştürülerek redaksiyon işlemleri başlatılmalıdır. Redaksiyon işlemi tamamlandıktan sonra tekrar orijinal formata dönüştürülmelidir. Ancak, bu işlem, belgenin karmaşıklığına ve kullanılan formatlara bağlı olarak dikkatlice ele alınmalıdır. Oluşabilecek biçimlendirme kayıplarının ve bilgi sızıntılarını önlemek için dönüşüm süreçleri iyi anlaşılmalı ve test edilmelidir.

Genel olarak redaksiyon sürecinde belge: anlam kaybı, kamuoyunun muhtemel ilgi düzeyi, harcanan çaba ve hata riski bakımından gözden geçirilmelidir (The National Archives, 2015, s. 28, 29). Redaksiyon yapıldıktan sonra belge anlamını yitiriyorsa tekrar değerlendirilmeli veya kapatılmalıdır. Belge kamuoyunun ilgisini çeken bir konuyu içeriyor ve kamu yararı oluşmuşsa redaksiyon için harcanan zaman ve emek daha fazla olmalıdır. Ayrıca redaksiyon işleminde hata riski oluşabileceğinden deneyime muhtaç bir titizlikle yürütülmelidir.

Belge ve belge gruplarına yönelik kısıtlamalar sınırlı düzeydedir. Belgelerin aranabilir olmamasını sağlayan uygulamalar ve redaksiyon sağlamanın dışında arşivcilerin koruma önlemleri bulunmamaktadır (Dressler ve Kearns, 2023, s. 181). Kısıtlanamayacak ölçüde hassasiyet içeren belgeler kapatma işlemlerine tabi tutulmaktadır.

III.1.3. Kapatma/Kapalı Tutma

Kamu belgelerine ve arşivlerine açık-engelsiz erişim, şeffaf ve güvenilir modern demokrasilerde önemli bir işleve sahiptir. Arşivlerin ve arşiv kurumlarının amacı sahip olduğu belgeleri olabildiğince kamu hizmetine açık hale getirmektedir. Bu hususta "kapatma (*closed*) kararı" en son başvurulması gereken seçenektir. Belgeler üzerinde kapatma kararlarının alınması ulusal güvenlik, ekonomik çıkar, bireysel mahremiyet ve

gizlilik, yasal düzenleme, bozulma ve yıpranma gibi çeşitli sebeplere dayanabilir. Hassas bilgilerin varlığı da bu kapsamdadır. Hassasiyet değerlendirmesi yapılan belgeler, içerik olarak hassas ise kamu yararına erişime kapatılma (*closed to access in the public interest*) değilse kamuyu aydınlatma (*public disclosure*) yoluyla erişime sunulur. Bu sebeple "bilginin açıklanmasında veya saklanmasında kamu yararı var mıdır?" sorusunun cevaplanması gerekmektedir (Özdemir, 2009, s. 138). Bu bağlamda hassasiyet değerlendirmesi kavramı, İngiltere Ulusal Arşivleri tarafından hazırlanan "*Access to public records*" başlıklı rehberde, belgelerin saklanıp saklanmayacağını ya da erişimin kısıtlanıp kısıtlanmayacağını belirleme süreci olarak tanımlanmıştır (The National Archives, 2015, s. 6). Erişim durumu kısmî sınırlılık olarak belge üzerinde anonimleştirme/maskeleme ve redaksiyon işlemleri ile sağlanır. Ancak belge ve belge gruplarının kısmî sınırlılık uygulanamayacak hacimde veya nitelikte hassas bilgi içermesi durumunda kapatma kararının alınması gerekir. Redaksiyon işlemi sonucunda belge veya belge grubunun tamamının ya da bir bölümünün kapatılması da gerekebilir. Kapatma kararları süreli veya süresiz olarak uygulanır. Bu durum belgenin hassas/özel nitelikli bilgi taşıdığını ifade eder. Kapatma kararı alınırken; hassas bilgi konusunda deneyimli personel görüşü ile benzer belgelerin durumu değerlendirilip belgenin sınırlama sebebi, fon içerisinde hangi belgelerin kapalı kalacağı, kapatma süresi ve üst veri öğesi görünür şekilde tanımlanmalıdır (The National Archives, 2015, s. 7; Rukancı, Anameriç ve Başar, 2021, s. 169). Örneğin X arşivi/belgesi KVKK'nın [ya da FOIA/BEHK muafiyetinin] ilgili maddesi gereğince 100 yıl süre ile erişim kapalıdır. Kapatılan belge içeriği hakkında tam bir açıklama yapılmasa da genel ifadeler ile tanımlanması gerekir (The National Archives, 2019b, s. 6). Bu konuda kurum veya konu esaslı olarak sınıflamalar[35]

[35] Man Adası Kamu Belgeleri Ofisi (Public Record Office) bazı belgeler için kapatma kararlarını sınıflamıştır. Örneğin; hasta kayıtları, sağlık bilgileri, adlî tıp soruşturma dosyaları, mahkeme kayıtları okula kabul kayıtları 100 yıl süre ile kapatılmaktadır (Public Record Office, 2022, s. 2).

yapılmaktadır. Eğer belgenin özeti[36] sunulabiliyorsa üst veri alanına eklenmelidir. Araştırmacılar, personel ve ilgililerin belgenin varlığı hakkında bilgi sahibi olabilmesi için üst veri alanının mutlaka var olması gerekir. Hangi bilgi türün veya fon-seri-dosya grubunun ne kadar süre ile kapatılacağına dair zaman cetvelinin[37] bulunması bu süreci kolaylaştıracaktır. Bu konuda anılan rehberde konulara göre sürelerin belirlendiği, belirlenemeyen alanlar için kamu yararı testinin uygulanacağı belirtilmiştir. Örneğin ulusal güvenlik (*national security*) konusu kamu yararı testi gerektiren ve buna bağlı olarak sürenin belirsiz olduğu bir alandır. Bunun dışında mahkeme belgelerinin (*court records*) mutlak suretle 20 yıl kapalı olacağı belirtilmiştir (The National Archives, 2015, s. 10, 11).

Süreli veya süresiz kapatma kararı alınan hassas bilgi içerikli belgeler için değerlendirme işlemi nihai olarak tamamlanmış değildir. Tekrar değerlendirme tarihi belirlenerek kaydedilmelidir. Bu işlem, kısıtlı veya kamu yararına erişime sunma durumu oluşmayana kadar rutin olarak devam etmelidir. Gizliliği kaldırılmış veya saklama süresi dolmuş bu tür belgeler için imha süreci başlamaktadır. Ancak normal belgelere uygulanan imha işleminden farklı bir süreç[38] işlemektedir.

[36] Özetleme hassas bilgi içerikli belgeleri koruma/gizleme hususunda uygulanacak bir kısıtlama yöntemi olarak kullanılabilir. Üst veri alanında belgeye dair özet bilgisinin verilmesi ihlale sebebiyet vermiyorsa tercih edilebilir.

[37] İngiltere Ulusal Arşivi tarafından yayınlanan "*Access to public records*" başlıklı rehberde erişim muafiyetleri, testleri (kamu yararı) ve kapatma sürelerine ilişkin çeşitli temalarda (ekonomi, mahkeme belgeleri, ulusal güvenlik vs.) çerçeveler sunulmuştur.

[38] Nihai imha yöntemleri belgelerin hassasiyetine, formatlarına ve imha işlemine göre değişmektedir. Bu bağlamda sıradan çöp kutularının kullanımı sadece kamu malı olan belgeler için geçerli olmaktadır. Hassas veya kişisel bilgi içeren belgelerin imhası onaylı bir imha firması/şirketi tarafından gerçekleştirilmek suretiyle çöp kutularına konulmalıdır (The National Archives, 2012, s. 18). BM Arşiv ve Belge Yönetimi Bölümü belgelerin imhasının geri döndürülemez olması gerektiği tavsiyesinde bulunarak bu durumun hassas bilgi içeren belgeler açısında riski ortadan kaldıracağını ifade etmektedir (National Records of Scotland, 2021, s. 31). Hassas arşiv belgelerinin imhasına yönelik Dışişleri Bakanlığı Arşiv Hizmetleri Yönetmeliği (22/6) makineler aracılığıyla kıyıldıktan sonra yakılacağını belirtmektedir. Dijital belgeler için imha işlemi farklı işlemektedir. Dijital belgenin silinmesi nihai olarak yok edilmesini sağlamayabilir. Daha fazla bilgi için The National Archives tarafından yayınlanan "Disposal Scheduling" adlı kaynak ile ICO (Information Commisiner's Office) tarafından sunulan yöntemlere bkz. https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/practical-methods-for-destroying-documents-that-are-no-longer-needed/

III.1.4. Kamu Yararına Erişime Sunmak

Erişim kısıtlamasına yönelik herhangi bir durumun artık bulunmayarak gizliliğin kaldırılması (*declassification*), kısıtlama süresinin sona ermesi ve kamu yararına erişim gerekçeleriyle erişim kararı alınır. Kapatma kararı alınan veya ilk defa değerlendirilen belgeler üzerinde erişim kararı verirken bazı hususlara dikkat etmek gerekir:

a) Belgelerin gerçekten var olup olmadığını (doğası gereği yok edilme riski yüksektir) belirlemek,
b) Belgede hangi güvenlik/gizlilik derecelerinin veya sınıflandırmaların bulunduğunu ve bunların kısa veya uzun vadeli etkilerinin olup olmadığını değerlendirmek,
c) Belgede hangi kişisel bilgilerin bulunduğunu ve geçen zaman göz önüne alındığında hala kapatılıp kapatılmaması gerektiği değerlendirmek,
d) Belgelerdeki bilgilerin nasıl erişilebilir kılınacağına karar vermek,
e) Belgelere kimlerin hangi koşullarda erişebileceğini belirleyen bir erişim politikası oluşturmak,
f) Belgeleri, hassasiyet konularını ve mevzuatı bilen personel ile kapatma konusu görüşmek,
g) Arşiv hizmetlerindeki benzer belgelerin erişim durumunu değerlendirmek,
h) Belgede kullanılan dil dahil olmak üzere içerik hakkında bilgi sahibi olup danışmanlık hizmeti sunmak (Mathers, 2000, s. 60; The National Archives, 2015, s. 19; The National Archives, 2019b, s. 4).

Bu hususlara hassasiyetin devam edip etmediğini tespit etmek ve erişim koşullarını ortaya koymak için dikkat edilmelidir. Hassasiyet değerlendirmesi sürecinde, erişim öncelikli bir amaçtır. Kısıtlı erişimin olmadığı durumlarda tamamen kapatma yoluna gidilmelidir.

Bunun dışında kapalı belgelere erişimin tamamen engellenmediği uygulamalar[39] da bulunmaktadır.

III.2. Hassasiyet Değerlendirmesi Zorlukları

Değerlendirme, belgelerin entelektüel içeriğine erişimin ilk safhasını oluşturan, mahremiyet ve gizliliğin gözden geçirildiği bir süreçtir. Değerlendirme sürecinde esasen hassas içeriğe sahip belgelerin – özellikle kişisel bilgi olarak yorumlanabilecek her şeyin – saklanması veya erişime sunulması bir risktir. Hassasiyet değerlendirmesi konusu nihayetinde riskle ilgilidir. Belgeyi olması gereken zamanda yayınlamama, belirlenen kapatma süresinden daha uzun saklama veya doğrudan erişimi aksatma riski kurumların güvenilirlik konusundaki itibarına zarar vermektedir (Moss ve Gollins, 2017, s. 18-19). Erişim ve kapatma kararlarının alınma sürecinde karşılaşılan her zorluk kamu ve kişi haklarının korunması noktasında birtakım riskleri beraberinde getirmektedir. Risk oluşumunun temeli, hassasiyet tespitinin yapılması ile başlamaktadır. Hassasiyet yargısının verilmesi, erişim sınırlamalarının uygulanması varsa kapatma sürelerinin belirlenmesi sistematik yürütülecek bir sürecin kritik adımlarıdır.

Bir belge hassasiyet açısından değerlendirilirken kurumsal işleyişlerdeki farklılıklar başta olmak üzere pek çok etken zorlayıcı olabilmektedir. Bu süreçte mantıksal çıkarımların ve karşılaştırmaların yapılması gerekli olabilir. Örneğin, bir çalışanın kurum içerisinde aldığı isimler, görevler veya kararlar hakkında bilgiler normal olarak açıklanırken kurum içi disiplin meseleleriyle ilgili bilgiler hassasiyet oluşturduğundan belge dolaşımının erişim ve kullanım sınırlamaları ile yürütülmesi beklenmektedir. Bu durum çalışanın kurum içerisindeki çalışma barışını sağlaması, çalışma ortamında oluşacak sosyal baskının engellenmesi için gereklidir. Bununla birlikte

[39] Belge hassas bilgi içerse bile "önemli kamu yararının" olmasından dolayı erişime sunulması Man Adası Kamu Belgeleri Ofisi için geçerli bir gerekçe olarak listelenmiştir (Public Record Office, 2022, s. 4).

iş tartışmalarıyla ilgili belgelerde bir çalışanın maaşıyla ilgili ayrıntıların hassas olma olasılığı, politik tartışmalarla ilgili belgelerde politikacıların, maaş ve harcama bilgilerinin yer almasından daha yüksektir. Çünkü politikacıların kamuya mal olmuş, şeffaf ve hesap verebilir yapıdaki kişiler olması, maaş mevzu bahis olsa da paralarını nasıl harcadıklarının şeffaflığında güçlü bir kamu yararı bulunmaktadır (McDonald, 2019, s. 40; Narvala, McDonald ve Ounis, 2022a, s. 4931).

Bilginin ifşasında ağır basan bir kamu yararı olmalıdır. Ancak bireyin onayının gerekli olduğu durumlarda – örneğin sağlık kayıtları – gizlilik yükümlülüğü eklenebilir. Bir bireyin sağlık kayıtlarına güven beklentisi, ölümünden bir süre geçene kadar ifşa edilmemesi şeklindedir (The National Archives, 2018, s. 32). Bu durum hassasiyetin uzunca bir süre devamlılık gösteren, zamana bağlı olarak kontrol edilmesi gereken bir süreç olduğunu göstermektedir.

Hassasiyet değerlendirmesi sürecinde, belgede yer alan her kelimenin, bilginin veya ifade biçiminin hassasiyet tespitini ve derecelendirmesini zorlaştırdığı durumlar da bulunmaktadır. Kelimeler bağlamlarına bağlı olarak hassastır veya hassas değildir. Doğal dilde farklı ifadeler kullanılarak aynı anahtar kelime hassas veya hassas olmayan bir karakter kazanabilir. Örneğin bir kişinin kötü bir hastalığa yakalanmasını, "X kişisi, AIDS'e yol açan HIV virüsünü taşımaktadır" olarak ifade etmek ile adres veya çalışma bilgilerinin belirtilerek söylenmesi arasında hassasiyet bakımında fark bulunmaktadır. İlk ifadede kişiye ait tanımlayıcı bir bilgi yoktur. Kişinin tanımlanarak netlik kazanması bu durumu daha hassas bir hale getirmektedir. Benzer bir şekilde bir kurum içerisinde yaygın olarak kullanılan bir isim ile nadir bulunan isme ait hassasiyet durumları arasında farklılık vardır. Bazen iki hassas bilgiden biri diğerine göre daha hassas olabilir. Hastalık teşhisleri arasında bile farklılıklar oluşmaktadır. Kalp hastalığı teşhisiyle grip veya soğuk algınlığı, hassasiyet bakımında eşdeğer değildir. Kalp hastalığı hayat sigortası primlerinin artması ve istihdamın azalması gibi kişi için daha fazla kişisel kayba neden olabilir.

Hassasiyetin objektif olarak ölçülemeyen sosyal ve kültürel faktörlere bağlı, gizlilik uzmanları tarafından belirlenmesi gereken bir konu olduğu düşünülmektedir (Geng ve diğerleri, 2011, s. 164). Hassas bilgi kavramı, yaygın bir şekilde mevcut gibi görünse de, bazı yönleri belirsizdir. Hassas bilgilerin ayrı bir bilgi türü veya kategorisinde olup olmadığı, hassasiyetin neye göre ölçüleceği konusunda bir fikir birliğinin olmaması, insanların genel bilgilerle ilgili olarak uygulayacağı hassasiyet kodlamasına ihtiyaç olup olmadığı ve hassas durumlar hakkındaki bağlamsal bilgilere referans yapılıp yapılmayacağı gibi konular belirsizdir (Thompson ve Kaarst-Brown, 2005, s. 248; Greene ve Meissner, 2005, s. 252). Tüm bu tartışmalar, değerlendirme sürecinin titizlikle yürütülmesi gereken çok katmanlı bileşenlerden etkilendiğine işaret etmektedir. Tüm değerlendirme kararları, iyi bir mesleki uygulama meselesi olarak belgelenerek değerlendirme politikalarına uygun hale getirilmelidir.

Değerlendirme arşiv iş süreçleri içerisinde en hassas ve zorlayıcı konuyu oluşturmaktadır. Hassasiyet değerlendirmesiyle birlikte bu süreç, kurumlar ve değerlendiriciler için çeşitli zorluklar yaratmakta ve bu zorluklar hem fiziksel hem de dijital ortamlardaki bilgi taşıyıcıları ve arşivlerde kendini göstermektedir (Jaillant, 2022a, s. 536). Bazı zorluklar, ortama özgü dinamiklerden kaynaklanmakta ve bu dinamiklere uygun çözümler geliştirilmesini gerektirmektedir. Diğer zorluklar ise ortamdan bağımsız olarak, format fark etmeksizin varlığını sürdürmektedir. Bu sebeple sürecin detaylı olarak incelenmesi gerekmektedir.

III.2.1. Bağlam ve İlişki Kurma

Değerlendirme sürecinde belgelerin üretim ve kullanım amaçları, bir başka kurum veya birimdeki belgeler ile ilişkisi, tamamlayıcılığı gibi pek çok unsur dikkate alınır (Rukancı, Anameriç ve Başar, 2021, s. 48). Belge özelinde ilişki (*relations*) kurma ve bağlamsal (*context*) incelemeler hassasiyetin tespit edilmesini zorlaştıran en önemli konudur.

Hassasiyet hem nesnel hem de öznel bir bileşene sahip (McCullagh, 2007, s. 197) olduğundan mevzuat nesnel, bağlam ise öznel yönünü oluşturmaktadır. Hassasiyet; bilginin türü ne olursa olsun kimin, kime, ne zaman, hangi bağlamda söylediğine, paylaşım ve kullanım koşullarına ve inceleme yetkisine bağlı olarak bağlamsal parametreler ile değerlendirilmelidir. Son yıllarda verilerin işlendiği bağlama giderek daha fazla vurgu yapılmaktadır (Kindt, 2016, s. 125; Martin ve Nissenbaum, 2017, s. 113). Hassas olan ve toplanması, kısıtlanması hatta yasaklanması gereken veri türlerini veya kategorilerini sıralamanın mümkün olmayacağı ileri sürülmektedir. Ancak verilerin/sözcüklerin özünde "özel" veya "hassas" olmadığı, ancak bağlamları ve kullanımları göz önüne alındığında hassas ve hassas olmayan ayrımı olabileceği ihtimali bulunmaktadır (OECD 2002, s. 40; Elliot, Mackey ve O'Hara, 2020, s. 136). Bu durum hassasiyet değerlendirmesini zorlaştırmaktadır. Hassasiyet yargısı insan uzmanlığı gerektiren, karmaşık genellikle bilginin üretildiği bağlama ve gözden geçirildiği zamana bağlıdır (McDonald, MacDonald ve Ounis, 2018a, s. 440; Narvala, 2024, s. 4). Pek çok durumda hassasiyetin bağlama bağlı olduğu görülmektedir ve bu her zaman dilbilimsel bir analizde ele alınamaz (Al-Fedaghi, 2007, s. 165). Dilbilimsel analiz yalnızca belgedeki terimlere veya varlıklara odaklanan, hassasiyetin bu yaklaşımlar ile tespit edilmesi anlayışına dayanmaktadır. Hassasiyetin belge içerisindeki terimlerden veya belgenin konusundan tespit edileceği durumlar vardır. Fakat bu yaklaşımları belge değerlendirmesinin odağına almak kapsayıcı olmamaktadır. Terimlerle birlikte hassasiyet, büyük ölçüde bilgilerin bağlamına da bağlıdır.

Hassasiyet, mutlaka konu odaklı değildir, daha çok neyin ve kimin hakkında söylendiğinin birleşiminden kaynaklanmaktadır (McDonald, 2019, s. 65). Bağlama göre hassasiyet senaryoları değişmektedir. Bağlamın hassas olmayan verileri hassas verilere dönüştürebileceğini göz önünde bulundurmak önemlidir. Veriler kullanıldığı bağlamda (örneğin kültürel, coğrafî, dinî, siyasî koşullar vb.), açıkça kişisel veya hassas olmasa bile,

veri analizinin bir birey(ler) veya birey(ler) grubu üzerine etki edebilir (Birleşmiş Milletler Geliştirme Grubu, 2017, s. 5). Bu sebeple salt terim ve konulara göre listeleme yapılarak hassasiyet çerçevesi sınırlandırılır. Terim ve konu listeleri ancak yardımcı bir başvuru kaynağı niteliğindedir. Aynı bilginin hassasiyeti ortama, kişiye, zamana bağlı olarak değişiklik gösterdiğinden, değerlendirme sürecinde olasılıkların değerlendirilmesi ve belirlenmesi gerekmektedir.

Değerlendirme sürecinde hassasiyet metinden çıkarılamıyor ya da bir dizi terim veya kuraldan çıkarılamıyorsa ve aynı zamanda bağlamın da hesaba katılması gerekiyorsa, hassasiyeti tespit etmek çok daha karmaşıktır (Thompson ve Kaarst-Brown, 2005, s. 248). Hassas bilgiler örtük veya dolaylı olabilir. Bağlama bağlı olarak kişisel, kurumsal, siyasî ve ulusal güvenlik konuları ve diğer çağrışımlarla ilgili olabilir (Moss ve Gollins, 2017, s. 13). Bilginin hassas olup olmadığını belirleyen değerlendirici, bilgiyi kamuya açık hale getirmenin muhtemel etkisi hakkında karar vermek durumundadır.

Tek başına hassas olmayan veya daha az hassas olan kişisel veri öğeleri, diğer verilerle ilişki kurularak birleştirildiğinde hassasiyet meydana gelebilir (Photopoulos, 2011, s. 32; Belen-Sağlam, 2022b, Nurse ve Hodges, s. 14). Bu durum "mozaik hassasiyet" kavramı ile açıklanmaktadır. Mozaik hassasiyet, bilgi kırıntılarının bir araya getirilmesi veya birbiriyle doğrudan bağlantılı olmayan bilgi ve belgeler arasında kurulan ilişkiler sonucunda ortaya çıkan hassasiyet durumunu ifade etmektedir. Mozaik hassasiyet iki veya daha fazla belgedeki bilgiler birleştirildiğinde ortaya çıkmaktadır. Belirli bir konu için ilgili bir belge belirlendiğinde veya aynı konuyu kapsayan başka bir belgenin alaka düzeyinin değişebileceği görüşünden kaynaklanmaktadır (McDonald, 2019, s. 185). Mozaik hassasiyet "*ilişki*" kurma kavramı ile bağdaşmaktadır.

Bir belge veya nesne düzeyindeki açıklama tek başına zararsız olabilir, ancak daha yüksek düzeydeki bağlamsal bilgilerle birleştiğinde bireyin veri koruma haklarını ihlal edebilir. Örneğin, bir isim ve doğum tarihi tek başına zararsız görünse de, akıl sağlığı

hastanesi hastalarının vaka dosyaları bağlamında hassas hale gelebilir (The National Archives, 2018, s. 30). Bir isim tek başına bir kişiyi tanımlamak için yeterli değilken kişinin tanımlanmasını sağlayacak olan, ismin sahip olduğu pozisyon, bir olay veya yer gibi diğer bilgilerle ilişkilendirilerek netlik kazanması sağlanır (The National Archives, 2018, s. 30-31). Bilgi kırıntılarının-veri parçalarının bir araya getirilmesi ile hassasiyet oluşabilir. Özellikle kurumsal belge dolaşımının yoğun olarak yürütüldüğü birimlerde çalışanlara ait bilgilerin hassasiyete sebebiyet verecek ilişkide olmaması gerekir. Örneğin bir çalışanın düzenli olarak yılın veya ayın belirli günlerinde izin kullanması – izin belgesinin herkes tarafından görülmesi durumunda – o kişinin dinî inanç ve hastalık bilgisinin açığa çıkmasına yol açabilir. Bununla birlikte belge içeriğinde yer alan ortam/mekân, hassasiyetin oluşmasına sebep olabilir.

Bazı ifadeler bir kamu hizmeti bilgilendirmesinde yer alıyorsa hassastır; bir gazete makalesinde yayınlanıyorsa hassas değildir. Benzer şekilde, bir kabine toplantısında söylenen sözler gizli olabilirken, parlamentoda söylenen ve kaydedilen aynı sözlerin hassas olarak kabul edilmesi mümkün değildir (Tough, 2018, s. 177). Bir basın haberi gibi halihazırda yayınlanmış bir içerikte yer alan bilgilerin, özel olarak iletilen bilgileri tartışsa bile kamuya açıklandığından gizli olmadığı düşünülür. Ancak belge, hükümetten veya başka bir kuruluştan bir yetkilinin basın açıklamasının içeriği hakkında ek bilgi sağlayan görüşlerini içeriyorsa, bu durumda görüşlerin hassas ve gizli olduğu kabul edilebilir (McDonald, 2019, s. 34). Bir silah anlaşmasıyla ilgili bilgiler içeren belgelerde; ülke, iyi bilinen ve mevcut dostluk ilişkilerinin pozitif olduğu modern, liberal bir demokrasi ise bu belgenin hassasiyeti çok az olabilir. Öte yandan, monarşik ve baskıcı bir rejim tarafından yönetilen bir ülke ise, anlaşmanın doğası oldukça hassas hale gelebilir (Moss ve Gollins, 2017, s. 14).

Değerlendirme sürecinde belgenin bağlamını çözümlemek, sadece terim ve konulara dayalı olarak yürütülemeyecek kadar zorludur. Özellikle bu sürecin hassasiyet

odaklı bir yönünün olması, bağlamın belge düzeyinde ayrıntılı bir şekilde irdelenmesini gerekli kılmaktadır. Fakat ele alınan her belge özelinde bağlamsal zorluklar ortaya çıkmayabilir. İçerik hacmi, standart olarak üretilen belge yapısı ve kurumsal farklılıklar, bağlama dayalı olarak hassasiyet değerlendirmesini etkileyebilir.

III.2.2. Zaman

Belgeler, arşiv değerlerini koruduğu sürece saklanırlar (Rukancı, Anameriç ve Başar, 2021, s. 49). Değerlendirme sürecinde, belgelerin arşivsel değerine bağlı olarak içermiş olduğu hassasiyetler, saklama sürelerine doğrudan etki etmektedir. Koruma sağlama ihtiyacı zamanla azalırken bazı durumlarda bir olayın üzerinden onlarca yıl geçmesine rağmen mahremiyet beklentisi hala geçerli olabilir (The National Archives, 2018, s. 33). Genellikle kamu ve özel/tüzel kişilerin haklarının korunmasına ihtiyaç duyulduğu sürece saklanır (Rukancı, Anameriç ve Başar, 2021, s. 48). Buna karşın toplumsal koşulların değişmesi, sosyal ve kültürel gelişmişlik gibi faktörler hassasiyet algısına etki ederek önem atfedilmeyen bir bilgiyi sonradan hassas veri kategorisinde nitelendirmeyi gerekli kılabilir (Bulut, 2020, s. 124). Ancak hassasiyetin zaman geçtikçe azaldığı, kısıtlamalara olan ihtiyacın zamanla ortadan kalktığı yaygın olarak kabul edilmektedir (Sillitoe, 1988, s. 12; Peterson, 2007, s. 7; The National Archives, 2015, s. 7; Moss ve Gollins, 2017, s.17; McDonald, 2019, s. 51). Zaman faktörü, çoğunlukla kişilere bağlı olarak ortaya çıkan hassasiyetler için öne çıkmaktadır. Hassas bilgi içerikli belgelerde; kişinin yaşı, ölümü, ölümünden sonra yakınlarına olan olası etkileri zamana bağlı olarak hassasiyet değerlendirmesini zorlaştıran noktalardır. 2004 yılında Ulusal Arşivler ve Kayıtlar İdaresi'nden (NARA) Bilgi Edinme Hakkı Kanunu kapsamında ölen bir avukata ait cesedin fotoğraflarının istemesi üzerine yüksek mahkeme, ölüm sahnesi fotoğraflarının yayınlanmasının kişisel mahremiyetin haksız ihlali anlamına geleceğini ifade ederek bu talebi reddetmiştir. Her ne kadar ölen kişinin kendi kişisel mahremiyeti tehlikede olmasa

da, hayatta kalan aile üyeleri bu duruma müdahale ederek yürürlükte olan kişisel gizlilik yasasına itiraz etmişlerdir. Kamuya açıklanması, ilgili bireyin veya birinci dereceden soyundan gelenlerin bilgilendirilmiş rızasını gerektirdiğinden mahkeme, ölen kişiye ait ölüm fotoğraflarının kişisel gizliliğini, hayatta kalan aile üyelerini kapsayacak kadar genişlemesine karar vermiştir (Sillitoe, 1988, s. 12; Entrikin, 2020, s. 827). Amerikan Arşivistler Derneği Etik Kuralları başta olmak üzere normatif arşiv uygulamalarına göre, gizlilik hakları bireyle birlikte yok olmaktadır. Ancak bağış yoluyla sağlanan bir özel arşiv materyali söz konusu olduğunda bağışçıların ölmeden önce hassas bilgilere erişimi kısıtlamadığı veya bu bilgilere ilişkin isteklerini belirtmediği durumlar gizlilik kaygısı oluşturabilmektedir. Böyle durumlarda arşivciler, arşiv normları esasınca bireyin ölümüyle birlikte mahremiyet haklarının sona erdiğini (The National Archives, 2015, s. 9) öne sürerken, diğer yanda bağışçıların yakınları tarafından talep edilen makul kısıtlamalara sıklıkla saygı göstermektedir (Poole, 2020, s. 6-7).

İngiltere Ulusal Arşivi tarafından yayınlanan rehberler ve pek çok bilimsel çalışma, hassas bilgi içerikli belgelerde yaşanması muhtemel zamana dayalı problemler ve belirsizlikler için bazı çerçeveler çizmiştir. Hassas kişisel bilgiler, çoğu Avrupa ülkesinde 100 ila 110 yıl süreyle (biliniyorsa kişinin yaşı düşülerek) kapatılmaktadır. Buna karşın ABD Bilgi Edinme Hakkı Kanunu (BEHK), yaşayan bir bireyin mahremiyetini ihlal edecek hassas bilgi içeren belgelerin 75 yıla kadar saklanmasına izin vermektedir (Borden ve Baron, 2016, s. 3225). Kapatma süreleri Avrupa ülkelerinde kişinin yaşı bilinmiyorsa, reşit olmayanlar için tüm süre boyunca (100 ila 110 yıl kapatma süresi), 16 yaşın üzerinde olduğu düşünülenler için ise 80 veya 94 yıl boyunca kapatılmaktadır (Moss ve Gollins, 2017, s. 13). Kişisel hassas bilgiler söz konusu olduğunda ilgili kişinin hayatta olup olmadığının bilinmediği durumlarda, belgenin kapalı tutulma süresinin, 100 yıl olarak – bir yaşam süresi – varsaymak ve bir yetişkin için (eğer yaşı bilinmiyorsa), belgenin düzenlendiği tarihte yaşının 16 olduğu varsayılmaktadır. Bir

kişinin yaşı bilinmiyorsa, kapatma süresini tahmin etmek için belgedeki kişisel bilgiler ve bağlamsal kanıtlar kullanılmalıdır. Kişinin bir yetişkin olduğu açıksa, tahmini yaş 16 olarak belirlenmelidir. Bağlamsal kanıtlardan kişinin kaç yaşında olduğu anlaşılamıyorsa, örneğin suç mağduru veya bakım evinde ikamet eden bir çocuk olabileceği durumlarda, 100 yıllık kapatma süresinin tamamı kullanılmalıdır (Sillitoe, 1988, s. 11; Thompson ve Kaarst-Brown 2005, s. 252; Allan, 2014, s. 14; The National Archives, 2021b, s. 4). Bu süre, ölüm için keyfi ya da yaklaşık bir rakam olarak değil, aksine doğal yaşam süresi boyunca ve ölüm sonrasında sınırlı bir koruma sağlamak amacıyla öngörülmektedir (Sillitoe, 1988, s. 11). Sınırlı koruma, kişinin ailesi ve yakınlarının zarar görmemesi anlayışı için dikkate alınmalıdır.

İngiltere Ulusal Arşivler ve Danışma Konseyi, hassasiyetin ne kadar süreyle geçerli olacağının bilinmediği ve İngiltere Bilgi Edinme Hakkı Yasası'nda herhangi bir son tarihin öngörülmediği hassas bilgiler için 10 yıllık bir kapatma süresini savunmaktadır. Koşullar zaman içinde değişebileceğinden, belgelerin her on yılda bir yeniden gözden geçirilmesi tavsiye edilmiştir (The National Archives, 2021b, s. 2). Kapatma süreleri, hassasiyet zaman içinde azaldığından, belgenin bitiş tarihinden itibaren tanımlanmış bir süre için olmalıdır. Belgelerin erişime sunulma tarihinin belirlenmesi mümkün olmadığı durumlarda, kapatmaya devam edilmesinin gerekli olup olmadığına karar verilmelidir. Bu karar, ilgili birim tarafından yeniden gözden geçirileceği ileri bir tarih olarak belirlenmelidir. Yaygın kapatma süreleri kişilerle ilgili olanlar için "ömür boyu" veya yeniden inceleme için on yıllık dönemlerdir (The National Archives, 2015, s. 7; The National Archives, 2021a, s. 3). Bazı görüşlerde, bu süre 30 yıl olarak ifade edilmektedir. Eğer 30 yıl sonra hala önemli sorunların yaşanacağı hissediliyorsa bu bilginin bireyin yaşamı boyunca yayılması da aynı etkiyi yaratacaktır. Bir belgedeki bilginin ne kadar süreyle önemli bir soruna yol açacağı konusunda daha fazla öznel tartışmaya bağlı kalmak yerine, daha basit ve nesnel ölçütler kullanılması gerekir

(Thompson ve Kaarst-Brown 2005, s. 252). Bu bağlamda standart izleme dönemlerinin ilgili hassas bilgi türü doğrultusunda oluşturulması, zamana bağlı ortaya çıkacak problemlerin çözülmesine yardımcı olacaktır.

Zamana bağlı olarak hassasiyet değerlendirmesi, bağlam unsurları çerçevesinde zorluklar oluşturmaktadır. Belge konusunun zamanla önem kaybetmesi veya önem kazanması; belgede adı geçen kişilerin konum-mevki-görev faktörleri doğrultusunda zamanla bürokratik, siyasî ya da kamu tanınırlığı yüksek kişiler haline gelmesi; uluslararası ilişkilerin zaman içinde değişmesi; zamanla sosyal, siyasî ve kültürel farklılıkların meydana gelmesi hassas bilgi içerikli belgelerin hassasiyet durumlarını pozitif veya negatif yönde etkileyebilir. Bu durum belgenin üretim aşamasında hassas olarak belirlenmesi ve gizlilik derecesinin oluşturulmasını zamana karşı anlamını yitirmesi olarak ifade edilebilir. Bunun dışında hukukî varlık, gizlilik ve hassasiyet değerlendirmesinin uygulanabilmesi için gereklidir. Örneğin Osmanlı dönemi arşiv belgelerini içeren Osmanlı Arşivi'nde yer alan belge ve belge gruplarına yönelik bir gizlilikten ve hassasiyetten bahsetmek çoğunlukla mümkün değildir. Ancak son dönem siyasî ve yönetimsel faaliyetler, kişi ve ailelere ait belge gruplarının içeriği oluşabilecek etki bakımından ayrıca değerlendirilebilir.

Hassasiyet, tarihsel olmamak ile güncel bir bakış açısıyla sürekli değişime açık olarak değerlendirilmesi gereken zorlu bir süreçtir. Değişen siyasî koşulların ikili ülke ilişkilerindeki hassasiyete etkisi bulunmaktadır. Örneğin Brexit müzakerelerine duyulan ihtiyaç, daha önce yapılan bazı yorumların artık Birleşik Krallık'ın AB'den ayrılmadığı duruma göre daha hassas olabileceği anlamına gelmektedir (McDonald, McDonald ve Ounis, 2019, s. 3).

Bunun dışında açıklanma zamanı birtakım ticarî risklere sebebiyet verecek belgeler için de aynı durum söz konusudur. Şirketler için önemli piyasa sonuçları olan bir ticarî anlaşmayı açıklayan belge resmî duyurudan önce hassastır. Duyurunun ardından

kamuya açık bir bilgidir. Aynı şekilde, kamu sektörü bağlamında, bir ekonomi veya ticaret politikası oluşturulurken çok hassas olabilir, ancak ortaya çıkan politika yayınlandıktan veya yasalaştıktan sonra hassas değildir (Moss ve Gollins, 2017, s. 14). Bu bağlamda, zamanın hassasiyet oluşumu için önemli ve dikkat edilmesi gereken nokta olduğu anlaşılmaktadır

III.2.3. Belge Hacmi, Kaynak ve Bütçe

Kamu kurumlarında üretilen ve kullanılan belge miktarında yaşanan artış değerlendirme işlemlerini zorlaştırmaktadır. Özellikle elektronik belge yönetim sistemlerine (EBYS) geçilmesi, çok sayıda belgenin üretilmesini kolaylaştırırken birikmekte olan belge yığınının değerlendirme, analiz, koruma ve yetkisiz erişim ihlallerini önleme süreçlerini karmaşık hale getirmektedir. Değerlendirme sürecinin odak bir yönünü oluşturan hassas bilgi içerikli belgeler söz konusu olduğunda bu durum ayrıca zorluk çıkarmaktadır. Fiziksel ortamdaki belgeler, değerlendiriciler tarafından el yordamı (*manuel*) olarak geleneksel bir değerlendirme işlemine tabi tutulmaktadır. Elektronik belgeler için ortama bağlı farklılıklar bulunsa da büyük ölçüde benzerdir. Her belge özelinde yapılan bu işlem, hassas bilgi içerikli belgeler için daha fazla zamana, teknolojik altyapıya ve uzman personele gereksinim duyulan kaynak ve bütçe planlamasına yük oluşturmaktadır.

Hassasiyet değerlendirmesi, uzmanlık gerektiren, karar verme süreçlerinde çoğunlukla geleneksel yöntemlerinin kullanıldığı bir süreçtir. Bu sürecin büyük belge yığınlarına karşı yürütülmesi, işlemlerin yavaşlamasına, birikmelerin kademeli olarak artmasına sebebiyet vermektedir. Hacim sorununa bağlı olarak değerlendirme için gelişmiş teknolojik altyapının oluşturulması, güvenli bir ortamın kurulması ve sürdürülmesi, mevcut bilgi sistemleriyle entegrasyonun sağlanması gerekir. Belgelerin hassasiyet derecesine uygun güvenlik seviyelerinde yönetilmesi, personel, fiziksel alanlar, bilgisayar donanımı, işletim ve ağlar gibi bilgi sistemlerine yönelik çeşitli altyapı

gereksinimlerini ortaya çıkarmaktadır (Kaymak ve Külcü 2024, s. 247). Bu bağlamda her belgeyi baştan sona incelemek pratik olmadığından, hassas bilgilerin tespitinde gözden kaçmalar meydana gelebilir.

Belge hacmi, değerlendirme sürecinde insan hatası olasılığını artırarak yorgunluk ve aşırı bilgi yüküyle kritik ayrıntıların fark edilmemesine sebep olabilir. Daha büyük hacimli kamu belgelerinin ele alınması, değerlendirme için daha fazla personel, zaman ve maliyet gerektirir (McKechnie ve McDonald, 2024, s. 1). Hata oranı, değerlendirmenin yardımcı araçlar kullanılarak yapıldığı sistemler/yazılımlar için de geçerlidir. Hassasiyet değerlendirmesi için kullanılan otomatik araçlar, yanlış pozitifler[40] (hassas olmayan bilgilerin yanlışlıkla hassas olarak tanımlanması) veya yanlış negatifler (hassas bilgilerin eksik olması) üretebilir. Doğruluk oranının artırılmasını sağlamak, hem fiziksel hem de elektronik ortamdaki büyük belge toplulukları ile zorlaşmaktadır.

III.2.4. Mevzuat

Mevzuat, bilgileri korumak, güvenlik çerçevesi çizmek ve bilgi güvenliğini tehlikeye atan kişi veya kurumlar için yasal sonuçlar oluşturarak koruyucu bir görev üstlenmektedir. Hassas bilgiler daha önce belirtildiği üzere hukukî düzenlemelerde çeşitli kavramlar ile yer bulmuştur. Bu düzenlemelerde hassas bilgiler, genellikle sayılma yoluyla aktarılarak örneklemeler yapılmıştır. Ancak hassasiyetin sayılarak listelenmesi veya konulara ayrılması, bağlamsal faktörlere bağlı sınırsız hassasiyet senaryolarının göz ardı edilmesi anlamına gelmektedir. Sadece üst mevzuat düzenlemelerinde sayılan konu veya durumlar hassasiyet çerçevesini daraltmaktadır.

[40] Yanlış pozitif sonuca bir örnek olarak, e-posta arşivlerindeki hassas bilgileri değerlendiren ePADD yazılımının bir hatası gösterilebilir. Örneğin, ePADD, alışveriş listesinde “mantar” kelimesini gördüğünde, bu kelimeyi uyuşturucu kategorisinde değerlendiriyor çünkü yazılım, sözlük anlamında 'mantar' kelimesini uyuşturucu olarak sınıflandırmaktadır (Jaillant, 2022b, s. 433).

Hassas bilgilerin mevzuat düzenlemelerinde hangi koşullarda işleneceği ifade edilmektedir. Kamu yararına yürütülen bir görev, resmî yetkinin kullanılması veya meşru bir menfaat gibi alternatif bir hukukî dayanağın daha uygun olması halinde, arşiv hizmetlerinin veri sahiplerinden onay alması zorunlu değildir. Verilerin kamu yararına arşivleme amacıyla daha fazla işlenmesi, uyumlu bir yasal işleme olarak kabul edilmektedir. Bu nedenle herhangi bir ek yasal dayanak gerekmez. Bu, öncelikle kurum içi arşiv hizmetlerine sahip kuruluşlar için geçerli olmaktadır (The National Archives, 2018, s. 16). Ancak bir kişinin dinî inancının hassas bir kişisel bilgi olduğu ve hukuka uygun bir dayanak olmaksızın işlenemeyeceği açık olsa bile, dinî bayram izinlerinin hassas kabul edilip edilmeyeceği açık değildir. Ayrıca veri sorumlularının bu tür kişisel bilgileri daha fazla koruma altında saklama yükümlülüğü altında olup olmadığını bilmek kolay değildir. Bazı mevzuatlarda yer alan ancak bazı mevzuatlarda göz ardı edilen kategoriler (sosyal ihtiyaçlar gibi) için, daha fazla yönlendirme olmaksızın bilgilerin hukuka uygun şekilde nasıl işleneceğinin yorumlanması daha da zordur (Belen-Sağlam, Nurse ve Hodges, 2022b, s. 9). Arşivciler bilgi edinme hakkı ve veri koruma mevzuatı hükümleri çerçevesinde dijital çağda mahremiyet ve gizlilik konusunda [artan endişelerle giderek büyüyen] bir dizi yasaya uymak zorundadır. Bu kanunların yorumlanması ve uygulanması, arşivcilerin erişim sağlama görevini karmaşık hale getirmektedir (Lemieux ve Werner, 2024, s. 3).

Mevzuat ve bağlı düzenlemelerde (tebliğ ve talimatlar, usul ve esaslar, yönergeler vs.), hassas bilgi çerçevesinin ve hassas bilginin hangi koşullarda işleneceğinin kapsamlı bir yapıda olmaması, değerlendirme sürecinde sadece belirli unsurların hassas olarak değerlendirilmesine yol açmaktadır. Değerlendirme sürecinde mevzuatta sayılan hassasiyetler ve bilgi işleme koşullarına ek olarak bağlam hassasiyet oluşumu ve işleme süreçlerinde büyük bir etkiye/zorluğuna sebep olmaktadır.

III.2.5. Sosyal ve Kültürel Farklılıklar

Belirli konular farklı kültürlerde hassas veya tabu olabilir. Bazı toplumların (Örneğin Amerika, Avrupa ülkeleri) kültürlerinde kişisel bilgiler konusunda nispeten yüksek düzeyde bir açıklık söz konusu olabilir ve bireyler yaşamlarıyla ilgili ayrıntıları kendi rızası ile paylaşabilir. Bunun aksine, mahremiyete daha fazla önem veren toplumlarda, kişisel konular daha özel kabul edilmekte ve bu tür bilgiler daha seçici bir şekilde ifşa edilmektedir. Bir kişi, kültür ya da durum için hassas olan bir konu başka bir kültürde benzer şekilde algılanmayabilir (Fule ve Roddick, 2004, s. 162). Mevzuat düzenlemelerinde sayılan hassas konuların seçimine ilişkin hukukî tercih, büyük oranda veri türlerinin hassas verilere dönüşmesinde etkili olan toplumsal değer yargılarının değişken olmasından ve kültürel kodlara göre kaynaklandığı söylenebilir (Bulut, 2020 s. 138). Bir ülkede evrensel kişisel tanımlayıcılar hem zararsız hem de yararlı olarak kabul edilirken, başka bir ülkede son derece hassas olarak kabul edilebilir, kullanımları kısıtlanabilir, hatta yasaklanabilir. Bazı ülkelerde, gruplar ve benzer varlıklarla ilgili verilere koruma sağlanırken, başka bir ülkede bu tür bir koruma tamamen mevcut olmayabilir (OECD, 2002, s. 38).

Sosyo-kültürel faktörler belirli verilerin hassasiyetini önemli ölçüde değiştirebilir. Bir kişinin yaşı Kuzey Amerika'da mahremiyet olarak kabul edilirken, bazı Asya ülkelerinde olmayabilir (Geng ve diğerleri, 2011, s. 164). Otoriter veya teokratik toplumlarda din, cinsel tercih, siyasî görüş yüksek derecede hassas bilgiler olarak görülmektedir. Cinsel yönelim, teokratik hukukunun uygulandığı ülkelerde çok daha hassastır. Algılanan hassasiyet, hem toplumlar veya etnik gruplar arasında hem de bu gruplar içerisinde büyük farklılıklar göstermektedir. Bazı özellikler sadece ayrımcılık potansiyeli nedeniyle hassastır; din, ırk ve etnik grup bilgisi bu sebeple çoğu veri koruma kanununda hassas olarak sınıflandırılmaktadır. Yanlışlıkla ya da kötü niyetle ifşa edildikten sonra kötüye kullanım potansiyeli de hassasiyet değerlendirmelerini

etkilemektedir. Din, yüksek derecede mezhep çatışmasının yaşandığı bölgelerde oldukça hassas bir konudur (Rumbold ve Pierscionek, 2018, s. 57).

Mahremiyet evrensel bir kavram gibi görünse de neyin özel olduğu ve hangi koşullar altında olduğu insan grupları arasında ve zaman içinde büyük farklılıklar göstermektedir. Örneğin, ABD'de Federal Soruşturma Bürosu'nun (Federal Bureau of Investigation/FBI) belgelerini değerlendiren arşivcinin bile dosyalarda gelir vergisi beyannamesi bilgilerini görmesine izin verilmezken, İsveç'te ise aksine gelir vergisi bilgileri kamuya açıktır (Henttonen, 2017, s. 288). Değerlendirici kişisel veya hassas veriler içeren belgeleri değerlendirirken şeffaflık ve kültürel normlara saygı arasında bir denge kurmakta zorlanabilir. Belirli konuları çevreleyen kültürel nüansların farkında olmamak veya bunlara karşı hassasiyet göstermemek, içeriğin gerçek önemini veya sonuçlarını değerlendirmeyi zorlaştırmaktadır. Özellikle yerel gupların veya belirli toplulukların farkında olduğu hassasiyetlerin değerlendirilmesi kurumlar ve değerlendiriciler için kritik bir süreçtir. Bir kişinin tuttuğu futbol takımı, dinî veya siyasî sempati gibi başka şeylere işaret etmesi durumunda sorun teşkil edebilir. Örneğin Kuzey İrlanda veya İskoçya'nın batısında, Celtic veya Rangers'ı desteklemek sırasıyla Cumhuriyetçi veya muhafazakâr olmakla güçlü bir şekilde bağlantılıdır (Rumbold ve Pierscionek, 2018, s. 56). Doğrudan olmamak ile birlikte böyle bir ilişkinin kurulması hassasiyet oluşumu için yeterlidir.

Hassasiyet bir kültürden diğerine farklılık göstermek ile birlikte aynı toplumsal yapı içerisinde kültürel yozlaşmaya, duyarsızlaşmaya veya artık hassas olarak algılanmamaya bağlı olarak değişmektedir. Örneğin Avrupa'da bazı ulusal arşivler evlilik dışı çocuklara yönelik bilgileri içeren belgeleri geçmişte redakte ederek yayınlarken artık günümüzde böyle bir uygulamaya ihtiyaç duymamaktadır. Dolayısıyla toplumsal ahlak ve etik anlayışındaki dönüşümler, hassasiyet tespitine ve erişime doğrudan etki etmektedir.

Hassasiyet değerlendirmesi sürecinde değerlendirici, yaşadığı toplumun bir üyesi olarak sosyal-kültürel farklılıkları tespit edebilmelidir. Ancak zaman içerisinde toplumlarda değişen hassasiyet algısı, yerel ölçeklerde bile olsa farklılaşması hassasiyet değerlendirmesini zorlaştırmaktadır. Değerlendiriciler, hassasiyetin hem yasal hem de kültürel boyutları olduğunu, araştırmacıları kültürel açıdan hassas malzemelerin erişim sınırlamalarına uygun bir şekilde kullanılmasını teşvik etmelidir (McCardwell, 2014, s. 4). Hassasiyet değerlendirmesi sürecinde, bireylerin ve toplumların kendi iç dinamiklerine ek olarak kültürel çeşitliliğin dikkate alınması beklenmektedir.

III.2.6. Kişisel Bakış ve Deneyim

Değerlendirme, önyargıdan ve öznellikten bağımsız olmamakla birlikte günün kültürel değerleri esasınca değerlendiricilerin eğilimlerine yansımaktadır (Johns, 2017, s. 32). Kişisel bakış açısı ve deneyim, belgelerin hassasiyet değerlendirmesini adalet ve güvenilirlik açısından olumsuz yönde etkileyebilmektedir. Değerlendirme, birisinin belgenin içeriğini yorumlamasını gerektirdiğinden son derece insan yargısına ve uzmanlığına bağlıdır (Thompson ve Kaarst-Brown, 2005, s. 248; Narvala, 2024, s. 3). Değerlendirme sürecinde, objektif ve tarafsız yaklaşılması beklenmektedir. Ancak değerlendiricinin kişisel bakış açısı ve deneyimleri kişinin yargısını istemeden de olsa şekillendirir. Bu noktada erişim ve mahremiyet arasındaki dengeyi gözetmek arşivciler arasında görüş ayrılığı, anlaşmazlık ve uyumsuzluğa sebep olacak düzeyde olabilir (Dressler ve Kearns, 2023, s. 175). Özellikle hassasiyet değerlendirmesi söz konusu olduğunda doğrudan etki edebilmektedir. Değerlendiriciler kişisel inançlarına, kültürel geçmişlerine veya deneyimlerine dayanarak belirli bir siyasî veya sosyal bakış açısıyla birbirlerinden farklı hassasiyet yargılarına ulaşabilmektedir. Karar verme sürecine etki edebilecek kişisel inanç ve görüşler farklı düzeyde bulunsa da çalışma ortamında yer alabilecektir (Dressler ve Kearns, 2023, s. 177). Hassasiyet yargısı; öğrenmenin, deneyim

süresinin, toplumsal kültürün ve çevre koşullarının bilinçsiz önyargılarını taşıyabilmektedir. Bu durum hassasiyetin tespitine, erişim kısıtlamalarına ve kapatma kararlarına da yansımaktadır. Mahremiyeti ve hassasiyeti tehdit eden bilgileri tespit etmek daha da zorlaşmaktadır. Çünkü belirleyici olan bireysel gerçeklerin oluşturmuş olduğu bilgi birikimidir (Henttonen, 2017, s. 288). Bir belge grubundaki tüm belgeler, tek bir kişi tarafından incelenmesi gerektiğinde, hassasiyet yargısı uzman değerlendiricinin deneyimine bağlı olarak değişebilmektedir. Hassasiyet değerlendirmesi, örtük bilgi birikiminin oluştuğu, ait olunan toplum içerisinde ilgili mevzuat hükümlerinin farkında olunduğu uzmanlık gerektiren bir süreçtir. Bu sebeple kişiler arası aktarılabilirliği zamana bağlıdır. Nesnel bir değerlendirme işleminin yapılamaması, belgenin somut göstergelere dayanmayan bağlamsal farklılıklar içermesiyle de zorlaşmaktadır. Bu sebeple kişisel değerlendirmelerden ziyade bu konuda komisyon veya çalışma grubu oluşturularak (Rukancı, Anameriç ve Başar, 2021, s. 46) değerlendirme işleminin farklı kişiler tarafından kontrolüne, değerlendiricilerin belge üst veri bilgisine eklenmesine ve değerlendirilen belgenin periyodik aralıklar ile tekrarına gereksinim duyulmaktadır.

III.3. Geleneksel Değerlendirme ve İnsan Değerlendirici

Değerlendirme, değerlendiricilerin bir belgedeki hassas bilgilerin keşfini amaçladığı hangi belgelerin kamuya açıklanabileceğini belirledikleri, materyalin entelektüel içeriğine erişim sağlarken bireysel mahremiyet çıkarlarını korumayı hedefledikleri zorlu bir süreçtir. Değerlendirme sürecinde hem erişim hem de mahremiyete saygı gösterilerek tabi olunan ilgili mevzuatın sınırları dahilinde hareket edilmelidir (International Council on Archives, 1996, Code 7). Değerlenme, geleneksel olarak uzman bir değerlendirici (arşivci/belge yöneticisi) tarafından belgelerin tek tek kontrol edildiği, diğer arşiv işlemlerinin kaynaklandığı [ilk sorumluluk] olarak ifade edilmektedir (Cox ve Samuel, 1988, s. 29; Cook, 2011, s. 174). Değerlendiriciler bu süreçte mahremiyet-gizlilik

gereksiniminin farkında olarak belgelerin kullanımını teşvik etme sorumluluğuna sahiptir. Geleneksel olarak uygulanmakta olan değerlendirme işleminde kâğıt tabanlı kamu belgeleri tipik olarak, her dosyanın birbiriyle ilişkili belgeleri içerdiği yapılandırılmış bir mantıksal dosya planı içinde depolanır ve arşivlere aktarılır. Kâğıt belgeler için hassasiyet değerlendirmesi, potansiyel olarak hassas bilgi içerdiği tespit edilen kâğıt her bir dosyanın sayfa sayfa el yordamı olarak gözden geçirilmesini içeren geleneksel bir yaklaşımla uygulanmaktadır. Dosyanın içeriği kontrol edilir ve bir belge hassas bilgiler içeriyorsa, belge kısmen düzeltilir (anonimleştirme veya redaksiyon) veya dosyadan kaldırılarak erişime (süreli/süresiz) kapatılır. Hassasiyeti değerlendiren kişi, redaksiyon sürecinde doğru işlemlerin yapılabilmesi adına kapsamlı bilgi sağlayabilmesi için bir belgedeki hassas metnin tüm pasajlarını tanımlamalıdır. Bir erişim sorumluluğu olarak edinilen belgede hassas bilgilerin nerede bulunabileceğini bilmesi ve uygun kısıtlamalar geliştirmesi gerekmektedir (Pugh, 1992, s. 56). Ayrıca dosya içerisinde erişim kısıtlaması olan belgelerin kullanıcıya bildirilmesi etik bir sorumluluktur (International Council on Archives, 1996, Code 3). Bu sebeple, değerlendirici incelenmekte olan belgelerin her birindeki metnin tamamını okumalıdır. Dosyanın büyük miktarda hassas bilgi içerdiği görülürse dosyanın tamamı kapatılır (Moss ve Gollins, 2017, s. 13; McDonald, 2019, s. 3, 155). Bu süreçte değerlendiricilerin genellikle ilgili bölümün hassas olabilecek konuları hakkında bilgi sahibi olması beklenmektedir (Allan, 2014, s. 14). Değerlendiricinin gizlilik mevzuatındaki yeni gelişmelerden haberdar olma ve bunun uzun vadeli sonuçlarını dikkate alma sorumluluğu bulunmaktadır (McCarville, 2004, s. 150). Uzman değerlendirici bir belgeyi incelediğinde, belgenin herhangi bir hassas bilgi içerip içermediği konusunda bir hassasiyet yargısı ortaya koymaktadır. Bu yargı, birden fazla bilgi veya özellik içerebileceğinden son derece insan yargısına bağlıdır (Thompson ve Kaarst-Brown, 2005, s. 248; Brown, 2018, s. XVI). Çünkü bir kişinin belgenin içeriğini yorumlamasıyla ulaşılmaktadır. Bu noktada danışma

konseylerinin/gizlilik komisyonlarının rolü de bulunmaktadır. Genellikle ulusal arşivler içerisinde kapalı veya kısıtlı olarak devredilmiş fonlara yönelik – bazı durumlarda kurumlar ile irtibat halinde – incelemeler yürütmektedir. Üzerinde mutabık kalınmayan belgelere veya gizlilik kararlarını göz geçirmeye işlevleri yürütmesi rağmen çoğunlukla kurumlardaki değerlendiricinin yönetimine bırakılmıştır. Bu bağlamda hassasiyet değerlendirmesi sürecinde arşivciler ve rol alan belge yöneticilerinin yapması gerekenler aşağıda özetlenmektedir:

- Değerlendirici paydaşların geniş ölçekli katılım sağladığı istişarelerde bulunmalıdır.
- Değerlendirici belgelerdeki hassas nitelikteki bilgileri tanımlayarak kimin hangi koşullarda erişebileceğini belirleyen politika ve prosedürler oluşturmalıdır
- Değerlendirici ihtiyaç duyulması halinde hangi danışmanlık ve yardım hizmetlerinin mevcut olduğunu öğrenmelidir (Mathers, 2000, s. 65).

Değerlendiriciler gizliliğin doğuştan gelen temel bir hak olduğunu ve yasalarca onaylandığını kabul ederek, kamusal ve özel yaşamları belgelenen bağışçıların, bireylerin, grupların veya kuruluşların çıkarlarını korumaya yönelik prosedür ve politikalar oluştururlar. Değerlendirici, mahremiyetin hem yasal hem de kültürel boyutları olduğunu kabul eder, araştırmacıları danışmaya teşvik ederek, kültürel açıdan hassas materyallerin kendi gözetimleri altında kullandırır (Society of American Archivist, 2011). Değerlendiricinin arşiv yönetimine özgü tüm sınırlardan çok daha geniş bir bağlamda, mahremiyet-erişim arasındaki fikir ayrılığı ve uyuşmazlıklar arasındaki bu dengeyi sağlamaya çalışması beklenmektedir (Sillitoe, 1988, s. 5; Dressler ve Kearns, 2023, s. 175). Bu dengenin kâğıt belgeler ile birlikte elektronik belgeler üzerinde kurulması günden güne zorlaşmaktadır.

Kamu kurumları başta olmak üzere pek çok kurumsal yapı işleyişlerinin çoğunluğunda elektronik belge kullanımına geçmiştir. Elektronik belgelerin artan hacmi ve karmaşıklığının (format çeşitliliği, dinamikliği, ağ bağımlılığı vs.) bir belgenin el yordamı olarak değerlendirilmesini ve analiz edilmesini zorlaştırmaktadır. Kâğıt tabanlı kamu belgelerinin hassasiyet değerlendirmesi el yordamı ile yürütülmektedir. Ancak hassasiyet değerlendirmesinin kâğıt belgelerde olduğu gibi elektronik belgelerde uygulanması konusunda farklı yaklaşımlar bulunmaktadır. Elektronik kamu belgelerinin hassasiyet değerlendirmesine yardımcı olması için, hassas bilgileri otomatik olarak tanımlayan yeni teknolojilere ihtiyaç olduğu yaygın olarak ifade edilmektedir (Sánchez, Batet ve Viejo, 2012; Berardi ve diğerleri, 2015; McDonald ve diğerleri, 2017; McDonald, 2019; Narvala, McDonald ve Ounis, 2022b). Bu bağlamda kâğıt belgelere uygulanan değerlendirme yaklaşımının ötesinde dijital bir değerlendirme sürecinin ortaya çıktığı ifade edilmektedir.

III.4. Dijital Değerlendirme ve Yardımcı Araçlar

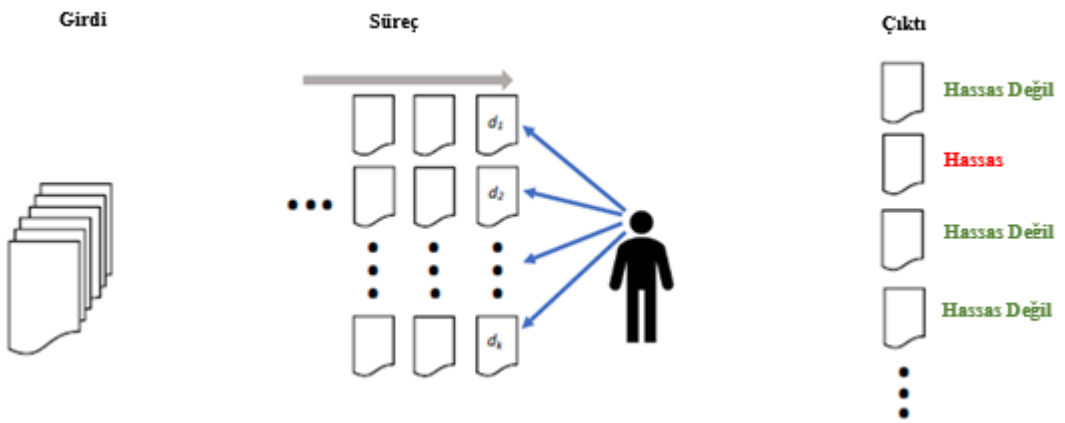
Son yıllarda kamu ve özel kurumlarda kâğıt belgeler yerine e-postalar ve kelime işlem belgeleri gibi doğuştan dijital belgeler daha fazla kullanılmaya başlanmıştır. Bu belgelerin artık kamuya sunulması ve dolayısıyla hassasiyet açısından değerlendirilmesi gerekmektedir. Elektronik ortamda üretilen belgelerin ortaya çıkarmış olduğu zorluk yenidir. Kâğıt belgelerin değerlendirildiği analog ortamda, hassasiyet değerlendirmesi genellikle içeriğin kontrol edilerek rahatsız edici öğelerin redaksiyonu veya sayfaların/paragrafların çıkarılması usulüne göre yapılmaktadır[41]. Kâğıt belgelerin

[41] Analog/kâğıt ortamda yapılan ve depolanan bu sürecin, elektronik ortamda muhafaza edilmesi gerektiğine dair BM Arşiv ve Belge Yönetimi Birimi'nin önerisi bulunmaktadır. BM'ye göre hassas belgeler her zaman resmî olarak kurulmuş elektronik belge yönetim sistemlerinde veya güvenli ağ sürücülerinde saklanmalıdır. Bu belgeler bilgisayar sabit diskleri veya güvenlik kontrolleri bulunmayan C sürücüleri gibi yerlerde tutulmamalıdır (Birleşmiş Milletler, 2024b).

değerlendirme süreçleri köklü olduğundan elektronik belgeler için benzer süreçlerin uygulanması konusunda endişeler bulunmaktadır. Bu endişeler arasında değerlendirme, seçim ve hassasiyet değerlendirmesi süreçleri daha büyük bir paya sahiptir (The National Archives, 2016, s. 25). Örneğin, kâğıt ortamın aksine elektronik belgeyi inceleyen insan değerlendirici, metindeki belirli anahtar kelimeleri tespit ederek hassasiyet çıkarımı yapıyorsa benzer bilgiler için gelecekteki hassasiyet yargılarına rehberlik edecek kurallar oluşturabilir ve algoritmalar geliştirebilir (Thompson ve Kaarst-Brown, 2005, s. 248). Nitekim günümüzde bu öngörüye dayalı olarak uygulamalar yapılmaktadır. Örneğin kişisel tanımlanabilir yapılandırılmış verilerin el yordamı olarak tanımlanması, hataya açık ve yoğun kaynak gerektiren bir süreçtir. Otomatik yöntemler kullanarak alan düzeyinde veri doğrulamayı, model eşleştirme tekniklerini kullanarak kişisel tanımlanabilir verileri gizleyen, maskeleyen ve anonimleştiren işlemleri gerçekleştirmeyi içerebilir (Johnson ve diğerleri, 2016, s. 12).

Dijital değerlendirme (*Digital Appraisal/Assesment*), elektronik ortamda üretilen veya dijitalleştirilerek elektronik ortama aktarılan belgelerin arşivsel değerlendirme teorileri esasınca incelendiği bir süreçtir. Dijital değerlendirme kavramının aynı arşiv teorisi tarafından beslendiği için kâğıt ortamdaki geleneksel değerlendirmeden farklı olmadığı düşünülmektedir. Ancak aynı sürecin farklı bir belge formatında olması ayrı bir süreç olarak görülme eğilimini ortaya çıkarmaktadır. Bu konudaki profesyonel görüşler geleneksel ve dijital olarak ikiye ayrılmıştır. Dijital değerlendirme savunucuları eski kavramların elektronik belgelerle başa çıkmak için yetersiz olduğuna ve yenilerinin tasarlanması gerektiğine inanmaktadır. Bunun aksine geleneksel bakış açısına göre kâğıt ve elektronik belgelerin çok farklı olmadığı, arşiv teorilerinin ve kavramların medyadan (ortam) bağımsız olarak kullanılacağı ifade edilmektedir (Sloyan, 2016, s. 22, 23; Johns, 2017, s. 32). Genel olarak özgünlük, kaynak ve bağlam gibi temel arşivcilik ilkelerinin ortamdan bağımsız olduğu, belgelerin fiziksel biçimi ya da formatından ziyade içeriğine,

bağlamına ve ilişkilerine odaklanılarak temel ilkeler korunduğu sürece arşiv teorilerinin elektronik belgelere uygulanabileceği savunulmaktadır. Dijital değerlendirme savunucuları ise elektronik belgelerin üretim biçimi, dolaşımı, dinamikliği, sık sık sürüm güncellemeleri ve sabit fiziksel varlıklarının bulunmaması sebebiyle geleneksel değerlendirmeden ayrıştığını öne sürmektedir. Kâğıt tabanlı belgeler için oluşturulmuş geleneksel değerlendirme yaklaşımları dijital materyallerin karmaşıklığını tam olarak ele almayabilir. Bu sebeple dijital ortamın beraberinde getirdiği farklılıkları karşılayan dijital değerlendirme yaklaşımları ve bu sürece yardımcı araçlar gelişmiştir. Genel olarak, kâğıt belgeler için kullanılan el yordamı değerlendirme yaklaşımları doğuştan dijital belgelerin hacmi ve yapı eksikliği göz önüne alındığında dijital ortama iyi bir şekilde aktarılamayabilir. Doğuştan dijital belgeler, değerlendirme zorluklarının üstesinden gelmek için teknolojiden yararlanma fırsatları sunmaktadır (The National Archives, 2016, s. 26). Başka bir ifade ile büyük ölçekli dijital arşivlerdeki hassas içeriklerin tespit edilmesi, manuel yöntemlerle gerçekleştirilemeyecek kadar karmaşık bir süreçtir; bu sebeple, kurumlar inceleme sürecini kolaylaştırmak ve büyük hacimli dijital belgelerin kilidini açmak için giderek artan bir şekilde hesaplamalı tekniklere başvurmaktadır (Yeo, 2018, s. 57; Jaillant ve Rees, 2023, s. 571; Narvala, 2024, s. 16).



Şekil 2. Dijital Hassasiyet Değerlendirmesi Girdi, Süreç ve Çıktı (McDonald, 2019, s. 2)

Hassas bilgi içeren elektronik belgelerin değerlendirme süreci, dijital hassasiyet değerlendirmesi (*Digital Sensitivitiy Review*) olarak ifade edilmektedir. McDonald bu sürecin üç aşamada gerçekleştirebileceğini (Şekil 2'de) belirtmektedir. Sürecin girdi bölümünü arşive aktarılacak belge (d=document: belge) grupları oluşturmaktadır. Değerlendirici (insan) elektronik belge gruplarını tek tek okuyarak (süreç) her bir belge ile ilgili hassasiyet yargısına (hassas/hassas değil) varmaktadır. Hassasiyet yargısı, belgelere ilişkin geçerli hassasiyet kategorisi, belgenin hangi bölümlerinin hassas olduğu ve nedenine ilişkin açıklama içermektedir (McDonald, 2019, s. 2). İlk bakışta geleneksel değerlendirme uygulamasında olduğu gibi değerlendirici tarafından tek tek kontrolün sağlandığı benzer bir süreç olarak gözükmektedir. Ancak taşıyıcı ortam, üst veri yapısı, redaksiyon-maskeleme araçlarının farklılaşması ve dolaşım gibi unsurlar gelenekselden ayrıştırmaktadır. Dijital değerlendirme artan belge hacmi, elektronik belgelerin karmaşık ve soyut yapısından dolayı daha yavaş ilerleyen bir süreçtir. Bu sebeple hassasiyet değerlendirmesi sürecinde yardımcı araçlar ortaya çıkmaktadır. Değerlendirilmesi gereken belgelerin hacmi ve dijital ortamın karmaşık yapısı sebebiyle dijital değerlendirme kapsamında teknoloji yardımlı değerlendirme (*technology-assisted review*) yaklaşımlarına ihtiyaç duyulmaktadır. Değerlendirme, seçim, hassasiyet değerlendirmesi ve transfer açısından kâğıt belgelere yapılan uygulamalar elektronik belgeler için yeterli olmamaktadır. Kâğıt belgelerden farklı olarak, elektronik belgelerde üst veriler parçalanmış ve dağınıktır. Bu dağınık yapı, özellikle e-posta arşivleri gibi ilişki ağının zor kurulduğu ve hassas bilgi içerik tespitinin çeşitli yönlerden karmaşıklaştığı dijital veri setlerinde, gizlilik yönetimini daha da zorlaştırmaktadır. Bir e-posta koleksiyonu üzerinde işlem yaparken, genellikle hassas bilgiler içeren mesajları tespit etmek[42] ve bunlara erişimi sınırlamak hedeflenir (Schneider ve diğerleri 2019, s. 317). E-

[42] E-posta arşivlerindeki hassas verileri tespit etmek ve işlemek amacıyla ePADD yazılımı tasarlanmıştır. Bu yazılım, özellikle kişisel bilgileri, gizli içerikleri ve yasal olarak korunması gereken verileri hızlı bir şekilde tanımlayıp kısıtlamayı sağlamaktadır. Daha fazla bilgi için bkz. Schneider ve diğerleri (2019).

posta verileri üzerindeki hassas bilgi tespiti ve anonimleştirilme uygulamaları, kullanıcıların veri koruma yasalarıyla uyumlu araştırmalar yapabilmesini sağlamaktadır. Bunun yanı sıra, hassas bilgilerin korunması ve doğru sonuçlara ulaşılması amacıyla makine öğrenmesi algoritmaları aracılığıyla test koleksiyonları ve hassasiyet sınıflandırmaları gibi yöntemler de kullanılmaktadır (Kaczmarek ve West, 2018; Bartliff, Kim ve Hopfgartner, 2024; McKechnie ve McDonald, 2024). Elektronik belgeleri analiz etmek ve bunları paylaşılan niteliklere göre gruplandırmak için yazılımlar bulunsa yalnızca gözden geçirenleri değerlendirme kararlarında destekleyebilir. Elektronik belgelerin soyut ve karmaşık doğasını dikkate alan yeni süreçlere ihtiyaç vardır (Özdemir, 2019, s. 233). Elektronik belgelerin hassasiyet değerlendirmesinin yalnızca yardımcı veya otonom teknolojiler aracılığıyla çözümü, hükümetler ve değerlendiriciler tarafından tutarlı bir güven geliştirene kadar benimsenemez. Bu sebeple, genel olarak erişime açılan tüm kamu belgelerinin, kabul edilebilir bir güven düzeyi sağlanana kadar el yordamı olarak değerlendirmeye devam edeceği kabul edilmektedir (McDonald, 2019, s. 52). Hassasiyet değerlendirmesi sürecinde, kamu kurumlarının gereğinden fazla dijital bilgi tutması, oluşan hacim nedeniyle personel tarafından uzun süre aranması ve hassasiyetin açığa çıkma potansiyelinin yaratmış olduğu riskler bulunmaktadır. Bu durum bilgilerin bazen kurumsal sistemlerin yanlış bölümlerine kaydedilmesi gerçeğiyle daha da artmaktadır (Özdemir, 2019, s. 235). Dolayısıyla henüz insan müdahalesi olmaksızın hassas bilgilerin belirlenmesine yönelik otomatik yaklaşımların öngörülebilir gelecekte insan değerlendiricisinin yerini tamamen alamayacağı kabul edilmektedir (Gollins ve diğerleri, 2014, s. 40; The National Archives, 2016, s. 26; Tough, 2018, s. 177). Dijital hassasiyet değerlendirmesine yönelik yardımcı araçların kullanılması konusunda kabul edilebilir bir güven düzeyi oluşana kadar tüm elektronik kamu belgelerin el yordamı olarak incelenmeye devam edeceğini ifade etmek mümkündür. Elektronik belgelerin

hassasiyet değerlendirmesi zor ve emek gerektirdiğinden sürecin çeşitli yazılımlarla desteklenmesi gerekmektedir (Özdemir ve Cengiz, 2019, s. 281).

Değerlendirme işlemlerinde [gizliliği güçlendiren teknolojilerin[43] (Privacy-enhancing technologies)], dijital araçların/yazılımların (Bulk Extractor[44], Forensic Toolkit, Encase Forensic vs.) kullanımı yaygınlaşmaktadır. Örneğin ABD'de bilgi edinme talepleri doğrultusunda belgelerdeki muhtemel hassas bölümleri tespit eden, redaksiyon önerilerinde bulunan "*FOIA Assistant*" aracı tüm kamu kurumlarda test edilmektedir. Nitekim 2022 yılında bilgi edinme talepleri çerçevesinde 928.300 başvurunun bulunması, yaşanan gecikmelerden kaynaklanan davaların 39 milyon dolarlık zarara yol açması dijital hassasiyet değerlendirmesi araçlarına olan ilgiyi artırmıştır (Summary of Annual FOIA Reports for Fiscal Year 2022; Branting ve diğerleri, 2023, s. 2, 5). Hassasiyet değerlendirmesi sürecini otomatikleştirmeye yönelik ilk yaklaşımlar posta kodu, doğum tarihi, sosyal güvenlik numarası gibi yapılandırılmış/belirli bir biçime sahip veri biçimlerini tarama formülasyonları geliştirerek tespit etmeyi amaçlamıştır (Lemieux ve Werner, 2024, s. 4). Teorik olarak hassasiyet değerlendirmesini belirli bir hassasiyetle ilgili veya yapılandırılmış[45] veri odaklı anahtar kelimelerle manuel olarak sorgular oluşturmak mümkündür. Ancak hassasiyetlerin potansiyel çeşitliliği sebebiyle, her bir hassasiyet türü ve veri biçimi özelinde ayrı sorguların manuel olarak oluşturulması, yönetilemeyecek miktarda/hacimde sonuç kümesiyle

[43] Dijital hassasiyet değerlendirmesi sürecinde gizliliği güçlendiren teknolojileri konu alan çalışma için bkz. Lemieux, V. L. ve Werner, J. (2024). Protecting Privacy in Digital Records: The Potential of Privacy-Enhancing Technologies. *ACM Journal on Computing and Cultural Heritage*, *16*(4), 1-18.

[44] Bulk extractor, özel hesap bilgileri (kredi kartı numaraları), benzersiz özel tanımlayıcılar (sosyal güvenlik numaraları), onaltılık ve Base64 kodlu metinler, internet alan adları, e-posta adresleri, e-posta mesajları ve başlıklar, Ethernet MAC adresleri, JPEG görüntülerinden EXIF verisi, telefon numaraları, URL'ler, arama geçmişleri, sıkıştırılmış dosyalar, Windows hibernasyon dosyası parçaları ve kullanıcı tarafından tanımlanan anahtar kelimeler gibi birçok veriyi tanımlayabilmektedir (Lee ve Woods, 2012, s. 306, 307).

[45]Yapılandırılmış verilerin tespit edilmesine yönelik çabalar, hassas içerik barındıran e-posta üzerinde işlem yapan ePADD yazılımı ile gerçekleştirilmiştir. ePADD'da regex (düzenli ifade) olarak adlandırılan tanımlanmış/yapılandırılmış biçimdeki veriler arama yoluyla incelenmiştir. Bu ifadeler, belirli bir veri dizisini veya örüntüsünü tanımak için kullanılır ve kişisel tanımlanabilir bilgilerin (PII) tespit edilmesine katkı sağlamaktadır. Örneğin, kredi kartı numaraları, banka hesap bilgileri veya vergi numaraları gibi hassas veriler kolayca bulunabilmektedir (Schneider ve diğerleri, 2019, s. 319).

sonuçlanabilmektedir (Sayed, 2021, s. 24). Bu sebeple sürecin daha pratik ve otomatik bir şekilde ilerleyebilmesi ihtiyacı kendisi göstermiş, doğal dil işleme ve makine öğrenmesi teknikleri uygulanmaya başlanmıştır. Özellikle hassas bilgi sınıflamasına yönelik otomatikleştirme uygulamaları gerçekleştirilmiştir. Otomatik hassasiyet sınıflandırması bir veri kümesinin veya parçasının hassas olup olmadığını tahmin etmek için makine öğrenmesi algoritmalarının kullanılması olarak ifade edilmektedir (Narvala, 2024, s. 16). Sınıflama işlemleri başta olmak üzere yardımcı araçların geliştirilmesi/kullanılması düşüncesinin yanı sıra elektronik belgelerin hassasiyet değerlendirmesi konusunda geleneksel yaklaşımlara benzer öneriler de bulunmaktadır. Bu durum hassas bilgilerin gözden geçirilmesine yönelik yaklaşımların hâlâ büyük ölçüde insan bilgisi, yargısı ve ilişkisine bağlı olduğu görüşünden kaynaklanmaktadır (Whyte ve Walsh, 2024, s. 18). Amerikan Kütüphane ve Bilgi Kaynakları Konseyi tarafından yayınlanan rehberde elektronik belgelerin incelenmesi konusunda iki öneri sunulmaktadır. İlki bilinen hassas terimlerin anahtar kelime ile aranmasıdır. Hassas terimler, biriktirilerek veya anımsanarak eşleştirilmek istenmektedir. Bu durum bağlama bağlı hassasiyetler konusunda yeterli değildir. Ancak sınırlı da olsa yardım sağlayabilir. İkinci öneri, belgeyi oluşturan kişinin bilgisinden faydalanmaktır. Çünkü elektronik belgelerin hassasiyet değerlendirmesi üretim aşamasında başlamaktadır. Belgenin üst veri alanında hangi kanunun hangi maddesine göre hassas olduğu ve gizlilik derecesi alanının zorunlu olarak doldurulması gerekmektedir (Cengiz Mater, 2022, s. 63). İkinci öneri belge üreticisinin belge hakkında iyi bilgiye sahip olduğu durumlarda etkili olmaktadır. Belge üreticisinin hafızasının güvenilir olmaması, hassas bilgi konusunda farkındalığının bulunmaması veya ulaşılamaması durumları süreci zorlaştırmaktadır (Redwine ve diğerleri, 2013, s. 7-8). Hem anahtar kelime araması hem de belge üreticisinden yararlanmak kullanışlı bir seçenektir ve uygun olduğunda kullanılmalıdır. Ancak bu yöntemlerin hiçbiri tek başına tam bir çözüm sağlamaz ve birlikte ele alındığında bile

hala birçok boşluk bırakabilir. Hassasiyeti tanımlamak zordur ve tespit ederken yalnızca bilinen hassas kelimeler için anahtar kelime aramasına güvenilmemelidir (Sloyan, 2016, s. 30). Dijital hassasiyet değerlendirmesi sürecinin çıktısı, hassasiyeti incelenen belgeler için hassasiyet yargılarının biriktiği kararlar kümesinin oluşumunu sağlamaktır. Her değerlendirme kararı sonrasında kaydedilen bilgiler, hassasiyet için bir geri bildirim sağlamalıdır. Bu amaçla yazılım araçlarının eğitilmesi ve güncel tutulması, inceleme sonuçlarının düzenli olarak departmanların doğruluk kabul seviyesine uygun olduklarından emin olunması gerekecektir. Hassasiyetler zaman içinde değişebilir ve yardımcı araçlar bu değişiklikler ışığında yeniden eğitilmelidir (The National Archives, 2016, s. 22). Fakat hükümetler hangi belgelerin kamuya açıklanması ya da açıklanmaması gerektiğine karar vermek için otomatik teknolojilere daha fazla güvenmeye başladıkça, hassasiyet belirlenirken karar verme önyargıların eklenmesi riski ortaya çıkmaktadır. Örneğin, belirli bir etnik veya toplumsal grubun üyelerinin terörist olma ihtimalinin daha yüksek olduğunu yanlış öğrenen bir hassasiyet sınıflandırıcısı, bu gruplarla ilgili belgeler için orantısız sayıda kapatma başvurusuna yol açabilir (McDonald, McDonald ve Ounis, 2019, s. 2). Farklı cinsel yönelimlerin paylaşılması, bunlar ile ilgili çeşitli sivil toplum örgütleri, terör gruplarının tanımlanması da farklılık gösterebilmektedir.

Dijital hassasiyet değerlendirmesi konusunda çeşitli araştırmalar ve uygulamalar yürütülmektedir (McDonald ve diğerleri, 2014; Berardi ve diğerleri, 2015; The National Archives, 2016; Moss ve Gollins, 2017; McDonald, McDonald ve Ounis, 2018b). Bu araştırmalarda hassasiyetin tespit ve kategorize edilmesi işlemlerinde kullanılmak üzere geliştirilen araçların yüksek başarı oranları elde ettiğine dair sonuçlar elde edilmektedir. Bu kapsamda hassasiyet değerlendirmesi yapılırken insan başarı oranının makine/yazılım başarı oranına göre daha iyi veya yüksek olacağı kesin değildir. Hata oranı değerlendiriciler açısından deneyim, bakış açısı ve ait olunan kurumsal yapı sebebiyle farklılık gösterecektir. Bununla birlikte her yardımcı veya otonom araçta hata payı,

algoritmaların beslendiği verilerin doğruluk oranı ve hassasiyetin bağlama duyarlı sonsuz senaryo ihtimali esasınca mevcuttur. Algoritmalar, insan yargısının içermiş olduğu öznelliği[46] ve deneyime bağlı karar verme sistemini nispeten nesnel bir zemine taşır. Ancak bu durum verilerin doğruluğuna (hassasiyet bağlamında bu tür bilgilere duyarlı) bağlıdır. Algoritmalar tıpkı bir insana ait öğrenme deneyiminde olduğu gibi ırk[47], etnik köken, cinsiyet, milliyet, gelir, cinsel yönelim, yetenek ve siyasî veya dinî inanç gibi hassas özelliklerle ilgili toplumsal önyargı ve ayrımcılık duygularını miras alabilmektedir (GOV. UK, 2021, s. 8). Bir diğer husus başarı/başarısızlık sorumluluğu ve yeni hassasiyet durumlarının ortaya çıkmasıyla yardımcı araçlara olan güvendir. İnsandan bağımsız bir değerlendirme işleminin uygulanması henüz olgunlaşmış bir yaklaşım olarak benimsenmemektedir. Yalnızca bu araçlara güvenmenin yeterli olmayacağı insan denetimi gerekliliğinden bahsedilmektedir (Whyte ve Walsh, 2024, s. 18). Bu bağlamda insan-makine iş birliği, değerlendiricilere destek mahiyetinde kullanılması amacıyla makul bir seçenek olarak ifade edilebilir. Yardımcı araçların uzman değerlendiricilerin ilgi alanlarına ve geçmiş değerlendirme tecrübelerine göre belge önerisinde bulunabileceği ifade edilmektedir (Narvala, 2024, s. 16). Belge önerileri doğrultusunda insan ve makine iş birliğinde gerçekleştirilen değerlendirme sürecinde, erişime açılan tüm belgelerin doğru belirlendiğine dair yüksek derecede bir güvene ulaşılması gerekir. Bu güvenin oluşması durumunda makinenin görevi karar vermek değil (henüz) öneride bulunmak olacaktır. Makine önerileri, insan değerlendiricinin gözden kaçırabileceği hassasiyetleri kaçırmamasına ve hem erişime açılacak hem de kapalı tutulacak belge içeriği hakkında daha hızlı karar vermesine yardımcı olabilir. Sürecin başarısı, doğru

[46] Hassasiyet değerlendirmesi sürecinde insan karar vericilerin kişisel deneyimlerinin kararlara etki edeceği "III.2.6. Kişisel Bakış ve Deneyim" başlığında incelenmektedir. Tespit ve karar verme süreçlerinde objektif bir süreç yönetimi için yardımcı araçların kullanılabileceği öngörülmektedir.

[47] ABD'de mahkumların potansiyel suç işleme riskinin değerlendirilmesi amacıyla oluşturulan algoritmaların ırk önyargısı içerdiğine dair örnek araştırma için bkz. Wadsworth, C., Vera, F. ve Piech, C. (2018). Achieving fairness through adversarial learning: an application to recidivism prediction. *arXiv preprint arXiv:1807.00199*. Bu konuda algoritmaların önyargı taşıdığı görüşünü Jaillant (2023, s. 576) desteklemektedir.

hassasiyet sınıflama verilerinin makine eğitiminde kullanılması ile artırılacaktır (Baron, Sayed ve Oard, 2022, s. 10). Ancak makine öğrenmesi araçları, insan eğitmenlerine dayanır ve bu durum, sonuçları etkileyebilecek bir değişkenlik ortaya çıkarır (Whyte ve Walsh, 2024, s. 6). Bunun dışında yardımcı araçlar, her dil yapısına göre değişen morfolojik, gramer ve semantik farklılıklar sebebiyle başka bir dil için çalışmaz. Bu amaç ile hazırlanan araçların dil yapısı ait olunan topluma göre tasarlanmalıdır. Örneğin Muammer Gaddafi isminin 112 farklı şekilde yazıldığından bazı karakterlerin yerleştirilmesinde zorluklar oluşmaktadır (The National Archives, 2016, s. 20). Dil farklılıkları yanlış pozitif (doğru olmayan onaylanan veriler) ve yanlış negatif (gerçek verileri negatif gösterme) sonuçlar doğurabilmektedir.

Dijital araçlar/gizliliği güçlendiren teknolojiler, hassasiyet değerlendirmesi sürecinde güçlü yönler ve fırsatlar sunarken tehdit ve zayıflıkları da barındırmaktadır. Büyük belge yığınlarının oluşturmuş olduğu hacim problemi artarak devam ederken var olan risklerin azaltılması, gizlilik ve mahremiyet kaygısını üstesinden gelmek için önemlidir. Bu sebeple yardımcı ve otonom araçlara/teknolojilere olan gereksinim açık olmak ile birlikte dönemin sunacağı yenilikler doğrultusunda değişkenlik gösterecektedir. Özellikle yapay zekâ, hassas ve hassas olmayan verilerin ayırt edilmesine yardımcı olarak dijital arşivlerin daha erişilebilir hale gelmesini sağlayabilir (Jaillant, 2022a, s. 545). Örneğin bir yapay zekâ alt yapısına sahip sohbet robotu (*chatbot*) olan ChatGPT'nin hassasiyet değerlendirmesi sürecinde; hassasiyeti tespit etmek, mevzuata dayandırmak, doğru bir tespiti onaylamak ve yanlış tespiti doğrulamak konuları üzerine araştırmalar yapılmaya başlanmıştır (Baron, Rolling ve Oard, 2023, s. 32). Bunun dışında metin dışı belgeler üzerinde görüntü işleme uygulamalarının kullanılması, hassas içeriklerin geniş ölçekli olarak redakte edilebileceği düşünülmektedir (Ranade, 2018, s 84). Bu konudaki araştırmalar, süreci iyileştirebilmek için gelişerek devam edecektir. Ancak kısa vadede, teknoloji destekli incelemenin/değerlendirmenin doğrulanmasına ihtiyaç duyulacaktır.

IV. BÖLÜM: ULUSAL ARŞİVLERDE HASSASİYET DEĞERLENDİRMESİ YAKLAŞIMLARI

Hassasiyet değerlendirmesi sürecine ilişkin adımlar, zorluklar ve teknolojik etkileşimler ifade edildikten sonra konunun uygulama kısmındaki faaliyetlerin açıklanması gerekmektedir. Ulusal arşivlerde, hassasiyet değerlendirmesi süreci başta olmak üzere pek çok arşiv uygulamasına yönelik farklı yaklaşımlar görülmektedir. Bu bölümde, odak konu gereği arşivcilik alanında önde gelen ve hassasiyet değerlendirmesi konusunda faaliyetleri bulunan ulusal arşivlerden örnekler sunulmaktadır. Ulusal/millî arşiv ve devlet arşivi kavramları genellikle birbirinin yerine kullanılan terimlerdir. Ancak bu kavramlar, ait oldukları toplumun ortak belge birikimini ve kültürel mirasını koruyarak gelecek kuşaklara aktaran, aynı zamanda diğer arşiv kurumlarına rehberlik eden önemli kuruluşları ifade etmektedir (Rukancı, Anameriç ve Başar, 2021, s. 23). Bu çerçevede, ulusal arşiv misyonuna sahip kurumların adlandırılmasında farklılıklar olsa da tümü aynı amaca hizmet etmektedir. Arşivlere yönelik sıralama, tespit edilen faaliyetlerin niceliği ve niteliği ölçüsünde yapılmıştır. Son olarak, Türkiye'de ulusal arşiv misyonunu taşıyan Devlet Arşivleri Başkanlığı'nın faaliyetleri, arşiv uygulamaları ve mevzuat düzenlemelerinde hassasiyet değerlendirme süreçlerine yönelik yaklaşımlar açıklanmaktadır.

IV.1. İngiltere (The National Archives/TNA)

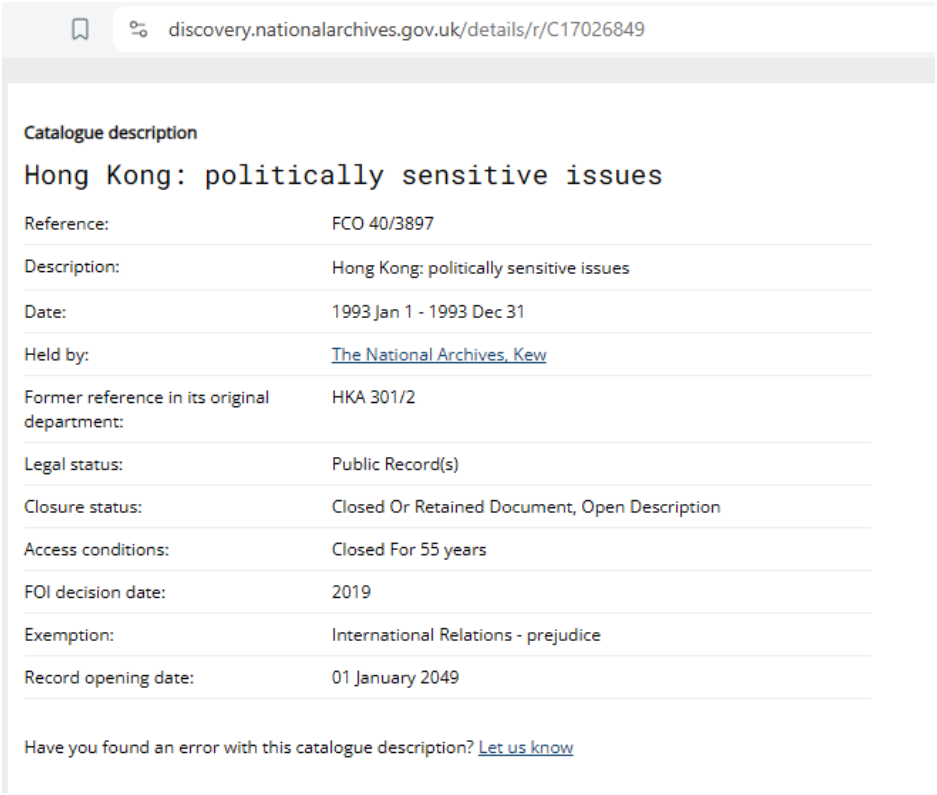
İngiltere Ulusal Arşivleri hassasiyet değerlendirmesi konusunda pek çok rehber/kılavuz ve rapor, doküman yayınlayan otorite bir kurumdur. Daha önce anılan bu dokümanlarda hassas bilgi içeren belgelere yönelik; imha (2012), genel amaç ve yöntem (2015), teknoloji destekli değerlendirme (2016), kapatma dönemleri/süreleri (2019b, 2021b), transfer (2021a), redaksiyon (2022) vb. kişisel bilgilerin genel ve özel amaçlı (2018,

2019a) işlenmesine yönelik bilgilendirmeler mevcuttur. Pek çok konuya ilişkin açıklamalar her dokümanda belirtilen konu bağlamında birbiri içerisine girmektedir.

TNA, elektronik belgelerin dijital transferini çeşitli aşamalara (değerlendirme, seçim, hassasiyet değerlendirmesi, transfere hazırlık, katalogta ve keşif araçlarında yer alma) ayırmıştır. Dijital transferin 3. adımı olarak hassasiyet değerlendirmesine yer vermiştir. Hassasiyet değerlendirmesi konusunda önemli bir birikime sahip olan TNA bu sürecin belge üretiminin başladığı ilk safhadan itibaren yürütülmesi gerektiğini vurgulamaktadır. Hassasiyet değerlendirmesini; "düşün ve bul", "kontrol et ve yap" olarak iki safhada ele almaktadır.

1. Düşün ve bul: Koleksiyondaki belgeler incelenerek temel hassasiyetlerin belirlenmesine yönelik üst veriler incelenmelidir. Bu kapsamda incelenen belgeler; mevzuata (İngiltere - Public Record Act) göre saklama, BEHK ve veri koruma düzenlemeleri kapsamında kapalı aktarım, Ulusal Arşiv'e açık aktarım ve kamu kurumları ile daha fazla istişare seçeneklerine göre değerlendirilmelidir.
2. Kontrol et ve yap: Bu safhada hassasiyet bakımından ele alınan belgelere yönelik kapatılma ve saklama kararlarının alınması için Ulusal Arşiv'e gönderim yapılır. Ulusal Arşiv'de görev alan danışma konseyi (*Advisory Council*) bu konuda bir karar vermektedir. Verilen karar doğrultusunda kapatılmış veya saklanan dosyalar üzerinde redaksiyon sürecine ilişkin talimatlar uygulanır. Bu iki aşamanın daha sağlıklı yürütülebilmesi için bağlamın ve geçmiş hassasiyetlerin öneminin farkında olup danışılması gereken birimler ile iletişim halinde olunması gerekmektedir. Ayrıca bazı ihtisas ve çalışma alanlarında kullanılan yazılımların hassasiyetlerin tespiti noktasında farkında olunması önemlidir (The National Archives, 2024).

TNA çevrimiçi kataloğunda[48] yer alan hassas bilgi içeren belgelerin tespitine yönelik bazı örnek sonuçlara ulaşılmıştır



Görsel 2. Hong Kong: Siyasî Hassas Meseleler (Belge ID: FCO 40/3897)

Üst veri bilgisinde uluslararası ilişkiler konusunda erişim muafiyeti olan bir kamu belgesi (Görsel 2) Hong Kong şehri ile ilgili siyasî hassasiyetler içermektedir. Hassas bilgi içeren bu belge 1993 yılına ait olup 2019 yılında karar bağlanarak 55 yıl süre ile kapalı olacağı bildirilmektedir. Erişim sınırlaması belgenin üretim tarihinden itibaren esas alınmış olup erişime açılma tarihi olarak 2049 yılı belirlenmiştir.

[48] İngiltere Ulusal Arşiv kataloğu için bkz. https://discovery.nationalarchives.gov.uk/

discovery.nationalarchives.gov.uk/details/r/C11155119

Catalogue description

MILLS, D: victim of unsolved murder at Wesley Tennis Staffordshire...

Reference:	MEPO 2/11523
Description:	MILLS, D: victim of unsolved murder at Wesley Tennis Club, West Bromwich, Staffordshire on 21 January 1961. Original statements 551- end
Date:	1961 Jan 01 - 1961 Dec 31
Held by:	The National Archives, Kew
Former reference in its original department:	201/61/19 PART 4
Legal status:	Public Record(s)
Closure status:	Closed Or Retained Document, Open Description
Access conditions:	Closed For 84 years
FOI decision date:	2013
Exemption 1:	Law enforcement
Exemption 2:	Health and Safety
Exemption 3:	Personal information where the applicant is a 3rd party
Record opening date:	01 January 2046

Görsel 3. Faili Meçhul Cinayet (Belge ID: MEPO 2/11523)

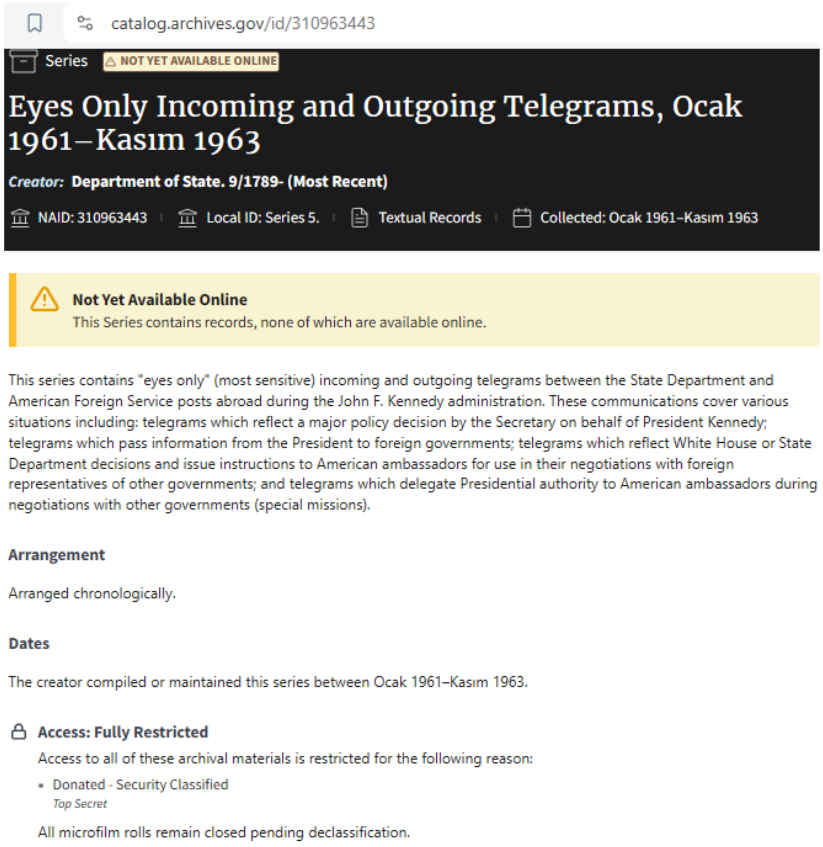
21 Ocak 1961 yılında West Bromwich kasabasında bulunan Wesley Tenis Kulübü'nde işlenen faili meçhul bir cinayeti konu alan belge (Görsel 3) 84 yıl süre ile erişimi kapatılmıştır. Bu belgeye ilişkin adlî geçmiş, sağlık ve güvenlik, başvuranın 3. taraf olduğu kişisel bilgiler olmak üzere 3 erişim muafiyeti belirtilmiştir.

IV.2. Amerika Birleşik Devletleri (National Archives and Records Administration/NARA)

Amerikan Ulusal Arşivleri'ne göre kurumlar elektronik belgelerini ulusal arşive transfer etmeden önce belge içeriğinde, yaşayan vatandaşlara ait sosyal güvenlik numarası, adlî geçmiş bilgisi ve mülkiyet bilgileri gibi kişisel tanımlayıcı hassas bilgiler belirlemelidir. NARA devraldığı belgelerin içerik incelemesini sağlayarak erişime kapatılacak belgeleri hassasiyet kontrolünden geçirmektedir. Bu sürecin daha verimli hale gelebilmesi için belge içeriğinde hangi hassas bilgi türünün yer aldığı ve hangi alanların neden

kısıtlandığına dair bilgilendirmelerin yapılması beklenmektedir (NARA Bulletin, 2014-4). Kurumlar transfer edilecek belgeleri iş amaçlı kullanımları sona erdiğinde ve hassasiyetleri azaldığında devretmelidir (NARA Bulletin, 2020-2). 2022-2026 Stratejik Planına göre, NARA 2026 yılına kadar bilgi edinme taleplerinin başlatılma süresini kısaltmayı hedeflemektedir. Bu sürecin genellikle 20 gün içerisinde yanıtlandığı, ancak karmaşık taleplerde 8 yıla kadar uzayabildiği ifade edilmektedir. Bu durumun ortaya çıkma sebebi, yüksek hassasiyete sahip Başkanlık ve federal belgelere yönelik erişim talebi ve buna bağlı olarak yapılan inceleme ve redakte sürecidir (NARA Strategic Plan 2022-2026, 2022).

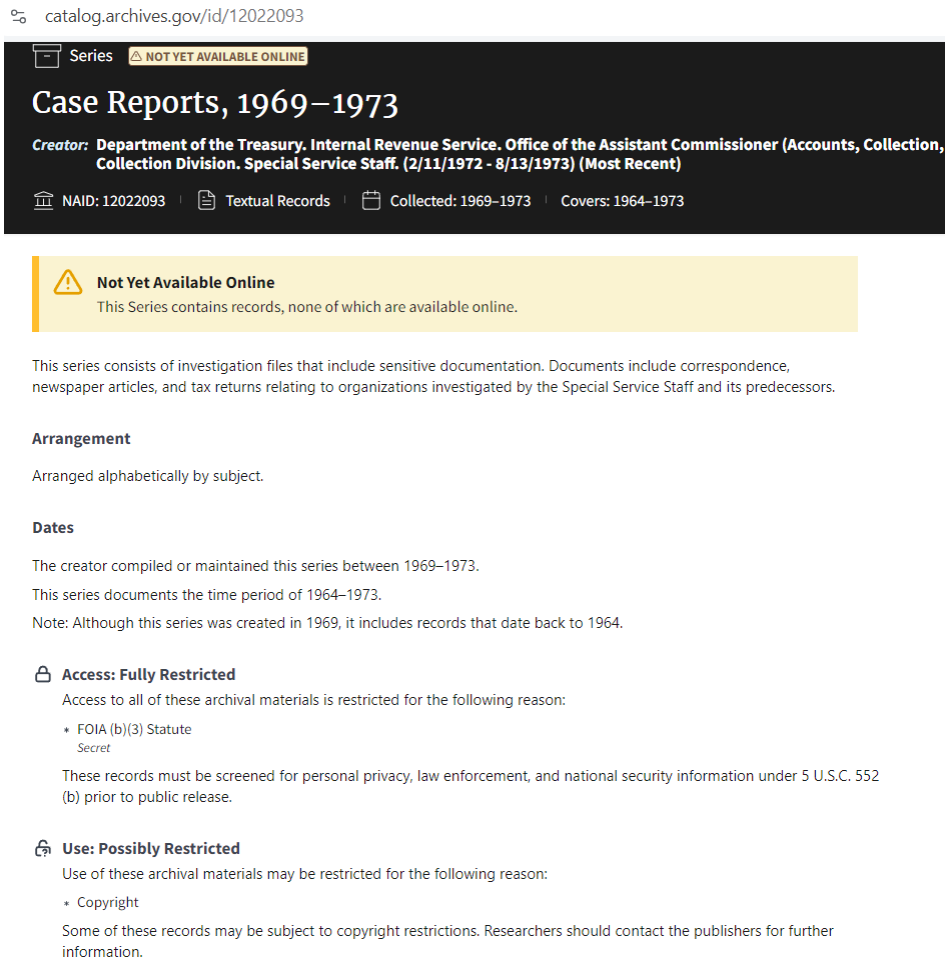
NARA çevrimiçi kataloğunda[49] yer alan hassas bilgi içeren belgelerin tespitine yönelik bazı örnek sonuçlara ulaşılmıştır.



Görsel 4. 1961-1963 ABD Dışişleri Gelen-Giden Telgraflar (Belge ID: 310963443)

[49] Amerikan Ulusal Arşiv kataloğu için bkz. https://catalog.archives.gov/

Eski Amerikan başkanı John F. Kennedy yönetimi sürecinde Dışişleri Bakanlığı ile yurtdışındaki Amerikan Dışişleri Servisleri arasındaki en hassas (*most sensitive*) yazışmaları konu alan telgraf belgelerine (Görsel 4) ulaşılmıştır. Uluslararası ilişkileri konu edinen bu belgeler, politika kararları, talimatlar ve yetki devirleri olmak üzere çeşitli hassasiyetler içerdiğinden erişime tamamen kapatılmıştır.



Görsel 5. 1969-1973 Vaka Raporları (Belge ID: 12022093)

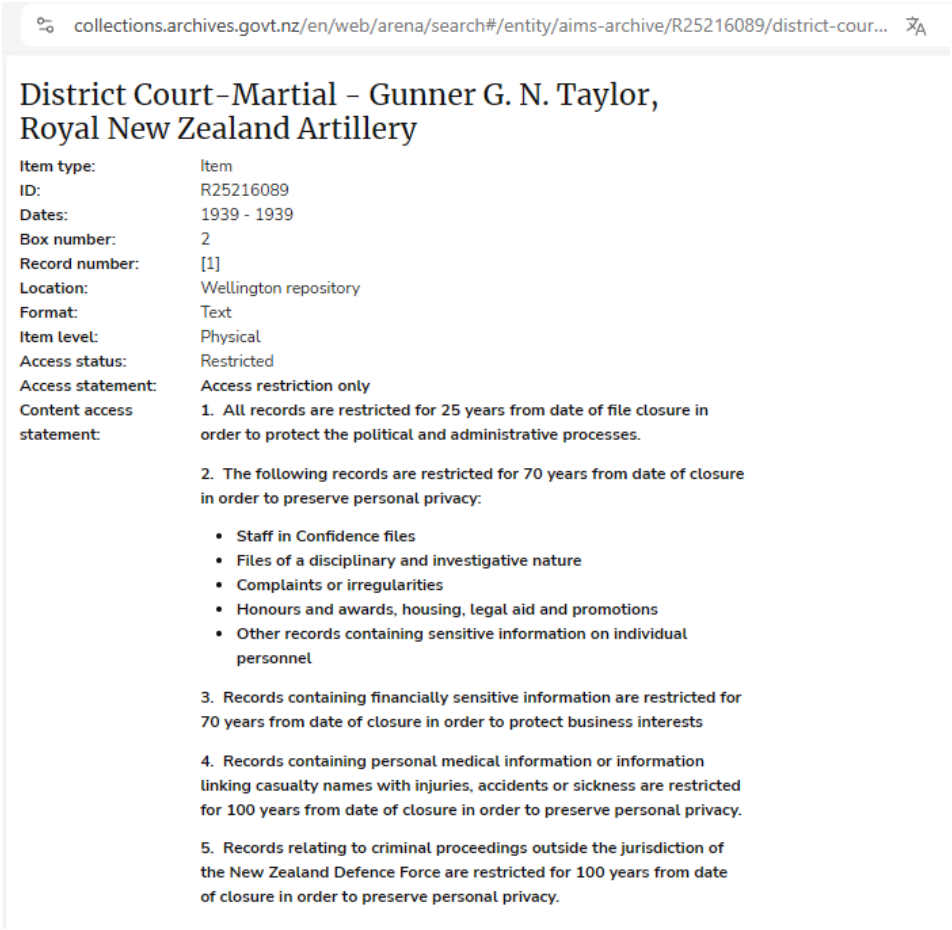
1969-1973 yılları arasındaki hassas belgeleri içeren bu seri (Görsel 5) özel hizmet personeli ve öncülerinin soruşturduğu kurumlar ile ilgili yazışma, gazete makalesi ve vergi beyannamesi dosyalarından oluşmaktadır. BEHK'nın ilgili maddesi (b.3) gereği bu belgelere erişim tamamen kısıtlanmıştır. Katalog kaydında bu belgelerin erişim açılmadan önce kişisel gizlilik, hukukî yaptırım ve ulusal güvenlik bilgileri bakımından

kontrol edilmesi gerektiği önerilmektedir. NARA, hassas bilgi içeren belgelere yönelik tam ve kısmî sınırlama seçeneklerini kullanmış olup herhangi bir süre sınırlamasını açık olarak belirtmemiştir.

IV.3. Yeni Zelanda (Archives New Zealand)

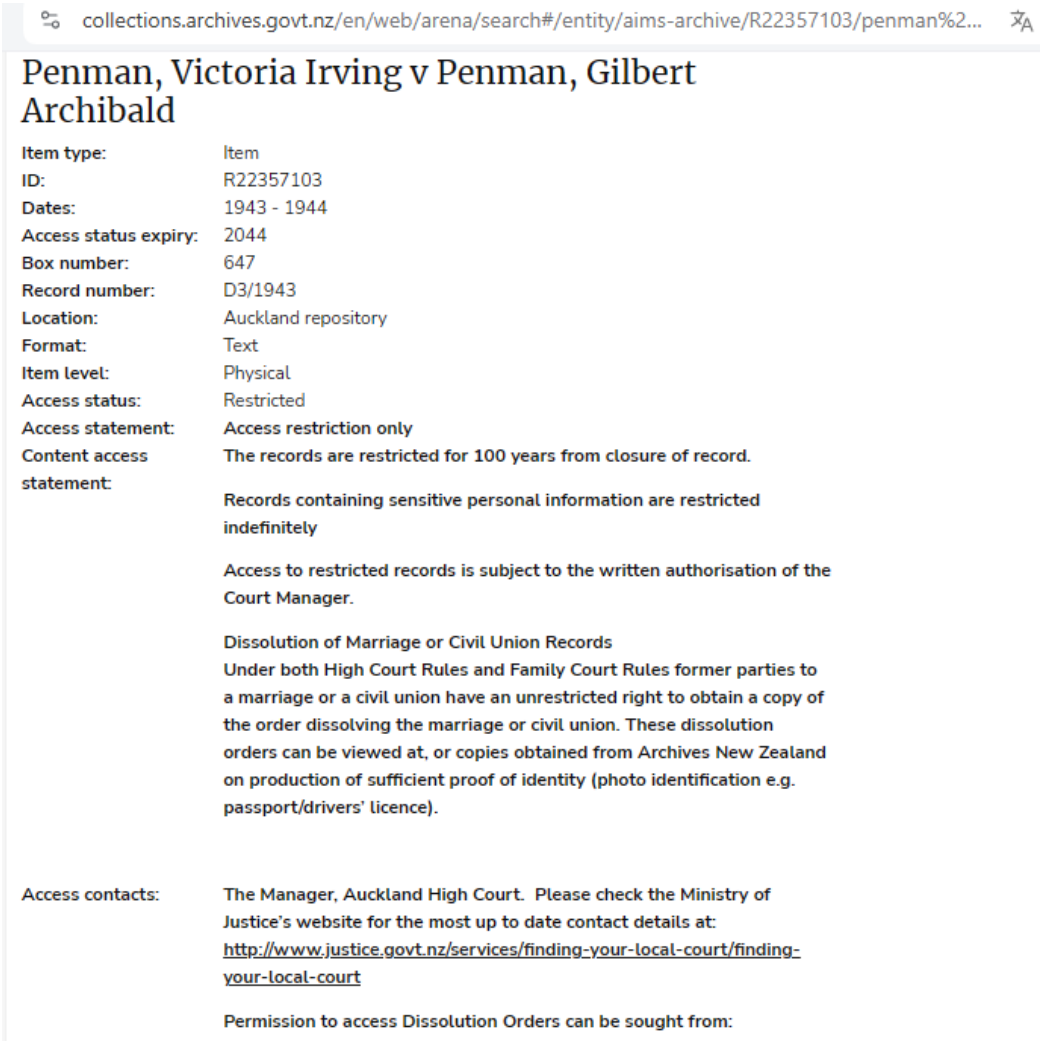
Yeni Zelanda'da kamu kurumları bir belgenin hassas bilgi içerip içermediğini belirleyerek bu tür belgelerin ulusal arşive devrinden sonraki süreçte erişim durumunu kontrol etme hakkına sahiptir. Ulusal arşivdeki personel, kurumdan izin almadan bu belgeleri erişime açamamaktadır. Belgeler üzerindeki erişim kısıtlaması genellikle kişisel bilgiler ve hassas bilgileri korumak amacıyla uygulanmaktadır. Bir vatandaş erişimi kısıtlanmış bir belgeye erişim talep ettiği durumlarda, erişim talebi genellikle ulusal arşiv yerine farklı bir devlet kurumu tarafından kontrol edilir ve dosyaları görüntülemek ve kopyalamak için yazılı izin talebinin bu kurumlara yapılması gerekir. Vatandaş yazılı izin aldıktan ve bu izin ulusal arşive ulaştıktan sonra, Yeni Zelanda Ulusal Arşiv personeli belgeye erişimle ilgili seçenekleri görüşebilir. Bu kapsamda erişime kapalı veya kısıtlanmış belgeleri ortaya koyabilmek amacıyla Yeni Zelanda Ulusal Arşiv çevrimiçi kataloğunda[50] yer alan hassas bilgi içeren belgelerin tespitine yönelik örnek sonuçlara ulaşılmıştır.

[50] Yeni Zelanda Ulusal Arşiv kataloğu için bkz. https://collections.archives.govt.nz/en/web/arena/search#/



Görsel 6. Kraliyet Topçusu G. N. Taylor (Belge ID: R25216089)

İkinci Dünya Savaşı sırasında Yeni Zelanda'da eğitim gören veya görev yapan askerî personele ilişkin mahkeme dosyaları arasında bulunan bir belgeye (Görsel 6) ulaşılmıştır. Yeni Zelanda Kraliyet Topçuluğu'nda görev alan Topçu G. N. Taylor adlı kişiye ait arşiv belgesi erişim sınırlamasına tabi tutulmuştur. Belgeye ilişkin erişim açıklaması bölümünde (2, 3 ve 10 maddeler), kişisel gizliliği korumak amacıyla hassas bilgi içeren personel belgeleri ile ticarî çıkarları korumak amacıyla finansal açıdan hassas olan belgeler 70 yıl süreyle sınırlandırıldığı belirtilmektedir. Ayrıca Yeni Zelanda Savunma Kuvvetleri dosyaları, askerî personele hizmet vermek ve kişisel gizliliği korumak amacıyla dosya kapanış tarihinden itibaren 100 yıl süre ile erişime kısıtlanmıştır.


collections.archives.govt.nz/en/web/arena/search#/entity/aims-archive/R22357103/penman%2...

Penman, Victoria Irving v Penman, Gilbert Archibald

Item type:	Item
ID:	R22357103
Dates:	1943 - 1944
Access status expiry:	2044
Box number:	647
Record number:	D3/1943
Location:	Auckland repository
Format:	Text
Item level:	Physical
Access status:	Restricted
Access statement:	Access restriction only
Content access statement:	The records are restricted for 100 years from closure of record. Records containing sensitive personal information are restricted indefinitely Access to restricted records is subject to the written authorisation of the Court Manager. Dissolution of Marriage or Civil Union Records Under both High Court Rules and Family Court Rules former parties to a marriage or a civil union have an unrestricted right to obtain a copy of the order dissolving the marriage or civil union. These dissolution orders can be viewed at, or copies obtained from Archives New Zealand on production of sufficient proof of identity (photo identification e.g. passport/drivers' licence).
Access contacts:	The Manager, Auckland High Court. Please check the Ministry of Justice's website for the most up to date contact details at: http://www.justice.govt.nz/services/finding-your-local-court/finding-your-local-court Permission to access Dissolution Orders can be sought from:

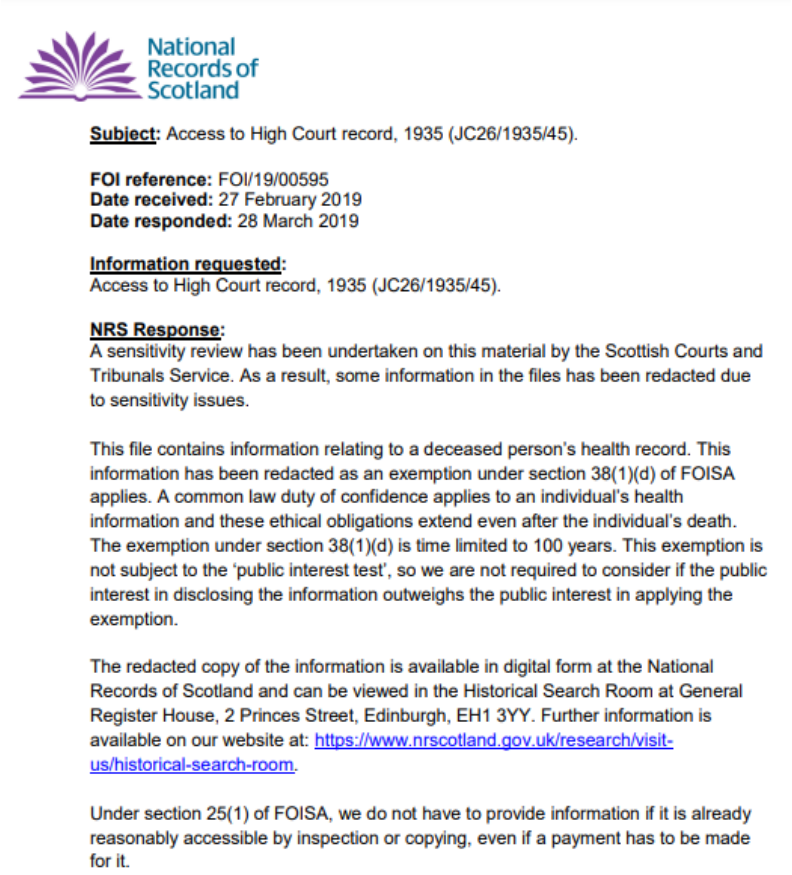
Görsel 7. Penman Ailesine İlişkin Belge (Belge ID: R22357103)

Boşanma davalarına ilişkin yasal belgeler arasında bulunan Penmann ailesine ilişkin arşiv belgesi (Görsel 7) erişim kısıtlamasına tabi tutulmuştur. Bu belgeye ilişkin erişim açıklaması bölümünde belgelerin kapatılma tarihinden itibaren 100 yıl süre ile kısıtlı olacağı ve hassas kişisel bilgi içeren belgelerin süresiz olarak kısıtlanacağına dair not düşülmüştür. Erişim sağlamak için mahkeme yöneticisinin izni şart koşulmuştur.

IV.4. İskoçya (National Records of Scotland)

İskoçya Ulusal Arşiv Başkanı, kamu kurumlarının işlemlerini yürütürken vatandaşlar hakkında hassas bilgiler içeren belgeler oluşturabileceğini ve bu durumda üretim aşamasında bilgi güvenliği kodlarının personele tavsiyede bulunması gerektiğini ifade

etmektedir. Ayrıca İskoçya'da kamu kurumları yaşan bireylere ait hassas kişisel bilgileri işlerken bir gizlilik bildiriminde bulunması gerekmektedir (National Records of Scotland, 2021, 37, 43).



National Records of Scotland

Subject: Access to High Court record, 1935 (JC26/1935/45).

FOI reference: FOI/19/00595
Date received: 27 February 2019
Date responded: 28 March 2019

Information requested:
Access to High Court record, 1935 (JC26/1935/45).

NRS Response:
A sensitivity review has been undertaken on this material by the Scottish Courts and Tribunals Service. As a result, some information in the files has been redacted due to sensitivity issues.

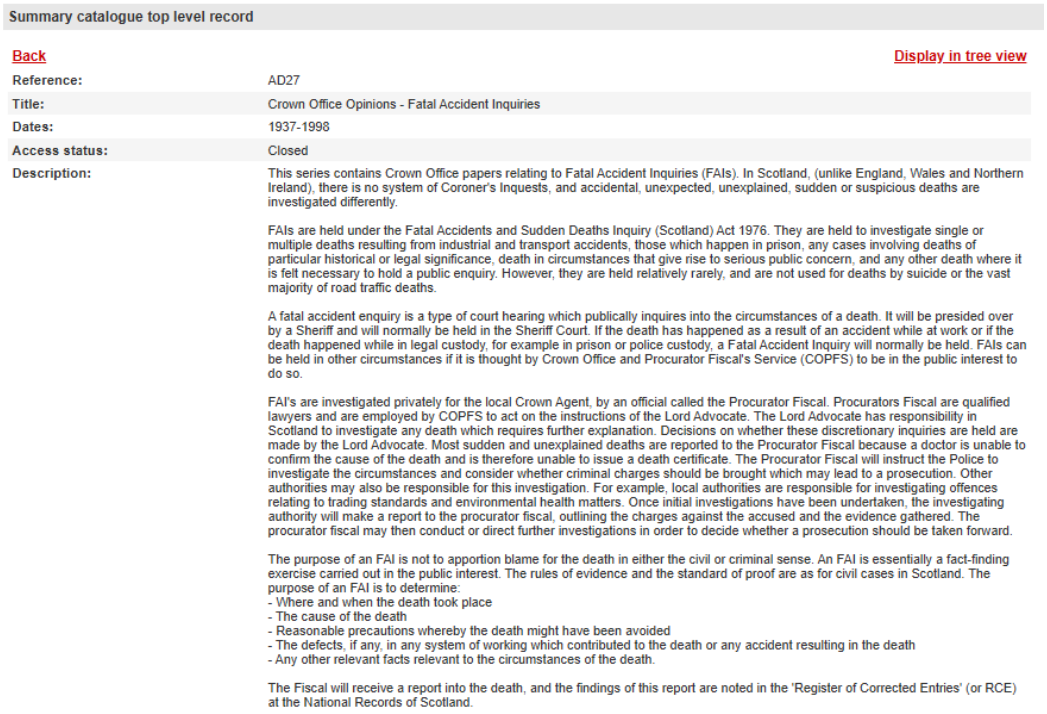
This file contains information relating to a deceased person's health record. This information has been redacted as an exemption under section 38(1)(d) of FOISA applies. A common law duty of confidence applies to an individual's health information and these ethical obligations extend even after the individual's death. The exemption under section 38(1)(d) is time limited to 100 years. This exemption is not subject to the 'public interest test', so we are not required to consider if the public interest in disclosing the information outweighs the public interest in applying the exemption.

The redacted copy of the information is available in digital form at the National Records of Scotland and can be viewed in the Historical Search Room at General Register House, 2 Princes Street, Edinburgh, EH1 3YY. Further information is available on our website at: https://www.nrscotland.gov.uk/research/visit-us/historical-search-room.

Under section 25(1) of FOISA, we do not have to provide information if it is already reasonably accessible by inspection or copying, even if a payment has to be made for it.

Görsel 8. Yüksek Mahkeme Belgelerine Erişim Talebi (Belge ID: JC26)

2019 yılında İskoçya Ulusal Arşivi'ne 1935 tarihli İskoçya Yüksek Mahkemesi belgelerine erişim talebi (Görsel 8) gelmiştir. Ulusal Arşiv, gelen talep üzerine İskoçya Mahkemeleri ve Mahkeme Servisi tarafından bir hassasiyet değerlendirmesi yapıldığı ve bazı bilgilerin hassas olduğu gerekçesiyle redakte edildiğini ifade etmiştir. Talep edilen dosya, vefat etmiş bir kişiye ait sağlık bilgilerini içerdiğinden İskoçya BEHK'nın ilgili maddesi (38/1.d) gereği redakte edilmiştir. Vatandaşlara ait sağlık bilgileri, İskoç genel hukukuna göre ölümünden sonra da devam etmekte olup anılan madde gereği kamu yararı testine gerek olmadığından 100 yıllık bir kısıtlamaya tabi tutulmaktadır (National Records of Scotland, 2019).



Summary catalogue top level record

Back — Display in tree view

Reference:	AD27
Title:	Crown Office Opinions - Fatal Accident Inquiries
Dates:	1937-1998
Access status:	Closed
Description:	This series contains Crown Office papers relating to Fatal Accident Inquiries (FAIs). In Scotland, (unlike England, Wales and Northern Ireland), there is no system of Coroner's Inquests, and accidental, unexpected, unexplained, sudden or suspicious deaths are investigated differently. FAIs are held under the Fatal Accidents and Sudden Deaths Inquiry (Scotland) Act 1976. They are held to investigate single or multiple deaths resulting from industrial and transport accidents, those which happen in prison, any cases involving deaths of particular historical or legal significance, death in circumstances that give rise to serious public concern, and any other death where it is felt necessary to hold a public enquiry. However, they are held relatively rarely, and are not used for deaths by suicide or the vast majority of road traffic deaths. A fatal accident enquiry is a type of court hearing which publically inquires into the circumstances of a death. It will be presided over by a Sheriff and will normally be held in the Sheriff Court. If the death has happened as a result of an accident while at work or if the death happened while in legal custody, for example in prison or police custody, a Fatal Accident Inquiry will normally be held. FAIs can be held in other circumstances if it is thought by Crown Office and Procurator Fiscal's Service (COPFS) to be in the public interest to do so. FAI's are investigated privately for the local Crown Agent, by an official called the Procurator Fiscal. Procurators Fiscal are qualified lawyers and are employed by COPFS to act on the instructions of the Lord Advocate. The Lord Advocate has responsibility in Scotland to investigate any death which requires further explanation. Decisions on whether these discretionary inquiries are held are made by the Lord Advocate. Most sudden and unexplained deaths are reported to the Procurator Fiscal because a doctor is unable to confirm the cause of the death and is therefore unable to issue a death certificate. The Procurator Fiscal will instruct the Police to investigate the circumstances and consider whether criminal charges should be brought which may lead to a prosecution. Other authorities may also be responsible for this investigation. For example, local authorities are responsible for investigating offences relating to trading standards and environmental health matters. Once initial investigations have been undertaken, the investigating authority will make a report to the procurator fiscal, outlining the charges against the accused and the evidence gathered. The procurator fiscal may then conduct or direct further investigations in order to decide whether a prosecution should be taken forward. The purpose of an FAI is not to apportion blame for the death in either the civil or criminal sense. An FAI is essentially a fact-finding exercise carried out in the public interest. The rules of evidence and the standard of proof are as for civil cases in Scotland. The purpose of an FAI is to determine: - Where and when the death took place - The cause of the death - Reasonable precautions whereby the death might have been avoided - The defects, if any, in any system of working which contributed to the death or any accident resulting in the death - Any other relevant facts relevant to the circumstances of the death. The Fiscal will receive a report into the death, and the findings of this report are noted in the 'Register of Corrected Entries' (or RCE) at the National Records of Scotland.

Görsel 9. Kraliyet Ofisi Görüşleri- Ölümlü Kaza Soruşturmaları (Belge ID: AD27)

İskoçya Ulusal Arşiv kataloğunda[51] 1937-1998 yılları arasında gerçekleşen beklenmedik, açıklanamayan veya şüpheli ölümlü kaza dosyalarına (Görsel 9) ulaşılmıştır. Bu dosyalar ölüm koşullarını (ölümün nerede, ne zaman, neden olduğu, kaçınılabilecek önlemler, kaza varsa sebep olan durumlar ve diğer gerekçeler) kamuya açıklayan bir mahkeme duruşması ile ilgilidir. Ancak bu dosyalara ilişkin seri, kamu yararını gerektirmeyen hassasiyetler içerdiğinden kapalı olarak tutulmaktadır.

IV.5. Estonya (National Archives of Estonia)

Estonya Ulusal Arşivleri'nin web sitesinden ulaşılan bilgilere göre diğer kamu arşivleri gibi muhafaza edilen belgelere erişimi olabildiğince mümkün kılmaktadır. Kamuya açık bilgilere erişim hakkını sadece iki durumda sınırlandırmıştır. Önemli kamu çıkarlarını savunmak ve kişileri özel hayatlarının ayrıntılarını kamuya açıklamaktan korumak. Bu

[51] İskoçya Ulusal Arşiv kataloğu için bkz. https://catalogue.nrscotland.gov.uk/nrsonlinecatalogue/browse.aspx

nedenle hassas ve özel kişisel veriler içeren kamu belgelerine erişim sınırlandırılmıştır. Bu kısıtlamaları kısmen Estonya Kişisel Verilerin Korunması Kanunu, kısmen de Aile Hukuku ve Noterler Kanunu gibi özel düzenlemelerle getirmiştir. Hassas ve özel kişisel bilgilere erişim iki koşula bağlamıştır:

1. Araştırmacının erişim ihtiyacının mevzuattan kaynaklanması. Örneğin bir soruşturmayı-denetimi yürüten görevliye erişim izni veren bir kararın olması ya da polis, mahkeme, savcılık veya diğer yetkililer tarafından yapılan bir erişim başvurunun olması gerekmektedir.
2. Araştırmacının önemli bir gerekçesinin olması.

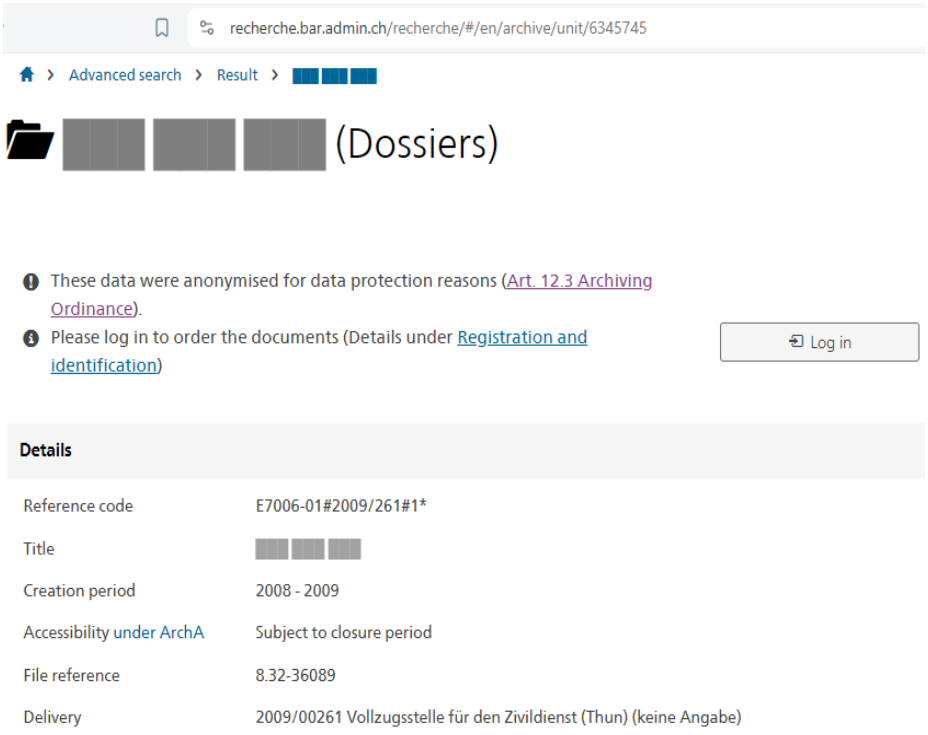
İskoçya Ulusal Arşivleri hassas olan ve mevzuata göre kısıtlanması gereken belgelerin olabileceğini ve bunları tespit etmenin çeşitli sebeplerden dolayı imkânsız olduğunu belirtmektedir. Bu noktada araştırmacıların eriştiği belgelerde vatandaşların aile ve özel hayatlarına müdahale hakkını kabul etmeli hassas ve özel kişisel verilerin kullanımı konusunda yürürlükteki mevzuata göre sorumluluk alması gerektiğini ifade etmektedir. Bu noktada sorumluluğu araştırmacıya yüklemiştir (National Archives of Estonia, 2024).

IV.6. İsviçre (Swiss Federal Archives)

İsviçre 2021-2025 Federal Arşiv Stratejisi'ne göre ulusal arşiv, hassas verileri transfer, koruma ve dijital kullanım süreci boyunca güvenli bir şekilde ele alarak gerektiğinde gizli elektronik belgeler için gelişmiş koruma sağlamayı hedeflemektedir. Ayrıca hassas kişisel veri içeren dijital araştırmaların mevzuata uygun olarak yürütülmesi sağlanarak korumalı meta verilere çevrimiçi erişim yeniden tasarlamak hedeflenmektedir (Federal Archives Strategy 2021-2025, 1.3, 4.5)

İsviçre Arşiv mevzuatında hassas bilgilere ilişkin bazı maddeler bulunmaktadır. Federal Arşiv Kanunu'na göre kişisel veri içeren arşiv belgelerin için uzatılmış saklama süreleri hassas kişisel veri söz konusu olduğunda (ilgili kişinin görüşüne başvurulmasına

izin verilmediği durumda) 50 yıllık bir saklama süresine tabidir (Federal Act on Archiving, 2023, 11/1). Federal Arşiv Yönetmeliği'nde ise hassas kişisel veri içeren araştırma araçları (*finding aids*) ancak saklama süresinin sona ermesinden sonra yayınlanabileceği ifade edilmektedir. (Ordinance to the Federal Act on Archiving, 2024, 12.3). İsviçre Ulusal Arşivi çevrimiçi kataloğunda[52] yapılan taramalar sonucu odak konuya örnek belgelere ulaşılmıştır.



Görsel 10. Anonimleştirilmiş Belge (Belge ID: 8.32-36089)

Tarama sonuçlarına göre (Görsel 10) hassas kişisel veri içeren arşiv belgelerinde araştırma araçları (belge başlığı/adı) ilgili madde (12.3) gereği maskelenmiş olarak katalogta yer almaktadır.

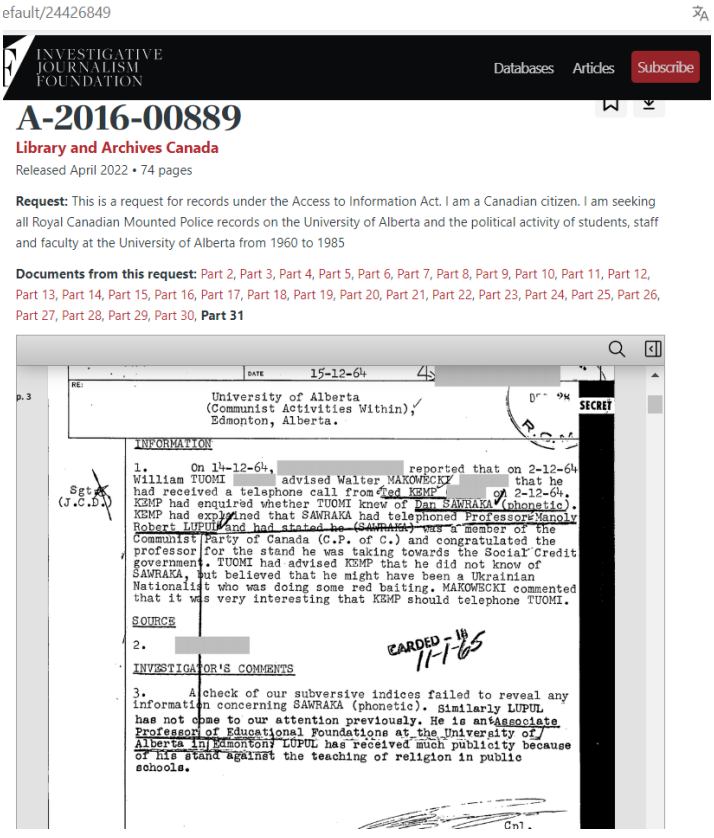
IV.7. Kanada (Library and Archives Canada)

Kanada Kütüphane ve Arşivler'ine göre ulusal güvenlik, diğer hükümetler, polis hizmetleri, program operasyonları, kişisel bilgiler, tıbbî ve yasal belgeler hakkında hassas

[52] İsviçre Ulusal Arşiv kataloğu için bkz. https://www.recherche.bar.admin.ch/

bilgiler içeren materyaller Bilgiye Erişim Kanunu (Canada Access to Information Act, 2024, 13, 26, 68, 69) ve Gizlilik Kanunu (Canada Privacy Act, 2023, 18, 28, 69, 70) uyarınca erişime sunulmamaktadır. Ayrıca 1919 yılından sonraki askerî hizmet dosyaları ve Kanada hükümet belgeleri (Kütüphane ve Arşiv kurumu dâhil) hassas bilgi içerdiği kabul edilmektedir. Bu dosyalara erişim sağlayabilmek için "Bilgi ve Mahremiyete Erişim (Access to Information and Privacy/ATIP)" talebinde bulunulması gerekmektedir (Library and Archives Canada, 2024).

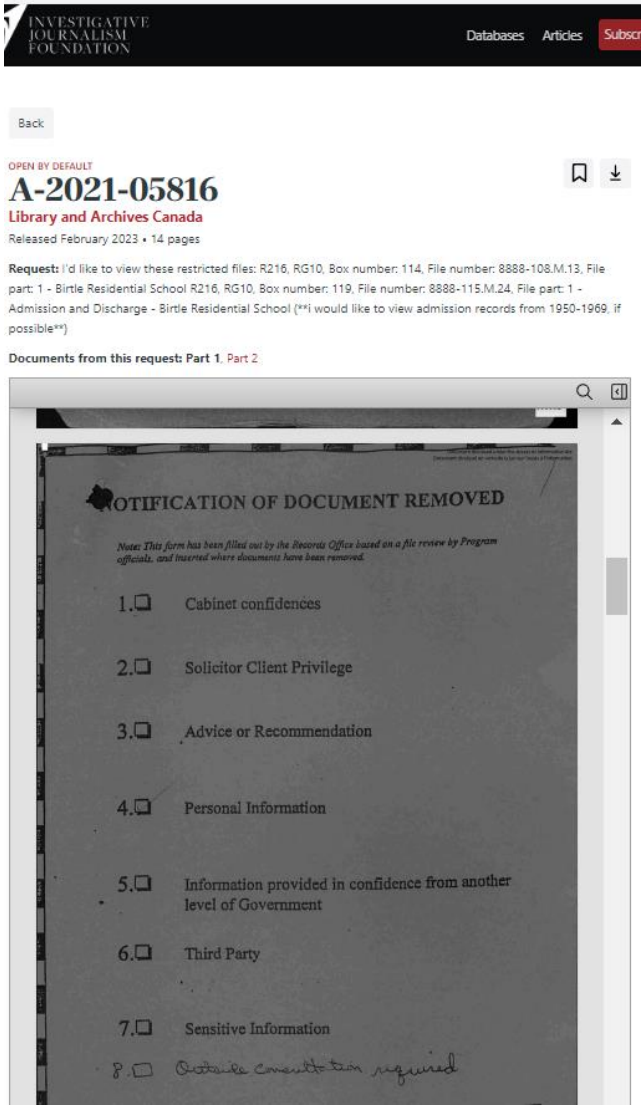
Yapılan ATIP başvuruları[53] üzerine belgeler hassasiyet açısında yeniden incelenmektedir. Örneğin 1960- 1985 yılları arasında Alberta Üniversite'sindeki öğrenci, personel ve fakültelerin siyasî faaliyetleri üzerine bir ATIP talebi üzerine ilgili belgelerdeki hassas bilgiler redakte edilmiş olarak (Görsel 11) kamuya açıklanmıştır.



Görsel 11. 1960-1985 Alberta Üniversitesi Siyasî Faaliyetler (Belge ID: A-2016-00889)

[53] 1960-1985 Alberta Üniversitesi Siyasî Faaliyetler konusunda yapılan bilgi edinme hakkı talebi ve ilgili benim tamamı için bkz. https://theijf.org/open-by-default/24426849

Bir diğer bilgi edinme talebi[54] (Görsel 12) örneği ise doğrudan erişim sınırlaması uygulanmakta olan belgeler üzerine yapılmıştır. Yapılan talep, Kanada Kütüphane ve Arşivler kurumu tarafından değerlendirilerek gerekli redaksiyonlar doğrultusunda belge kamu erişimine sunulmuştur. Bu belgenin 3 numaralı sayfasında belgenin kaldırılma bildiriminde yer alan seçenekler arasında "Hassas bilgi" gerekçe olarak bulunmaktadır. Nitekim belgenin kişisel bilgi içerdiği üzerine işaretlenmiş olup her iki kavramın sınırlama seçenekleri arasında olması bu konudaki ayrımın vurgulanması açısından önemli bir göstergedir.



Görsel 12. Erişim Sınırı Olan Belge Talebi (Belge ID: A-2021-05816)

[54] Erişim sınırı olan belge talebi konusunda yapılan bilgi edinme hakkı talebi ve ilgili belgenin tamamı için bkz. https://theijf.org/open-by-default/24417577

IV.8. Slovenya (Archives of the Republic of Slovenia)

Slovenya Cumhuriyet Arşivleri, hassas bilgi içeren belgelere yönelik "Belgelerin ve Arşivlerin Korunması ve Arşiv Kurumları Kanunu'nda" düzenlemede bulunmuştur. Anılan düzenlemeye göre gizlilik derecesi olan veya üçüncü taraflara açıklanması durumunda ulusal güvenliğe, kurumların güvenliğine ve yasal çıkarlarına zarar oluşturacak vergi sırlarını muhteva eden kamu arşivleri, 40 yıllık bir erişim sınırlamasına tabi tutulmaktadır. Bu bilgilerin dışında bireyin sağlık durumu, cinsel yaşamı, cinsel bütünlüğe karşı suç teşkil eden fillerin mağdurları, evlilik, aile ve çocuklar, suç teşkil eden fiil ve suçların failleri ile ilgili özel bilgileri içeren kamu arşivleri; eski tek parti rejimine muhalefet, dinî inanç ve etnik köken gibi sebeplerden dolayı hakkında işlem yapılan kişiler ile ilgili mevzuatta aksi olmadığı sürece belgenin üretiminde 75 yıl sonra, ilgili kişinin ölüm tarihi biliniyorsa 10 yıl sonra kamuya açık hale gelecektir (Protection of Documents and Archives…, 2014, 65/1, 65/2). Eski Devlet Güvenlik Servisi'ne ait arşiv kayıtlarına erişimle ilgili düzenlemeler, hem ulusal hem de uluslararası mevzuatlarda hassas olarak kabul edilen bilgilerin korunmasını gerektirirken, bu koruma Slovenya özelinde hassas bilgilerle eşdeğer kabul edilen verileri de kapsamaktadır. Ancak, Slovenya Cumhuriyeti Meclisi'nin 17 Mayıs 1990 tarihinde kurulmasından önce oluşturulan kamu arşiv belgeleri için bu sınırlamalar geçerli değildir. Bu tür belgelerde listelenen hassas kişisel verilerin yalnızca anonimleştirilmesi suretiyle bir kopyasının hazırlanması öngörülmektedir. İnsan hakları ihlalleriyle ilgili kararlar veren veya bu ihlalleri gerçekleştiren kişilere ait bilgilerin korunmasına izin verilmezken, mağdurlara ait hassas verilerin yalnızca anonimleştirilerek korunması gerektiği belirtilmiştir. Eski Devlet Güvenlik Servisi'nin insan hakları ihlalleriyle ilgili faaliyetlerinin ifşası kamu yararına olduğundan, arşiv kayıtlarının bu çerçevede açık tutulması gerektiği ifade edilmektedir. Arşiv Komisyonu ayrıca, 17 Mayıs 1990 öncesindeki tek parti rejimi dönemine ait siyasi inanç verilerinin, demokratik bir toplumdaki siyasi inanç bilgileriyle

eş tutulamayacağını vurgulamaktadır (Melik ve Košir, 2013, s. 135; Protection of Documents and Archives…,2014, 65/3, 65/4). Slovenya'da temel arşiv mevzuatında listelenilen hassasiyetler ve bunlara ilişkin uygulamaların dışında genellikle hassas olarak kabul edilen kişisel tıbbî belgelere yönelik müstakil bir düzenleme de mevcuttur. "Tıbbî Belgelerden Kişisel Veri İçeren Arşivleri Düzenleme Kanunu" kişisel veri içeren tıbbî belgelere kamu erişimini yasaklamaktadır. Bu tür belgelere hastanın kendisi, yazılı izin verdiği kişiler, sağlık hizmetlerine ilişkin kanun uyarınca ölümünden sonra erişim hakkına sahip kişiler ve bilimsel araştırma amaçları ile erişim sağlanabileceği/sağlayabileceği ifade edilmektedir (Act Regulating Archives…, 2016, 6/1, 6/2, 6/3, 6/4).

Ulusal arşivlerin uygulamalarının yanı sıra AP ve Konseyi'nin hassas belgelere ve arşivlere erişim hususunda düzenlemeleri vardır. "Avrupa Parlementosu, Konsey ve Komisyon Belgelerine Halkın Erişimi'ne İlişkin" 30 Mayıs 2001 tarih ve 1049/2001 sayılı AP ve Konsey Tüzüğü'nde oldukça hassas içeriğe sahip belgelere özel bir işlem yapılması gerektiği vurgulanmaktadır. Bu tür içeriğe sahip belgeler hakkında AP'nin bilgilendirmesine ve kurumlar arası mutabakatın sağlanması gerekmektedir (European Parliament and Council, 2001…, 9). Tüzüğün 9/1 fıkrasında tanımlandığı üzere kurumlardan veya bağlı kuruluşlardan, üye devletlerden, üçüncü ülkelerden ya da uluslararası kurumlardan ilgili kurum kurallarına bağlı olarak "ÇOK GİZLİ", "GİZLİ" veya "ÖZEL" olarak sınıflandırılan belgelerdeki bazı bilgiler hassastır. Bu bilgiler 4/1-a bendinde AB veya daha fazla üye devletin kamu güvenliği, savunma ve askerî konular, uluslararası ilişkiler, topluluğun veya üye devletin malî/parasal ekonomi politikaları olarak açıklanmıştır. Gizlilik veya ticarî çıkarlar ile ilgili istisnalar kapsamındaki belgeler ve hassas belgeler söz konusu olduğunda, bu belgelere 30 yıldan fazla koruma sağlanabilmektedir. Hassas belgelere erişim için yapılan başvurular bu tüzüğün 7. ve 8. maddelerinde belirtilen kurallar çerçevesinde, sadece bilgi sahibi olma hakkına sahip olan

kişiler tarafından ele alınır. Bu kişiler erişim sağlarken anılan hassasiyetleri ihlal etmemek ve atıfta bulunmak zorundadır. Hassas belgeler yalnızca belgeyi düzenleyicinin izin vermesi durumunda erişime açılır. Erişime izin vermeme kararı veren bir kurum anılan hassasiyetlere zarar vermeyecek şekilde gerekçeleri açıklar. Süreç, tüm üye devletlere yapılan başvurular için bu tüzükte yer alan ilkelere uygun tedbirlerin alınması şeklinde gerçekleştirilmelidir. Ayrıca kurumların hassas belgelere ilişkin kuralları kamuya açıklaması gerekmektedir. Komisyon ve konsey hassas belgeler üzerine kurumların mutabık olduğu düzenlemelere göre AP'yi bilgilendirir. Her kurum önceki yıla ait red kararları, gerekçeleri ve kaydedilmeyen hassas belge sayısı hakkında rapor hazırlayarak yayınlar (European Parliament and Council, 2001…, 9/1, 9/2, 9/3, 9/4, 9/5, 9/6, 9/7, 17/1).

Bir diğer düzenleme, Avrupa Konseyi Bakanlar Komitesi tarafından arşivlere erişim konusunda Avrupa politikasına yönelik üye devletlere tavsiye kararıdır. Bu kararda doğrudan hassas belgelere yönelik bir ifade kullanmak yerine korunan kişisel veri (*protected personal data*) kavramı yer almıştır. Kararın 1-c bendinde korunan kişisel veri, kimliği belirli veya belirlenebilir bir kişiye ilişkin kanun, düzenleyici metin veya mahkemeler tarafından söz konusu kişinin çıkarlarına zarar verme riski olmaksızın kamuya açıklanamayacak her türlü bilgi anlamına gelmektedir. Bu bilgilerin dışında kamu arşivlerine özel bir kısıtlama olmaksızın erişime izin verilmesi gerektiği bazı istisnai hallerin oluşması durumunda mevzuatın uygun olması vurgulanmaktadır. Bu istisnai haller tavsiye kararında ulusal savunma, dış politika ve kamu düzeni gibi korunmaya değer önemli kamu çıkarları ile özel hayatları ile ilgili bilgilerin yayınlanmasına karşı olan özel kişileri kapsamaktadır. Kararda hassas bilgilere işaret eden bu tanımlama ve önlemler, arşiv içeriğinde yer alan anılan nitelikteki belgelere erişim hususunda araştırma araçlarına da etki etmektedir. Araştırma araçları kapalı belgelerin varlığını ortaya koymasına rağmen mevzuat gereği korunan bilgiler (hassas bilgiler) içermediği sürece kullanıcıların erişim izni talep edebilmeleri amacıyla

erişilebilir olmalıdır (Council of European, 2000, 1.c, 1.e, 7/1.a 7/1.b, 8). Bu karar sonrası anılan türde bilgi içeren resmî belgelere ilişkin 2009 yılında Avrupa Konseyi "Resmî Belgelere Erişim Hakkında Avrupa Konseyi Sözleşmesi" emsal teşkil etmektedir. Sözleşmenin 3/1 fıkrasının alt bentleri gereği ulusal güvenlik, savunma ve uluslararası ilişkiler; kamu güvenliği; suç faaliyetlerinin önlenmesi, soruşturulması veya kovuşturulması; disiplin soruşturmaları; kamu yetkililerince yürütülen teftiş, denetim ve gözetim; mahremiyet ve diğer meşru özel çıkarlar; ticarî ve diğer ekonomik çıkarlar; devletin ekonomik, parasal ve döviz kuru politikaları; mahkeme işlemlerinde tarafların eşitliği ve adaletin etkin bir şekilde idaresi; çevre veya kamu yetkilileri bünyesinde ya da arasında bir meselenin incelenmesi hakkında müzakereler hakkında bilgi içeren belgelere yönelik olarak sözleşmeye taraftar olan ülkeler, erişim sınırlaması uygulayabilmektedir (Council of European, 2009). Bu denetimler, bilgilerin korunması ile kamu erişimi arasındaki dengeyi gözetmenin gerekliliğini ortaya koymaktadır.

IV.9. Türkiye'deki Yaklaşımlar

Türkiye'de T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı (DAB) kamu kurumlarında arşiv hizmetlerinin ve işlemlerin nasıl yürütüleceğine dair ulusal düzeyde denetleyici ve yönlendirici bir role sahiptir. Bu anlamda ulusal/millî arşiv vasfını taşımaktadır. Arşiv ve arşivciliğe dair uygulamalar diğer ülkelerde olduğu gibi mevzuat ve mevuzata dayalı olarak oluşturulan yönlendirici/eğitici dokümanlar çerçevesinde yürütülmektedir. Türkiye'de yürürlükte olan bir arşiv kanunu bulunmadığından gizlilik ve hassasiyete ilişkin yaklaşımlar diğer hususların da işlendiği kararname, yönetmelik, standart, ilgili bağlayıcı kanun ve rehber çerçevesinde (Tablo 5'te sunulan) uygulanmaktadır.

Tablo 5. Mevzuat, Standartlar ve Rehber

Mevzuat	Adı ve tarihi
Doğrudan Mevzuat	1. Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi, 2018 2. Devlet Arşiv Hizmetleri Hakkında Yönetmelik, 2019 3. Arşivlerden Yararlanma Usul ve Esasları Hakkında Yönetmelik, 2021 4. Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik**,** 2022 5. 6698 sayılı Kişisel Verilerin Korunması Kanunu, 2016 6. Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik, 2020 7. 4982 sayılı Bilgi Edinme Hakkı Kanunu, 2003 8. 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, 2024
İlgili Mevzuat	1. 25611 sayılı Türk Ceza Kanunu, 2004 2. 5902 sayılı Savunma Sanayii Güvenliği Kanunu, 2004 3. Dışişleri Bakanlığı Arşiv Hizmetleri Yönetmeliği, 2016 4. 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu, 2021 5. Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik, 2006 6. Güvenlik Soruşturması ve Arşiv Araştırması Yapılmasına Dair Yönetmelik, 2022 7. 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi
Standartlar	1. TS 13298 Elektronik Belge ve Arşiv Yönetim Sistemi Standardı, 2015 2. TSE K 523 Bilgi Varlıklarının Gizlilik Derecelerine Göre Sınıflandırılması Kriteri, 2016
Rehber	1. Bilgi ve İletişim Güvenliği Rehberi, 2020

DAB'ın kuruluşuna, görevlerine ve arşiv işlemlerine dair en üst bağlayıcılığı olan düzenleme 2018 yılında yayımlanan 11 sayılı Cumhurbaşkanlığı Kararnamesi'dir. Kararnameye göre "devlet ve kişilerin ulusal ve uluslararası haklarını belgelemek ve korumak" DAB'ın görevi olarak kabul edilmektedir (5/1.b). Arşiv belgelerinden

yararlanırken bu hakları korunmak, "Tasnif ve Araştırma Hizmetleri Dairesi Başkanlığı" görevleri arasında sayılmıştır. Anılan daire başkanlığının gizlilik kapsamında "kişi ve devlet haklarını belgelemek"; "kişisel bilgilerin gizliliği sağlanarak arşivlerin erişim ve kullanılabilirliğini arttırmak amacıyla arşivlerden yararlanma usul ve esaslarını belirlemek, araştırma taleplerini değerlendirmek ve gerektiğinde izin vermek"; "9/10/2003 tarihli ve 4982 sayılı BEHK çerçevesinde talepleri ve kamu kurum ve kuruluşlarının taleplerini usulüne uygun olarak karşılamak" görev ve sorumlulukları bulunmaktadır (10/1.b, f, ç). Bu sorumluluklara dair detaylı açıklama, kararnameye dayalı olarak oluşturulan 2019 yılında yayımlanan Devlet Arşiv Hizmetleri Hakkında Yönetmelik'te ele alınmıştır. Yönetmeliğin 7. maddesinde gizlilik ve gizliliğin kaldırılması hususu şu şekilde düzenlenmiştir:

(1) İşlem gördüğü dönemde gizlilik derecesi olan veya gizli kabul edilen ve halen bu özellikleri koruyan belgeler gizlilikleri kaldırılmadıkça bu özelliğini muhafaza eder.

(2) Gizlilik dereceli arşiv belgesi, Başkanlığa geçtikten sonra da gizli kalır. Bu çeşit arşiv belgesinin gizliliğinin kaldırılmasına, yükümlülerin görüşü alındıktan sonra Başkanlıkça karar verilir. Gizliliği kaldırılan arşiv belgeleri, "… tarih ve … sayılı karar ile gizliliği kaldırıldı" ibaresi düşülür.

(3) Başkanlığa devredilen arşiv belgelerinin gizliliğini kaldırma iş ve işlemlerine yönelik hususlar, Başkanlıkça çıkartılacak yönerge ile belirlenir.

Birinci fıkrada belirtilen gizlilik derecesi, Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmeliğin[55] 4/1 fıkrasında Çok Gizli, Gizli ve Hizmete Özel[56]

[55] Bu yönetmelik, 13.05.1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan mülga "Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkında Esaslar" ın yerine hazırlanmıştır. Bu esasların belirli konuları (savunma, güvenlik, istihbarat vs.) kapsaması, hizmete özel gizlilik sebebiyle erişimin kısıtlı olması ve "gizlilik derecelerinin değerlendirilmemesinden kaynaklı arşive devir sürecinde yönetilemeyecek şekilde belge yoğunluğunun oluşması" vb. pek çok sebepten dolayı yeni yönetmeliğe gereksinim duyulmuştur (Gizlilik Dereceli Belgelerde…, 2022, s. 2, 3).

[56] Millî gizlilik dereceleri 4. Maddenin 1. Fıkrasının alt bentlerinde (a, b, c) bu dereceler şu şekilde açıklanmıştır: "Çok Gizli: Açıklanması veya yetkisiz kişilerce öğrenilmesi hâlinde Devletin dış ilişkilerine,

olarak üç adet millî gizlilik derecesini (Şekil 3) ifade etmektedir. Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmeliğin 25/1,2 fıkralarına göre kurumsal bilgi/belge sistemlerinde gizlilik derecesi olan belgeler arasında sadece "Hizmete Özel" nitelikte gizlilik içeren belgeler elektronik ortamda üretilecektir[57]. Bunun dışında Çok Gizli ve Gizli dereceli olan belgeler fiziksel (kâğıt) ortamda üretilmesi gerektiği ifade edilmektedir[58].

Şekil 3. Millî Gizlilik Dereceleri (Gizlilik Dereceli Belgelerde…, 2022, s. 5)

Gizlilik derecelerinin kullanımı hassas ve korunması gereken belgeler için uygun önlemlerinin alınmasına yardımcı olacaktır (Gizlilik Dereceli Belgelerde…, 2022, s. 7). Gizlilik dereceleri arasında hassas bilgi içeren belgelere doğrudan değinen ve

millî savunmasına, millî güvenliğine ve müttefiklerle olan faaliyetlerine önemli derecede zarar verebilecek belgeler için kullanılır. Gizli: İzinsiz açıklanması veya yetkisiz kişilerce öğrenilmesi hâlinde Devletin menfaatlerine, güvenlik, istihbarat ve teknoloji faaliyetlerine zarar verebilecek belgeler için kullanılır. Hizmete Özel: İzinsiz açıklanması veya yetkisiz kişilerce öğrenilmesi hâlinde herhangi bir idari faaliyete, gerçek veya tüzel kişiye, idari soruşturmaya, adlî soruşturmaya ve kovuşturmaya zarar verebilecek belgeler için kullanılır."

[57] Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmeliğin 9/7 fıkrasında sayılan kurumlar gizlilik dereceli belgelerini gizlilik dereceli belgelere ilişkin işlemlerini gerekli güvenlik tedbirlerini almak şartıyla kapalı ağa bağlı cihazlarda gerçekleştirebilir. Anılan fıkrada sayılan kurumların dışında EBYS'lerde Hizmete Özel belge üretilebilmektedir.

[58] Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmeliğin 31/3 fıkrasında "Hizmete Özel" haricindeki gizlilik dereceli belgeler "23/10/2010 tarihli ve 27738 sayılı Resmî Gazete'de yayımlanan "Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik"in 2 nci maddesinde yetkili kılınan idareler, gizlilik dereceli belgeleri gerekli güvenlik tedbirlerini almak şartıyla güvenli elektronik imza ile imzalayarak elektronik ortamda da gönderebilir."

kullanılması/seçilmesi gereken derece, "Hizmete Özel" olarak belirtilmektedir. Anılan gizlilik yönetmeliğinin 5/3-a bendinde bu durum "yetkisiz kişilerce öğrenildiği takdirde idarece yürütülen faaliyeti engelleyici veya faaliyete zarar verici ya da eşitlik ilkesine aykırı olacak şekilde gerçek veya tüzel kişiye çıkar sağlayıcı sonuçlara sebebiyet verecek hassas bilgi içeren belgeler" olarak işaret edilmiştir. Belgelerin hassas olma koşulu kuruma zarar, gerçek veya tüzel kişilere haksız fayda olmak üzere sınırlı çerçevede ifade edilmektedir. Hizmete Özel gizlilik derecesi, elektronik ortamdaki belgelerde kullanılabileceğinden kurumlar EBYS'de hassas bilgi içeren belgelerini bu derece ile üretebilmektedir. Bununla birlikte Gizli ve Çok Gizli olarak üretilen belgeler, içerik bağlamında hassas nitelikteki [BEHK, 4. bölüm ve Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik 5. maddede[59] listelenen] bilgileri taşımaktadır. Ancak bu belgelerin kâğıt ortamda üretilmesinden ve anılan gizlilik yönetmeliğinin 9/7 fıkrasında listelenen idareler hariç olmasından dolayı EBYS'lerde üst veri alanında bu dereceler kullanılamamaktadır. Kâğıt ortamda üretilen benzer muhtevada belgeler için üst gizlilik dereceleri kullanılmaktadır. Bu bakımdan gizlilik derecesi verilen belgelerin farklı güvenlik düzeylerinin bulunması hibrit (hem elektronik hem fiziki ortam) bir yönetim anlayışını da beraberinde getirmektedir (Kaymak ve Külcü, 2024, s. 274). Anılan yönetmeliğe göre çok gizli gizlilik dereceli belgeler ile gizli ve hizmete özel gizlilik dereceli belgelerin değerlendirme komisyonları da ayrıdır. Her iki değerlendirme komisyonu, belgelerin sahibi birimin yöneticisinin veya yetki verdiği yöneticinin başkanlık edeceği şekilde toplam üç kişiden oluşmaktadır (Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik, 2022, 7). Bu değerlendirme komisyonları bakanlık ve bağlı kamu kurumlarındaki gizlilik derecesi olarak belgeleri

[59] Anılan Yönetmeliğin 5. maddesinde, çok gizli, gizli ve hizmete özel gizlilik derecesine giren bilgiler hakkında açıklamalar yapılmıştır. Bu bilgiler, hem BEHK hem de KVKK kapsamında hassas bilgilerle veya bu kapsamdaki muafiyetlerle ilişkilendirilmektedir. Örneğin: Örneğin 2/f "Açıklanması veya yetkisiz kişilerce öğrenilmesi hâlinde uluslararası ilişkilere zarar verebilecek belgeler" ile 3/b "Yetkisiz kişilerce öğrenildiği takdirde herhangi bir gerçek veya tüzel kişiye ticari, maddi veya manevi olarak zarar verici sonuçlara yol açabilecek belgeler" bentleri her iki düzenleme kapsamında değerlendirilmektedir.

için oluşturulmaktadır. Değerlendirme komisyonları görevlerini ulusal arşive devir öncesi yapmaktadır. Devlet Arşivleri Başkanlığı'nda ise "Arşiv Belgesi Gizlilik Değerlendirme Komisyonu" tarafından bu işlemler yürütülmektedir. Yönetmeliğin üçüncü fıkrasında belirtilen Arşiv Belgesi Gizlilik Değerlendirme Yönergesi DAB'ın devraldığı belgelere yönelik esas aldığı hukukî düzenlemedir. Bu yönergeye göre, DAB bünyesinde kurulan Arşiv Belgesi Gizlilik Değerlendirme Komisyonu; belgelerin gizlilik derecesini belirlemek, gizlilik özelliği taşıyan belgelerin gizliliğinin kaldırılıp kaldırılmayacağına ya da devam ettirilmesine karar vermekle yetkilidir. Komisyon gizliliğin devam ettirilmesi veya kaldırılması [Gizliliği Kaldırılan Arşiv Belgeleri Listesi hazırlayarak] konusunda karar almaktadır. Yönergede gizlilik derecesinin düşürülmesi veya yükseltilmesi ile erişime kapalı belgelerin sınırlı olarak sunulması konusu yer almamaktadır. Ayrıca elektronik ortamda üretilen gizlilik derecelerine sahip belgelerin üst verilerine değişikliklerin nasıl işleneceğine değinilmemektedir. Özellikle gizlilik derecelerinin değişkenlik gösterebileceği gizlilik konulu yönetmelikte belirtilmektedir. Gizlilik derecesi olmayan ya da belirli bir gizlilik derecesine sahip belgeler, ilişkili belgelerle bir araya getirildiğinde gizlilik kazanabilir veya daha yüksek bir gizlilik seviyesine ulaşabilir. Bu durum yönetmeliğin (2022) gizlilik derecelerinin açıklandığı bölümün 5/1-f, 5/2-ğ ve 5/3-e bentlerinde şu şekilde ifade edilmektedir:

f) Gizli veya Hizmete Özel gizlilik dereceleri ile derecelendirilen fakat bir araya getirildiklerinde kapsadıkları bilgiler bakımından daha yüksek biçimde derecelendirmeyi gerektiren belgeler

ğ) Hizmete Özel gizlilik derecesiyle derecelendirilen fakat başka belgelerle bir araya getirildiklerinde kapsadıkları bilgiler bakımından daha yüksek biçimde derecelendirmeyi gerektiren belgeler.

e) Gizlilik derecesi olmayan fakat başka belgelerle bir araya getirildiğinde Hizmete Özel olarak derecelendirmeyi gerektiren belgeler.

Anılan bentler, gizliliğin ilişki kurma yönüne dikkat çekmektedir. Bu yaklaşım, daha önce tartışılan mozaik hassasiyeti kavramıyla benzerlik göstermekte ve hassasiyetin bilgi parçacıklarıyla olan bağlantısına odaklanmaktadır.

Devlet Arşiv Hizmetleri Hakkında Yönetmelik'te gizlilik ile ilgili bir diğer husus dosyaların hazırlanmasıdır. Yönetmeliğin 13/2 fıkrasına göre "içerisinde tamamen veya kısmen gizlilik derecesi taşıyan dosya/klasör etiketi üzerine en yüksek gizlilik dereceli belgenin ibaresi yazılır. Gizlilik dereceli dosya/klasörler, arşivlerde tasnif ve yerleştirme sırasında normal belgeler gibi işleme tabi tutulur". Gizlilik derecesi olan belge sayısının veya içeriğin bu noktada etkisi olmamaktadır. Bu nitelikte bir adet belgenin yer alması dosya etiketini belirlemek için yeterli olup dosya düzeninin değiştirilmesine etki etmemektedir. Bu bağlamda dosyada gizli/hassas nitelikte olan belgenin erişim hususu düzeni/tasnifi dışında değerlendirilmektedir. Gizlilik dereceli, hassas veya kişisel bilgi içeren belgelerin erişim durumuna yönelik 2019 yılından yayımlanan Devlet Arşiv Hizmetleri Hakkında Yönetmelik'te açıklanan bazı hususlar 2021 yılında yayımlanan "Arşivlerden Yararlanma Usul ve Esasları Hakkında Yönetmelik" kapsamında genişletilmiştir. Yönetmeliğin 9/1-c bendine göre "gizlilik derecesi/özelliği olan belgeler" araştırma hizmetine sunulmamaktadır. 9/2 fıkrasına göre "24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu gereğince özel nitelikli belgeler de araştırma için verilmez. Ancak bilimsel araştırma için gerekli olan belgeler, 6698 sayılı Kanun gereğince kişisel veriler korunarak verilebilir". Anılan fıkra "özel nitelikli belge" tanımının KVKK kapsamında (6/1 fıkrasında listelenen) dikkate alınacağına atıfta bulunmuştur. Bu tür hassas belgelerin korunarak erişime sunulması hususunda KVKK'nın 28/1-b bendinde "kişisel verilerin resmî istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi" şartı koşulmaktadır. Belge üzerinde anonimleştirme yapılarak kısıtlı erişim mümkün kılınmaktadır. Nitekim

bu durum 2003 yılında yayımlanan BEHK'nın 9. maddesinde şu şekilde ifade edilmektedir:

> İstenen bilgi veya belgelerde, gizlilik dereceli veya açıklanması yasaklanan bilgiler ile açıklanabilir nitelikte olanlar birlikte bulunuyor ve bunlar birbirlerinden ayrılabiliyorsa, söz konusu bilgi veya belge, gizlilik dereceli veya açıklanması yasaklanan bilgiler çıkarıldıktan sonra başvuranın bilgisine sunulur. Ayırma gerekçesi başvurana yazılı olarak bildirilir.

Bununla birlikte Arşivlerden Yararlanma Usul ve Esasları Hakkında Yönetmeliğin 9/2 fıkrası arşiv mevzuatında hassas/özel nitelikli belgeleri doğrudan [Gizlilik yönetmeliğinin 5/3-a bendinde de konu olan] işaret etmesi bakımından dikkate değerdir. Daha önce anılan Devlet Arşiv Hizmetleri Hakkında Yönetmelik'te belirtilen hususlar (Madde 7), Arşivlerde Yararlanma Usul ve Esasları Hakkında Yönetmeliğin 10. maddesinde genişletilerek arşiv belgelerinin gizliliğinin değerlendirilmesine dair şu bilgiler sunulmuştur:

(1) Gizlilik derecesi/özelliği bulunan ve halen bu özelliğini koruyan arşiv belgeleri Başkanlığa devredildikten sonra da bu özelliği korur.

(2) Gizlilik derecesi/özelliği olan arşiv belgelerinden üzerinde tanımlanmış olan saklanma, kullanma, paylaşma ve yayımlama kısıtlamalarının, geçen zaman ve değişen koşullar sonucu tekrar gizliliğinin değerlendirilmesi ve gizliliğinin kaldırılması, Başkanlık tarafından kurulacak Arşiv Belgesi Gizlilik Değerlendirme Komisyonu tarafından yürütülür.

(3) Komisyon, Başkanın görevlendireceği başkan ve üyeler ile kurumunun belgeleriyle ilgili görüş ve değerlendirmede bulunabilecek üyelerin katılımı ile en az beş kişiden oluşur.

(4) Komisyon üye çoğunluğu ile toplanır ve oy çokluğu ile karar alır. Oyların eşit olması halinde komisyon başkanının oyu kararı belirler.

(5) Gizlilik derecesi/özelliği değerlendirilen ve bu özelliği kaldırılanlar, Başkanlıkça düzenlenen Gizliliği Kaldırılan Arşiv Belgeleri Listesi'ne eklenir. Liste, komisyon başkanı ve üyeleri tarafından imzalanır.

(6) Arşiv Belgesi Gizlilik Değerlendirme Komisyonunun aldığı kararlar Başkanın onayını müteakip kesinlik kazanır. Gizliliği kaldırılan arşiv belgelerine, "… tarih ve … sayılı olur ile gizliliği kaldırıldı" ibaresi düşülür.

(7) Arşiv Belgesi Gizlilik Değerlendirme Komisyonu Kararları, Başkanın oluru ve bunlarla ilgili yazışmalar imha edilmez ve sürekli olarak saklanır.

(8) Gizlilik derecesi kaldırılan arşiv belgeleri, diğer belgeler ile aynı usulde araştırma hizmetine sunulur.

(9) İlga edilen ve faaliyeti sonlandırılarak belgeleri Başkanlığa devredilmiş kurum ve kuruluşlara ait belgelerin değerlendirilmesi ve gizliliğinin kaldırılması işlemlerine yönelik süreç Başkanlıkça yerine getirilir.

Arşiv belgelerinin gizliliğine ilişkin daha önce anılan[60] değerlendirme zorlukları bu maddenin 2. fıkrasında açıkça belirtilmektedir. Değerlendirme sürecinde bir komisyonunun bulunması (Fıkra 2), gereken durumlarda devir yapan kurum ile istişare[61] yapılması (Fıkra 3) pek çok ulusal arşivin uygulamada yer verdiği bir yöntemdir. 8. Fıkrada ifade edilen belgelerin gizliliğinin kaldırılması durumunda araştırmaya sunulması, BEHK'nın 28. maddesinde "gizliliği kaldırılmış olan bilgi veya belgeler, bu kanunda belirtilen diğer istisnalar[62] kapsamına girmiyor ise, bilgi edinme başvurularına

[60] 2. fıkrada belirtilen geçen zaman ve değişen koşullara ilişikin değerlendirme gereksinimi III.2.2 Zaman ve III.2.5. Sosyal ve Kültürel Farklılıklar başlıklarda zorluk olarak ele alınmıştır.

[61] DAB kurum ve kuruluşlarda devredilen belgeler hakkında bilgi ve tecrübe sahibi kişilerin görüşüne başvurmaktadır.

[62] Bilgi Edinme Hakkı Kanunu'nun dördünce bölümünde (Madde 15-28 arası) bazı sınırlamalar belirtilmektedir. Bu sınırlamalar: Yargı denetimi dışında kalan işlemler, Devlet sırrına ilişkin bilgi veya belgeler, Ülkenin ekonomik çıkarlarına ilişkin bilgi veya belgeler, İstihbarata ilişkin bilgi veya belgeler, İdarî soruşturmaya ilişkin bilgi veya belgeler, Adlî soruşturma ve kovuşturmaya ilişkin bilgi veya belgeler, Özel hayatın gizliliği, Haberleşmenin gizliliği, Ticarî sır, Fikir ve sanat eserleri, Kurum içi düzenlemeler, Kurum içi görüş, bilgi notu ve tavsiyeler, Tavsiye ve mütalaa talepleri olarak ifade edilmiştir. Kanunda sayılan unsurlar genellikle Çok Gizli, Gizli ve Hizmete Özel gizlilik dereceleri kapsamında tarif edilmektedir. Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmeliğin 5. Maddesini fıkra ve bentlerinde benzer sayım yapılmaktadır.

açık hâle gelir" olarak garanti altına alınmıştır. İstisna olarak da ifade edilen sınırlılıklar çoğunlukla kişilere bağlı olmayan hassas bilgileri işaret etmektedir.

Gizlilik komisyonlarında gizliliğin kaldırılması veya düşürülmesine dair incelemelerin güncel olarak yürütülmemesi arşive devir hususunda problem oluşturmamaktadır. Ancak bilgi edinme süreci başta olmak üzere birçok işlem engellenebilmektedir. Bu durum erişime açık olması gereken belgeleri veya kısıtlama sürelerini olumsuz yönde etkilemektedir. Ayrıca gizlilik dereceli belge miktarının artması, yeterli güvenlik tedbirleri ile iş gücü ve maliyet oranını artırarak arşivlerin işlevselliğine zarar verecektir (Gizlilik Dereceli Belgelerde…, 2022, s. 49). Gizlilik söz konusu olduğunda, Türkiye'de tasarı düzeyinde kalsa da bir düzenlemenin varlığını belirtmek gerekir. 2011 yılında TBMM'ye kanun telifi olarak sunulan "Devlet Sırrı Kanun Tasarısı", Türk Ceza Kanunu ve Ceza Muhakemesi Kanunu'nda[63] yer alan devlet sırrı kavramnıa dayandırılarak oluşturulmuş ve hukukî boşluğu doldurmak amacıyla hazırlanmıştır. Tasarıda devlet sırrı (Devlet Sırrı Kanun Tasarısı, 2008, Madde 3), "açıklanması veya öğrenilmesi, Devletin dış ilişkilerine, milli savunmasına ve milli güvenliğine zarar verebilecek; anayasal düzeni ve dış ilişkilerinde tehlike yaratabilecek ve bu nedenlerle niteliği itibarıyla gizli kalması gereken bilgi ve belgelerdir" olarak tanımlanmıştır. Bununla birlikte devlet sırrı niteliği taşımayan diğer gizli bilgi ve belgeler (Devlet Sırrı Kanun Tasarısı, 2008, Madde 4), "devlet sırrı niteliği taşımayıp da, açıklanması veya öğrenilmesi hâlinde ülkenin ekonomik çıkarlarına, istihbarata, askerî

[63] 25673 sayılı Ceza Muhakemesi Kanunu'nun 47/1 fıkrasına göre "Bir suç olgusuna ilişkin bilgiler, Devlet sırrı olarak mahkemeye karşı gizli tutulamaz. Açıklanması, Devletin dış ilişkilerine, milli savunmasına ve milli güvenliğine zarar verebilecek; anayasal düzeni ve dış ilişkilerinde tehlike yaratabilecek nitelikteki bilgiler, Devlet sırrı sayılır". 25611 sayılı Türk Ceza Kanunu'nun "Devlet Sırlarına Karşı Suçlar ve Casusluk" başlıklı 7. Bölümünde devlet sırrı tanımlanmasa da türlere/konulara ayrılarak işlenecek suçlara ilişkin cezai yaptırımlar açıklanmıştır. Bu kapsamda "devlet güvenliğine ilişkin belgeler", "Devletin güvenliğine ilişkin bilgileri temin etme", "Siyasal veya askerî casusluk", "Devletin güvenliğine ve siyasal yararlarına ilişkin bilgileri açıklama", "Gizli kalması gereken bilgileri açıklama", "Uluslararası casusluk", "Askerî yasak bölgelere girme", "Devlet sırlarından yararlanma, Devlet hizmetlerinde sadakatsizlik", "Yasaklanan bilgileri temin", "Yasaklanan bilgilerin casusluk maksadıyla temini", "Yasaklanan bilgileri açıklama", "Yasaklanan bilgileri siyasal veya askerî casusluk maksadıyla açıklama", "Taksir sonucu casusluk fiillerinin işlenmesi", "Devlet güvenliği ile ilgili belgeleri elinde bulundurma" fiileri açıklanmıştır.

hizmetlere, idarî soruşturmaya ve adlî soruşturma ve kovuşturmaya zarar verebilecek nitelikteki veya yetkili makamlar tarafından gizlilik derecesi verilmiş bilgi ve belgeler, gizli bilgi ve belge" olarak tanımlanmıştır. Devlet sırrı niteliğinde olan belgeler süreli ve süresiz olarak saklanabilir. Süreli olarak saklanacak belgelerin 75 yılı geçemeyeceği ve 5 yılda bir gözden geçirileceği; süre belirtilmeyenlerin 50 yıl sonra bu niteliklerinin kalmayacağı ve her 10 yılda bir gözden geçirileceği ifade edilmektedir (Devlet Sırrı Kanun Tasarısı, 2008, 7/1,2,4). Bu tasarıda gizlilik sürelerine yönelik bir yapılandırmaya yer verilmesi önemlidir. Yürürlükte olan mevzuat düzenlemelerinde gizlilik derecesi olan belgelere yönelik sürelere ilişkin herhangi bir düzenleme bulunmamaktadır. Süreler kurumların değerlendirme komisyonları tarafından belirlenmektedir (Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik, 2022, 6/4) Gizlilik süresinin en fazla ne kadar olacağı ve bu konuda belge içeriğine dair objektif değerlendirme ölçütünün ne olacağı yer almamaktadır (Kaymak ve Külcü, 2024, s. 219). Tasarı, gizlilik sürelerinin belirlenmesi noktasında olay/konu bazlı olmasa da genel bir ölçüt ortaya koymaktadır.

Anılan düzenlemeler doğrudan gizlilik ve hassasiyete dair uygulama adımlarını ve ilkeleri ortaya koymaktadır. Bununla birlikte gizlilik hususundaki bazı konularda veya alanlarda işlerliğin sağlanması amacıyla çeşitli düzenlemeler bulunmaktadır. Örneğin 5902 sayılı Savunma Sanayii Güvenliği Kanunu, 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu, Dışişleri Bakanlığı Arşiv Hizmetleri Yönetmeliği[64], Güvenlik Soruşturması ve Arşiv Araştırması Yapılmasına Dair Yönetmelik, Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik, 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi, Millî Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesi vb. düzenlemeler

[64] Yönetmelikte Dışişleri Bakanlığı bünyesinde yer alan hassas bilgi içerikli arşiv belgelerinin imha işlemleri (22/6) kâğıt kıyma makineleri ile kıyılması ve ardından yakılması şeklinde tarif edilmektedir.

bulunmaktadır. Bu düzenlemeler çeşitli gizlilik derecelerini, yetki durumlarını, gönderim süreçlerini, transfer işlemlerini, muhafaza ve imhayı, değerlendirme komisyonlarını ve dosya yönetim süreçlerini ele almaktadır. Bunun dışında Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2020) tarafından yayınlanan "Bilgi ve İletişim Güvenliği" rehberi anılan tedbir genelgesi ile tüm kamu kurumlarına zorunlu kılınmıştır. Rehbere göre (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2020) özel nitelikli (hassas) veriler kritik bilgi/veri[65] olarak kabul edilmiş olup bu verilere yönelik tedbirler şu şekildedir:

- Veri tabanı üzerinde yer alan özel nitelikli kişisel veriler açık metin olarak tutulmamalıdır. İlgili bilgiler, ulusal ve/veya uluslararası standartlar tarafından kabul görmüş kriptografik yöntemlerden faydalanılarak saklanmalıdır (Tedbir No 3.2.7.10).
- Uygulama, özel nitelikli kişisel veri içeren hata mesajı veya iz kaydı üretmemelidir (Tedbir No 3.2.8.3).
- Özel nitelikli kişisel veriyi barındıran kayıtlar ulusal/uluslararası kabul görmüş güvenli yöntemlerle (şifreli metin olarak, güçlü şifreleme algoritmaları kullanarak, disk seviyesinde şifreleme vb.) saklanmalıdır (Tedbir No 4.1.1.9).
- Erişim kayıtları özel nitelikli kişisel veri barındırmamalıdır. Kayıtlarda özel nitelikli kişisel verinin bulundurulmasının zorunlu olduğu durumlarda, işlem detayının anlaşılabileceği şekilde kişisel verilerin güvenliği maskeleme vb. yöntemler ile sağlanmalıdır (Tedbir No 4.1.2.6).
- Özel nitelikli kişisel verilerin tutulduğu ortamlara erişim için çok faktörlü kimlik doğrulaması yapılmalıdır (Tedbir No 4.1.3.5).

[65] Kritik bilgi/veri olarak özel nitelikli veriler ile birlikte "Kritiklik derecesi 3 olarak hesaplanan varlıkların işlediği veriler" ve "Güvenlik zafiyeti oluşması durumunda yasal yaptırımlara neden olabilecek, içeriğinin yetkisiz personel veya kişiler tarafından görülmesinin kuruma çok ciddi maddi veya manevi zarar vereceği her türlü bilgi/veri" bu kapsamda değerlendirilmektedir (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi).

- Özel nitelikli kişisel verinin işlenmesi ve kişisel verinin üçüncü kişilere aktarılması durumunda açık rıza uygulama üzerinden alınmalı ve açık rıza beyan durumu sorgulanabilmelidir (Tedbir No 4.1.7.4).

Mevzuat ve güvenlik rehberi ile birlikte gizlilik konusunda standartlar da hem arşiv yönetimine hem de gizliliğe dair bir çerçeve sunmaktadır. Örneğin, TS 13298[66] Elektronik Belge ve Arşiv Yönetimi Sistemi Standardı'nda (2015, 9.2.3), "çok gizli", "gizli", "özel", "hizmete özel" ve "tasnif dışı" gizlilik derecelerine yer verilmektedir. Bu gizlilik dereceleri kapsamında yer alacak konulardan örnekler de sunulmaktadır. Bir diğer standart TSE K 523 Bilgi Varlıklarının Gizlilik Derecelerine Göre Sınıflandırılması Kriteri'dir. 2016 yılında yayımlanan bu standardın amacı "kurumlardaki bilgi varlıklarının belirlenmesi, gizlilik derecelerine göre sınıflandırılarak kurumlar arası bilgi paylaşımı esnasında bilginin gizliliğinin güvence altına alınması" olarak ifade edilmektedir (TSE K 523, 2016, s. 4). Standartta "çok gizli", "gizli", "özel", "hizmete özel", "ticari gizli", "ticari özel", "kişiye gizli", "kişiye özel" ve "tasnif dışı" olmak üzere 8 gizlilik derecesine yer verilmektedir.

Gizlilik söz konusu olduğunda erişime ve kurumsal şeffaflığa yönelik çerçeveyi Bilgi Edinme Hakkı kanunları oluşturmaktadır. Türkiye'de Bilgi Edinme Hakkı Kanununun Uygulanmasına İlişkin Esas ve Usuller Hakkında Yönetmelik'te arşiv malzemesi ve arşivlik malzemelere yönelik başvurular mülga 40. maddede[67] Arşivlerde Yararlanma Usul ve Esasları Hakkında Yönetmeliğin 14. maddesi esasınca yürürlükten kaldırılmıştır.

[66] Bu standart, AB belge yönetimi standartı MoReq 2, DoD 5015.2 ve ISO 15489'a dayalı olarak oluşturulmuştur. 2005 yılında başlatılan e-Dönüşüm Eylem Planı ile temelleri atılan standart, 2006'da Elektronik Belge Yönetimi Sistem Kriterleri Referans Modeline dönüştürülmüş; 2007 yılında TSE 13298 Bilgi ve Dokümantasyon- Elektronik Belge Yönetimi standardı olarak yayınlamış; son olarak 2015 yılında TS 13298:2015 Elektronik Belge ve Arşiv Yönetim Sistemi adını almıştır (Eroğlu ve Külcü, 2014, s. 335).

[67] Mülga Madde 40: Başvuru sahiplerinin; Devlet Arşivleri Başkanlığı veya araştırma hizmeti veren diğer arşivlerde mevcut arşiv malzemesi ve arşivlik malzemeden yararlanma şartları, yükümlülükleri ve arşiv malzemesinin örneklerinin verilmesi hususunda, 31/1/2002 tarihli ve 2002/3681 sayılı Bakanlar Kurulu Kararı ile tespit edilen hükümler, süre hariç olmak üzere uygulanır.

BEHK'nın 30. maddesinin ilgili bentleri (a, b, c, d) esasınca kamu kurumları bir önceki yıla ait:

a) Kendilerine yapılan bilgi edinme başvurularının sayısını,
b) Olumlu cevaplanarak bilgi veya belgelere erişim sağlanan başvuru sayısını,
c) Reddedilen başvuru sayısı ve bunların dağılımını gösterir istatistik bilgileri,
d) Gizli ya da sır niteliğindeki bilgiler çıkarılarak ya da bu nitelikteki bilgiler ayrılarak bilgi veya belgelere erişim sağlanan başvuru sayısını,

raporlaştırıp Türkiye Büyük Millet Meclisine (TBMM) göndermeleri gerekmektedir. TBMM takip eden yıl içerisinde bu bilgileri kamuoyu ile paylaşmaktadır. Bu madde ve uygulama daha önce anılan 30 Mayıs 2001 tarih ve 1049/2001 sayılı AP ve Konsey Tüzüğü'ne benzer bir hesap verilebilirlik anlayışını göstermektedir. Bu kapsamda 2022 yılı Bilgi Edinme Genel Raporu yayımlanmış olup, Cumhurbaşkanlığı'na yapılan taleplere ilişkin veriler (başvuru sayısı, olumlu cevaplar, kısmen olumlu veya reddedilenler vb.) paylaşılmıştır. T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı bağlı bir kurum olmasına rağmen açıklanan verilerin sağlandığı kurumlar[68] arasında bulunmamaktadır (TBMM, 2023 Yılı Bilgi Edinme Genel Raporu). DAB'ın arşiv belgelerini araştırma hizmetine sunmak, bilgi ve belge taleplerini karşılama görevinin (Kararnamenin 10/1-f bendinde belirtilen) yasal dayanaklarından bir tanesi de BEHK ve bu kapsamda alınacak başvurulardır. Ancak yapılan başvuru ve sonuçlara ilişkin istatistikî paylaşım bulunmamaktadır. Bu durum bilgi edinme başvurularının alınmadığına veya alınan başvurulara yönelik istatiskî veri paylaşımının yapılmadığına yönelik bir izlenim oluşturmaktadır. DAB 2023 Yılı Faaliyet Raporunda tasnif hizmetleri adı altında 91.689 adet "Belge Taleplerinin Karşılanması ve Özet Kontrolü" işlemi yer

[68] Raporda Cumhurbaşkanlığı İdari İşler Başkanlığı, Diyanet İşleri Başkanlığı, Millî Güvenlik Kurulu Genel Sekreterliği, Strateji ve Bütçe Başkanlığı ve Tasarruf Mevduatı Sigorta Fonu'na ait veriler bulunmaktadır (TBMM, 2022 Yılı Bilgi Edinme Genel Raporu). Bir önceki yıl (2022) Milli Saraylar İdaresi Başkanlığı veri sağlayan kurumlar arasında yer almıştır.

almaktadır (Devlet Arşivleri Başkanlığı 2023…, s. 50). Bu faaliyet BEHK'dan ziyade Belge Tarama Sistemi (BETSİS[69]) üzerinden alınan taleplerdir. Faaliyet raporunda Başkanlık, Ankara Cumhuriyet Arşivi yerleşkesinde verilen hizmetlere dair verileri paylaşmıştır. Buna göre anılan yerleşkede 983 adet "Kişisel Bilgi İçeren Belge Taleplerinin Karşılanması" işlemi gerçekleşmiştir. Raporun "Bilgi ve Belge Talepleri" başlığında 2023 yılında "273 kamu kurum ve kuruluşlar ile 2480 şahıslar olmak üzere toplam 2753 talep" karşılandığı ifade edilmektedir (Devlet Arşivleri Başkanlığı 2023…, s. 57). Bu taleplerin hangi kapsamda gerçekleştiği belirsiz olmak ile BEHK'nın ilgili maddesi (Madde 30) kapsamına uygun olarak açıklanmamıştır.

Türkiye'de ulusal arşiv misyonu taşıyan DAB, ulusal arşiv envanterini BETSİS aracılığıyla kamu erişimine sunmaktadır. Bu sistem, anılan diğer ulusal arşivlerde olduğu gibi çevrimiçi katalog görevi görmektedir. BETSİS'de araştırma hizmetine kapatılan gizli veya hassas belgelere yönelik bir bilgi veya varlık yoktur (Sesigür, 2023, s. 335). DAB kişisel veri içeren belgeleri ilgili kişi olmadığı sürece araştırma hizmetine sunmamaktadır. Ancak daha önce belirtildiği üzere (The National Archives, 2015, s. 7; Rukancı, Anameriç ve Başar, 2021, s. 169) sınırlama sebebi, fon içerisinde hangi belgelerin kapalı olacağı, kapatma süresi ve üst veri bilgisi paylaşılması gerekirken çevrimiçi katalogta yapılan incelemeler doğrultusunda kapalı veya sınırlı erişime sunulan belgelere ulaşılamamıştır. DAB, hassas bilgilere yönelik özel bir tutumu yansıtan doküman, rehber veya politikaya sahip değildir. Ancak Muhacir ve Mübadil belgelerini ilgili kişinin talep etmesi durumunda maskelenerek verildiği görülmektedir.[70] Bu durum doğrudan kişileri ilgilendiren bir mesele olduğundan çevrimiçi katalogda

[69] Türkiye Ulusal Arşiv (Devlet Arşivleri Başkanlığı) kataloğu için bkz https://katalog.devletarsivleri.gov.tr/

[70] Muhacir ve mübadil belgelerinde uygulanmakta olan bu işlem, yapılan arşiv ziyaretinde görülen örnekler üzerinden anlaşılmıştır.

bulunmamaktadır; bu da DAB'ın meslekî ahlak ve etik kurallar çerçevesinde uygulamalar yaptığını göstermektedir.

İncelenen ulusal arşivler değerlendirildiğinde hassas belgelere yönelik yaklaşımları farklılık göstermesine rağmen konuya ilişkin yaygın bir önem ve farkındalığın olduğu açıktır. Hassas bilgi içeren belgelere yönelik olarak ayrı bir yönetim uygulanmakta, bu belgeler doğrudan arşiv mevzuatında işlenmekte; çeşitli konularda yayınlanan rehber ve kılavuzlarda özel olarak değinilmekte; kurumlar ve kullanıcılar sorumlu tutulmakta; yalnızca bilgi erişim talebi geldiğinde ilgilenilmekte ve çevrimiçi katalogda farklı üst veriler kullanılmaktadır. Bazı ulusal arşivler hassas bilgi yönetimi ile ilgili her safhaya yönelik bir kılavuz geliştirmiştir. Çoğu arşiv, kataloglarında bu tür bilgi taşıyan belgelere yer vermektedir. Özellikle kullanıcı bağlamında arşiv kataloglarında şeffaf ve hesap verebilir toplum gereği kapatma ve kısıtlama gerekçeleri kamuoyu ile paylaşılmaktadır. Türkiye'de yürürlükte olan mevzuatın uygulamaya engel olabilecek düzeyde bir eksiklik barındırmadığı, uygulama içerisindeki boşluğun farkındalık ve süreç yönetimine dair ilkelerin oluşturulması ile giderileceği görülmektedir. Politika yapıcı kurumların kamuyu yönlendirici dokümanlar oluşturması hassas bilgi yönetimini etkin hale getirecektir. Bununla birlikte BEHK kapsamında alınan taleplere yönelik yıllık tablonun paylaşılması bu durumu destekleyecektir.

V. BÖLÜM: HASSASİYET DEĞERLENDİRMESİ SÜRECİNE İLİŞKİN UZMAN GÖRÜŞÜ ARAŞTIRMASI

V.1. Görüşme Sorularının Hazırlanması

Araştırma sorularının cevaplanabilmesi amacıyla konu uzmanlarının deneyimlerini ve görüşlerini açığa çıkaran sorular hazırlanmıştır. Bu kapsamda yarı yapılandırılmış görüşme tekniğine uygun olarak görüşme formu (EK-3) oluşturulmuştur. Görüşme sorularının hazırlanma sürecinde literatür araştırması sonucu elde edilen kaynaklar yol gösterici olmuştur. Özellikle 4. 7. 8. 9. ve 11. sorular hazırlanırken literatürde benzer noktalara dikkat çeken çeşitli kaynaklar (Sillitoe, 1998; Gollins ve diğerleri, 2014; The National Archives, 2015; The National Archives, 2016; Sloyan, 2016; Moss ve Gollins, 2017, McDonald, McDonald ve Ounis 2018; McDonald, 2019) çıkış noktası olarak kabul edilebilir. Bununla birlikte çalışmanın hazırlık süreci boyunca araştırma planlamasına dair ön görüşmeler ve ulusal arşivler ile yapılan yazışmalar etkili olmuştur. Sorulara dair planlamalar tamamlandıktan sonra görüşme form taslağı oluşturularak uzman görüşlerine başvurulmuştur. Sorular Bilgi ve Belge Yönetimi alanında belge yönetimi ve arşivcilik üzerine çalışmalar yürüten 2 uzmana (Doç. Dr. ve Arş. Gör. Dr.) ve aynı alanda nitel araştırma yöntemi konusunda tecrübeli 1 uzmana (Dr. Öğr. Üyesi) e-posta yolu ile (EK-4) gönderilmiştir. 3 uzmandan gelen görüşler doğrultusunda tüm soru kalıplarında yer alan net ve yönledirici ifadeler yorumlamaya açık hale dönüştürülmüş, soruların anlaşılabilirliği ve çalışma kapsamındaki yeterliği konusundaki görüşler dikkate alınmıştır. Taslak formda 15 olan soru sayısı uzman görüşleri sonrasında “uygun”, “uygun değildir” ve “öneri” seçenekleri doğrultusunda 1 soru iptali 2 soru eklenmesi ile 16 olarak sonuçlanmıştır. 16. soru yeni bir soru içermemekle birlikte katılımcının/gönüllünün konu ile ilgili ekleme, düzeltme ve yorumlamalarına fırsat sunmak amacıyla oluşturulmuştur.

Sorulara yönelik görüşler dikkate alınıp gerekli düzenlemeler sağlandıktan sonra 07.06.2024 tarihinde Ankara Üniversitesi Etik Kurulu Başkanlığı'na başvuruda bulunulmuştur. 05.07.2024 tarihinde etik kurul başvurusu (EK-1) onaylanmıştır.

V.2. Çalışma Grubu

Çalışma kapsamında veri toplanması hedeflenen kurumlarda görevli katılımcıların yer aldığı bir çalışma grubu oluşturulmuştur. Çalışma grubunu oluşturan katılımcıların seçiminde maksimum çeşitlilik örnekleme tekniği ile çeşitli yapılarda kurumların olmasına özen gösterilmiştir. Çalışma grubunda yer alacak görüşmecilere çalışma konusu hakkında bilgi verilerek görüşme randevuları talep edilmiştir. Bu kapsamda kurum izni talep eden görüşmecilerin bağlı bulunduğu kurumlara kargo veya e-posta yolu ile ulaşılarak izin talepleri iletilmiştir. Bu süreçte hedeflenen kurumlardan çoğunlukla olumsuz dönüşler alınmıştır. Çalışmanın devamlılığının sağlanabilmesi amacıyla anlamlı veri toplanılacağı düşünülen 10 bakanlığın ilgili birimleri ile telefon ve e-posta yoluyla iletişime geçilmiştir. Görüşme talepleri bilgi eksikliği, kurum politikası ve meslekî olmayan personel gerekçeleriyle çoğunlukla (9/10) reddedilmiştir. Çalışmanın genellenebilir olması amacıyla belirli uzmanlık alanında nitelikli bilgi düzeyine sahip kişiler hedeflenmiştir. Bu durum odak konuda uzmanlığın gelişmemesi ve farkındalık eksiliğinin bulunması sebebiyle yerli katılımcı sayısına doğrudan etki etmiştir. Bu bakımdan toplamda 8 gönüllü katılımcı ile görüşmeler gerçekleştirilmiş olup veri doygunluğuna ulaşılmıştır.

Görüşmelerde temel sorulardan önce katılımcılara eğitim ve çalışma süreleri ile ilgili demografik sorular yöneltilmiştir. Bu kapsamda katılımcıların eğitim bilgileri Tablo 6 ve Tablo 7'da çalışma süreleri Tablo 8'de yer almaktadır.

Tablo 6. Katılımcıların Mezun Oldukları Bölümler

Bölüm	***n***	***%***
Bilgi ve Belge Yönetimi	*2*	*25.*
Tarih	*2*	*25.*
Dokümantasyon ve Enformasyon	*1*	*12.5*
İlahiyat	*1*	*12.5*
Matematik ve Bilgisayar Bilimleri	*1*	*12.5*
İşletme	*1*	*12.5*
Toplam	*8*	*100*

Tablo 6'da sunulan veriler doğrultusunda katılımcıların farklı bölümlerden mezun (lisans) kişilerden oluştuğu görülmektedir. Dokümantasyon ve Enformasyon bölümünün Bilgi ve Belge Yönetimi çatısı altında yer almasından dolayı 3 katılımcının (%37,56) doğrudan Bilgi ve Belge Yönetimi alanından olduğu söylenebilir. Bununla birlikte katılımcıların farklı eğitim alanlarından ve kurumlardan (7 kurum) kişilerden oluşması veri çeşitliliğinin ve zenginliğinin sağlanmasına katkıda bulunmuştur.

Tablo 7. Katılımcıların Eğitim Düzeyleri

Bölüm	***n***	***%***
Lisans	*1*	*12.5*
Yüksek Lisans	*6*	*75*
Doktora	*1*	*12.5*
Toplam	8	100

Tablo 7'de sunulan verilere göre 6 katılımcı (%75) yüksek lisans, 1 katılımcı (%12,5) doktora mezunudur. Katılımcıların %87,5'i lisansüstü eğitim görmüşlerdir. Ayrıca Tablo 7'de kişileri işaret etme ihtimalinden dolayı belirtilmese de Bilgi ve Belge Yönetimi alanı

dışındaki 2 katılımcının (%25) bu alanda lisansüstü eğitim almış olması bir diğer önemli gösterge olarak ifade edilebilir. Toplamda 8 katılımcıyla yapılan görüşmelerde, katılımcıların farklı bölümlerden mezun olmalarına rağmen, hem uygulama tecrübelerinin hem de lisansüstü eğitimlerinin Bilgi ve Belge Yönetimi – özellikle arşivcilik – alanına odaklandığı görülmüştür. Katılımcı çeşitliliğini ortaya koyması bakımından görüşülen kurumlar ve katılımcıların görevleri de önemlidir. Katılımcıların ulusal arşiv (yurtiçi ve yurtdışı), kütüphane, üniversite, kamu kurumu ve özel kurumlarda çalışan gönüllüklerden oluşması veri çeşitliliğini desteklemektedir. Bununla birlikte hassas bilgi ve hassasiyet değerlendirmesi konusunda bilinçli olmaları ayrıca göz önünde bulundurulmuştur. Katılımcı sayısı, çalışmanın genel geçerliliği açısından sınırlı olabilir, ancak nitel veri analizinde bu çeşitlilik farklı perspektifler sunabilir. Bununla birlikte çalışma grubunda 2 uluslararası katılımcının (%25) yer alması hassasiyet değerlendirmesi konusunda farklı kültürel bakış açılarının ve deneyimlerin dahil edilmesini sağlamıştır.

Tablo 8. Katılımcıların Görev Süreleri

Görev süresi	***n***	***%***
6-10 yıl	*1*	*12,5*
11-15 yıl	*2*	*25,0*
16 yıldan fazla	*5*	*62,5*
Toplam	8	100

Tablo 8'de verilen bilgiler yarı yapılandırılmış görüşmelere katılan kişilerin görev sürelerine göre dağılımını göstermektedir. Verilere göre katılımcıların çoğunluğu olan 5 kişi (%62,5) kurumlarında 16 yıldan fazla görev yapmaktadır. Bu durum, çalışma grubunun çoğunlukla tecrübeli ve alanlarında uzun yıllar görev yapmış kişiler oluştuğu bilgisini vermektedir. 11-15 yıl arası görev yapmış katılımcılar %25 oranıyla ikinci sırada yer almaktadır. Görev süresi 6-10 yıl olan katılımcı ise %12,5 oranıyla en düşük katılımı

göstermektedir. Genel olarak, katılımcıların büyük çoğunluğunun deneyimli olması, çalışmada sunulan verilerin derinlik ve güvenilirliğini arttırmıştır.

V.3. Görüşmenin Uygulanması

Görüşme sorularının uygunluğunu test etmek, araştırma metodolojisinin işleyişini değerlendirmek amacıyla 24.07.2024 tarihinde nitel araştırma konusunda bir uzman ile çevrimiçi olarak pilot görüşme gerçekleştirilmiştir. Yapılan pilot görüşmede bazı görüşme sorularına açıklamalar eklenmesi gerektiği ifade edilmiştir. Belirtilen sorular anlam ve bütünlük dikkate alınarak iyileştirilmiştir. Bu kapsamda 1. ve 13. soruda düzenlemeler yapılmıştır. 1. soruda belirtilen hassas bilgi türleri görüşme yapılan katılımcının yaşadığı ülke dikkate alınarak açıklanmış, 13. soruda belirtilen etik ve hukukî problemlere yönelik örneklemeler ifade edilmiştir. Uzman, hassasiyet değerlendirmesi sürecinin evrensel bir yaklaşım ile ele alınmasını, araştırmanın Türkiye'de yürütülmesi ve hedeflenen katılımcıların çoğunluğunun (%75) buradan olması durumunun sorulara sirayet etmemesi ve belirli bir ülke özelinde yöneltilmemesi gerektiği uyarılarında bulunmuştur. Ayrıca katılımcıların sorulara vermiş olduğu cevapların diğer sorular ile ilişkilendirilmesi durumunda akışın sağlanabilmesi amacıyla bu konunun bir soru olarak konuşulacağı uyarısının yapılması gerektiği not edilmiştir.

Görüşmeler 08.08.2024 tarihinde başlamıştır. Görüşmeler, Tablo 9'de sunulan verilere göre katılımcıların 7'si ile çevrim içi olarak gerçekleştirilmiştir. Çevrimiçi görüşmeler Zoom programı araclığıyla yapılmıştır. Görüşmelere dair planlamaların yapılabilmesi amacıyla katılımcılarla yazılı ve sözlü iletişimler kurulmuş, uygun zaman dilimleri belirlenmiştir. Bu planlamalarda katılımcıların iş yoğunlukları ve izinleri dikkate alınarak, görüşmelerin programı esnek bir şekilde oluşturulmuştur. Bir katılımcı ile aynı şehirde bulunmanın sağladığı kolaylık ve yarı yapılandırılmış formatın avantajı olarak, beden dili ve mimikler gibi iletişim unsurlarından da faydalanılmıştır.

Katılımcılardan biri (K6) görüşmenin kayıt altına alınmaması talebinde bulunmuştur. Bunun üzerine bir el notu oluşturularak görüşme sürecindeki bilgi ve deneyim aktarımları kaydedilmiştir.

Tablo 9. Görüşme tarihleri ve süreleri

Katılımcı (k)	***Tarih***	***Süre***	***Ortam***
K1	*08.08.2024*	*01:02:20*	*Çevrimiçi*
K2	*20.09.2024*	*00:48:07*	*Çevrimiçi*
K3	*21.09.2024*	*00:54:11*	*Çevrimiçi*
K4	*22.09.2024*	*00:51:15*	*Çevrimiçi*
K5	*26.09.2024*	*00:54:06*	*Çevrimiçi*
K6	*30.09.2024*	-	*Çevrimiçi*
K7	*03.10.2024*	*01:10:37*	*Yüz yüze*
K8	*19.10.2024*	*01:00:34*	*Çevrimiçi*

Çalışmaya katılım, tamamen gönüllülük esasına dayanmış, katılımcıların kimliklerinin gizli tutulacağı ve elde edilen verilerin yalnızca araştırma amaçlı kullanılacağı taahhüt edilmiştir. Tablo 9'da sunulan verilere göre görüşmeler, belirlenen tarihte ve katılımcıların onayıyla kayıt altına alınarak görüşme süreleri not edilmiştir. Görüşme süreci boyunca katılımcılara görüşme formundaki (EK-3) sorular sırası ile yöneltilmiştir. Görüşmelerin sonunda katılımcılara teşekkür edilmiş ve elde edilen bilgilerin analiz sürecinde nasıl kullanılacağına dair bilgilendirmeler yapılmıştır. Çalışma kapsamındaki görüşmeler 19.10.2024 tarihinde tamamlanmıştır.

Görüşmelere dair verilen bilgiler (Tablo 9) doğrultusunda en uzun görüşme 70 dakika 37 saniye (K7), en kısa görüşme 48 dakika 7 saniye (K2) olarak kaydedilmiştir. Kayıt altına alınan 7 görüşmenin toplam süresi 6 saat 41 dakika 10 saniye, ortalama görüşme süresi 66 dakika 51 saniyedir. Bu veriler doğrultusunda en uzun ve en kısa

süreler arasında büyük bir farkın olmadığı katılımcıların görüşme sürelerinin dengeli olduğu söylenebilir. Katılımcıların genel olarak benzer düzeyde katılım gösterdiği görüşmelerin derinlemesine yürütüldüğü anlaşılmaktadır.

V.4. Araştırmanın Geçerliği ve Güvenirliği

Nitel araştırmalarda geçerlik ve güvenirlik, araştırmanın bilimsel niteliğini ve bulguların güvenilirliğini arttıran temel unsurlardır. Nitel araştırma yöntemleri literatüründe geçerlik ve güvenirlik (kendi içinde iç ve dış olarak ayrılan) konusunda inandırıcılık, aktarılabilirlik, tutarlılık ve teyit edilebilirlik (doğrulanabilirlik) kavramları araştırmayı destekleyen unsurlar olarak ifade edilmektedir (Güler, Halıcıoğlu ve Taşkın, 2015, s. 373; Yıldırım ve Şimşek, 2021, 289; Altunışık ve diğerleri, 2022, s. 487). Görüşme süreci başta olmak üzere araştırma bulgularının güvenilir ve genellenebilir olabilmesi için geçerlik ve güvenirlik ölçütleri dikkate alınarak izlenmiştir. Bu kapsamda hem geçerliği hem de güvenirliği sağlamak amacıyla nitel araştırma literatüründe önerilen uygulamalara dayalı olarak yapılanlar Tablo 10'da yer almaktadır.

Tablo 10. Geçerlik ve Güvenirlik Uygulamaları

Geçerlik	İç Geçerlik	Uzun süreli etkileşim kurulması Uzman görüşünün alınması Katılımcı onayı Doğrudan alıntı
	Dış Geçerlik	Ayrıntılı betimleme Amaçlı örnekleme
Güvenirlik	İç Güvenirlik	Ses kayıt cihazı kullanılarak veri kaybının önlenmesi Bulguların yorum yapılmadan sunulması
	Dış Güvenirlik	Sonuç bölümüne uygun olarak verilerin tartışılması Veriler arası tutarlık kontrolü için uzman kontrolü

Çalışmada iç geçerlik (inandırıcılık/*credibility*) sağlanabilmesi amacıyla katılımcılar ile uzun süreli etkileşimler kurulmuştur. Bu kapsamda e-posta yazışmaları ve telefon aramaları yoluyla görüşme randevuları oluşturulmuştur. Bu süreçte katılımcıların gizlilik kaygılarına dair bilgilendirmeler yapılmış, araştırmanın amacı açıklanarak kendilerini güvende hissetmeleri sağlanmıştır. Araştırma süreci boyunca bir nitel araştırma uzmanına soruların oluşturulması, görüşmenin uygulanması ve analiz safhalarında başvurulmuştur. Ayrıca iç geçerlik uygulamaları kapsamında katılımcıların üç defa teyidi alınmıştır. İlk teyit işlemi araştırmanın başlangıcında Aydınlatılmış Onam Formu (EK-2) aracılığıyla sağlanmıştır. Daha sonra görüşme transkripsiyonları katılımcılara sunularak onayları istenmiştir. Onay işlemlerinde görüşme kayıtlarına dair çıkarılmasını istedikleri ifadelerin, hatalı-yanlış transkripsiyonların olup olmadığı konusunda kendilerinden geri bildirim istenmiştir. Katılımcılardan hatalı kelime düzeltmesi konusunda dönüşler olmuştur. Bir katılımcıya ise bu konuda doğrudan başvurulmuştur. Ancak katılımcılardan bilgi çıkarımı konusunda bir dönüş olmamıştır. Bununla birlikte görüşmelerde katılımcılara "bunu mu demek istediniz" ifadeleri kullanılarak teyitleri sıklıkla alınmıştır. Çalışma kapsamında bulguların güvenilirliğini artırmak ve iç geçerliği sağlamak amacıyla görüşmeler doğrudan alıntılar kullanılarak aktarılmıştır. Bu aktarım sürecinde birebir ifadeler, manipüle edilmeden konuşmanın doğal akış sürecindeki hali ile sunulmuştur. Ayrıca iç geçerlik uygulamaları kapsamında yapılan görüşmelerin tarih ve süreleri (Tablo 9) olduğu gibi sunulmuştur. Bunun dışında iç geçerliği sınırlasa da veri toplama aracı olarak sadece görüşme yapılmıştır.

Çalışmada dış geçerlik (aktarılabilirlik/*transferability*) sağlanabilmesi amacıyla veri toplama sürecine dair hazırlık aşamaları, veri toplama sürecindeki uygulamalar ve çalışma grubunun özellikleri detaylı bir şekilde sunulmuştur. Araştırmacı çalışmanın uygulama kısmında betimleyici bir yaklaşım ile sürece dair adımları aktarmıştır. Ayırca dış geçerlik uygulamaları kapsamında çalışmanın katılımcıları belirlenirken amaçlı bir

örnekleme yaklaşımı izlemiştir. Bu durum çalışmanın başka durumlara veya benzer çalışma gruplarına uygulanabilir olup olmadığının değerlendirilmesine olanak tanımıştır. Dış geçerliği sınırlayıcı bir faktör olarak çalışmaya 8 kişisinin katılım sağladığı ifade edilebilir.

Çalışmada iç güvenirlik (tutarlılık/*dependability*) sağlanabilmesi amacıyla ses kayıt cihazı kullanılmıştır. Bu yöntem ile görüşmeler sırasında katılımcıların söyledikleri eksiksiz olarak kaydedilmiş veri kaybının önlenmesi sağlanmıştır. Ayrıca bulguların yorum yapılmadan sunulması, iç güvenilirliği destekleyerek okuyuculara, katılımcıların düşüncelerini kendi bağlamlarında değerlendirme fırsatı sunulmuştur.

Son olarak çalışmada dış güvenirlik (doğrulanabilirlik/*confirmability*) sağlayabilmek amacıyla elde edilen veriler sonuç bölümüne uygun olarak değerlendirilerek tartışılmıştır. Bu süreçte araştırma sonuçlarını çalışma verileri ile karşılaştırmak için uzman kontrolüne başvurulmuştur. Uzmandan gelen dönüşler fikir ve görüş birliğini teyit ederek dış güvenirliği arttırmıştır.

Araştırmanın ve yapılan görüşmelerin geçerlik ve güvenirliğini destekleyen en önemli unsurlardan biri altı ayda bir düzenli olarak gerçekleştirilen tez izleme komitesi toplantılarıdır. Komite üyelerinin geri bildirimleri ve önerileri sürecin tutarlı bir şekilde ilerlemesine yardımcı olmuştur.

V.5. Veri Analizi

Veri analizi, görüşmecilere ait (7 kayıt) ses kayıtlarının deşifre edilme hazırlıkları ile (yazıya dökme) başlamıştır. Ses formatındaki kayıtlar yapay zekâ destekli çevrimiçi bir web sitesi olan *transgate.ai* kullanılarak dokümante edilmiştir. Bu web sitesi, ses dosyalarını hızlı ve doğru bir şekilde deşifre ederek verileri analiz edilebilir metin formatına dönüştürmüştür. Her kayıt sisteme yüklenerek, transkripsiyonları Microsoft Word formatında alınmıştır. Toplamda 401 (6 saat 41 dakika) dakika ses kaydından 112

(Times New Roman, 12 punto 1,5 satır aralığı) word sayfası metin oluşmuştur. Bu süreçte ayrıca 2 katılımcı ile yapılan İngilizce görüşme kayıtlarının transkripsiyonları Türkçeye birebir olarak çevrilmiştir. Daha sonra elde edilen metinler ses kayıtları ile karşılaştırılarak gözden geçirilmiş olası hata ve eksiklikler kontrol edilmiştir. Düzenlenen metinler, veri analizi için hazır hale getirilmiş ve kodlama aşamasına geçilmiştir.

Nitel veri analizinde elde edilen metinlerdeki temel kalıplar kod-kategori-tema yaklaşımı kullanılarak incelenmiştir. Bu yaklaşımın kullanılmasının temel sebebi, katılımcıların deneyimlerini ve algılarını derinlemesine analiz edilmesini ve araştırmanın teorik çerçevesine uygun şekilde yapılandırılmasını sağlamaktır. Analiz sonucu oluşan kodlar, "örüntüler saptamak, veriyi kategorize etmek, iddia ya da önerme geliştirmek, temellendirilmiş kuram gibi analitik süreçlerde kullanılmak üzere her bir veriye yorumlanmış anlamlar yüklemek amacıyla araştırmacı tarafından üretilmiş yapıları" ifade etmektedir (Saldana, 2019 s. 4). Çalışmada sınırlı düzeyde katılımcı yer aldığından kod atamalarında anlamlı, özgün ve farklılaşan ifadeler/yorumlar sunan bir katılımcın görüş bildirmesi yeterli kabul edilmiştir. Her bir katılımcının farklılaşan yorumlamaları veri kaybının önlenmesi için anlamlı olurken tekrar eden kodlamalar atanılan kodun değerini pozitif yönde etkilemiştir. Aynı konu veya ilişki grubundaki kodlar bir araya getirilerek kategoriler, benzer bir yaklaşım ile kategorilerden temalara ulaşılmıştır. Kod-kategori ve temalar oluşturulurken hem tümdengelimci hem de tümevarımcı analiz anlayışı benimsenmiştir. "Tümdengelimci içerik analizi var olan kuramlar ve araştırma sonuçları çerçevesinde önceden belirlenmiş temalara göre verilerin kodlanması ve analizi" sürecinde kullanılmaktadır (Yıldırım ve Şimşek, 2021, s, 82). Tümevarımcı analiz "veri içinde örüntülerin, temaların ve kategorilerin keşfedilmesini içerir. Veriler mevcut çerçevelere göre analiz edildiği tümdengelimsel analizin tersine, bulgular araştırmacının veriyle etkileşimi yoluyla verilerden çıkar" (Patton, 2018, s. 453). Analiz sürecinde iki yaklaşımın bir arada kullanılması, hem teorik çerçeveyi destekleyen bulguların test

edilmesine hem de verilerden yeni ve beklenmedik sonuçlar çıkarılmasına olanak sağlamıştır.

Nitel veri analizi sürecinde, kod-kategori ve tema oluşturma yaklaşımları belirlendikten sonra elde edilen görüşme kayıtlarının sistematik olarak incelenmesi amacıyla öncelikle ön kodlamalar yapılmıştır. Ön kodlama işlemi her katılımcıya ait görüşme transkripsiyonları tamamlandıktan sonra başlamıştır. Bu durum veri analiz sürecinin hızlanmasına ve kod sisteminin kümülatif olarak gelişmesine yardımcı olmuştur. Bu aşamada, MAXQDA veri analizi programına aktarılan verilerde öne çıkan önemli noktalar, tekrarlayan ifadeler memolar halinde ilk kodlama işlemine tabi tutulmuştur. Daha sonra, görüşme kayıtları belirli periyotlarda tekrar okumalardan geçirilerek ön kodlamalar olgunlaştırılmış nihai kod kitabı (EK-5) oluşturulmuştur. Kod kitabı, deneyimli bir uzmana sunularak kod-kategori-tema ilişkisi konusunda görüşleri istenmiştir. Uzman ile yapılan değerlendirme sonucunda ortaya çıkan görüş ayrılıkları, karşılıklı tartışma ve fikir alışverişi yoluyla çözüme kavuşturulmuştur. Böylelikle nihai temalar ve kategoriler oluşturulmuştur. Bu süreç sonucunda 5 tema, 18 kategori ve toplamda 101 kod oluşmuştur.

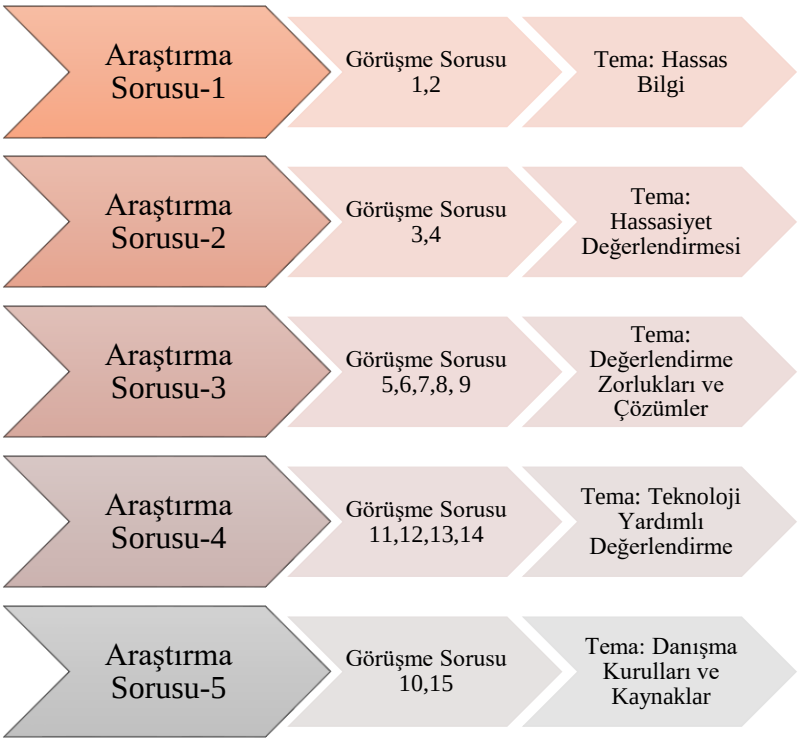
Aynı kodun (yapay zekâ) farklı temalardaki kategoriler altında yer alması bu kodun kategori olarak değerlendirilmesine sebep olmuştur. Bu durum, bir verinin ya da bilginin birden fazla kavramsal çerçeveye veya bağlama uyum sağlayabilme yeteneğini ortaya koyarken katılımcıların aynı kavram etrafında çözümler bulduğuna işaret etmektedir. İlişkili kategorilerde bu kategoriye yönlendirmeler yapılarak bağlantılar kurulmuştur.

V.6. Bulgular

Bulgular araştırma soruları çerçevesinde analiz edilerek tema-kategori-kod yapısına dayalı olarak sınıflandırılmıştır. Bulgular sunulurken verilerin anlamlı bir şekilde

organize edilmesi hedeflenmiştir. Her katılımcıya ilişkin kodlamaların tamamı alıntılara yansıtılmamıştır. Alıntılar sunulurken katılımcının kimliğini veya kurumunu açığa çıkarabilecek ifadeler ile ilgisiz konuların çıkarılması amacıyla (anlam bütünlüğünü bozmadan ve veri manipülasyonu yapmadan) "üç nokta (…)" işareti kullanılmıştır. Üç nokta kullanılan alanda öncesinde veya sonrasında bu tür ifadelerin olduğu anlaşılmaktadır. Ayrıca bu uygulama kodların hangi katılımcılar tarafından oluşturulduğu bilgisini sunarken kurum ve kişiler ile bağdaşmamasını sağlamıştır. Araştırma sorusu için anlamlı cevaplar aranırken tekrardan kaçınmak amacıyla belirli temalar altında yoğunlaşan ya da aynı anlama gelen ifadeler yalnızca örnek niteliğinde kullanılmıştır. Tekrarlayan kodlamalar, bir örüntü oluşturduğundan, anlamlı kodlamaların yapıldığını gösterir. Bu yaklaşımla bulguların daha açık ve anlaşılır bir şekilde sunulması, gereksiz detaylarla dikkat dağınıklığının önlenmesi, katılımcıların söylediklerinin özünü yansıtan ve araştırmanın genel sonuçlarını en iyi şekilde sunan kodların kullanılması sağlanmıştır.

Araştırma soruları çalışma içerisinde kavramsal arka planın verildiği bölümlerde literatüre dayalı olarak irdelenmiştir. Özellikle bazı araştırma soruları literatür, web siteleri, e-posta yazışmaları yolu ile cevaplanmıştır. Bulguların sunulduğu bu bölümde ise görüşme soruları aracılığıyla cevaplanması beklenen araştırma soruları (Tablo 11) katılımcılardan elde edilmiştir. Bu bakımdan araştırma soruları çerçevesinde yapılandırılan görüşme sorularına ait veriler, temalara ayrılarak kategori ve kodlamalar yolu ile değerlendirilmektedir. Araştırma soruları, görüşme soruları ve temalar arasındaki bu ilişki aşağıda sunulmuştur. Bulguların sunumunda bu yaklaşım benimsenmektedir.



Tablo 11. Araştırma-Görüşme Soruları Tema İlişkisi[71]

Bulguların sunumunda öncelikle kod-kategori-tema arasındaki ilişkilere dair betimsel bulgulara yer verilmektedir. Bu uygulama, verilerin daha hızlı, etkili ve derinlemesine anlaşılmasına katkı sağladığından, çalışma verilerine uygun görselleştirmeler tercih edilmiştir. Daha sonra katılımcıların konu hakkındaki görüşleri kategoriler altında sunulmuştur.

[71] Bu tablo, araştırma sorularının cevaplanması amacıyla hangi görüşme sorularının yöneltildiğini ve sonuç olarak hangi temaları oluştuğunu göstermektedir. Tablodaki araştırma soruları çalışmanın ikinci ve üçüncü bölümlerinde litetatüre bağlı olarak ayrıca incelenmiştir. Tabloda yer almayan altıncı araştırma sorusu çalışmanın 4. bölümünde ulusal arşivlerin incelenmesi yolu ile açıklanmıştır.

V.6.1. Kelime Bulutu

Görüşme verilerinde en az 10 kez tekrar eden 100 kelimeye ilişkin kelime bulutu (Görsel 13) oluşturulmuştur. Kelimelerin punto büyüklüğü-küçüklüğü, renklerin koyuluğu-açıklığı, kelimelerin ortada veya kenarda geçmesi tüm metinlerde geçme sıklığı ile birlikte önemini ifade etmektedir.

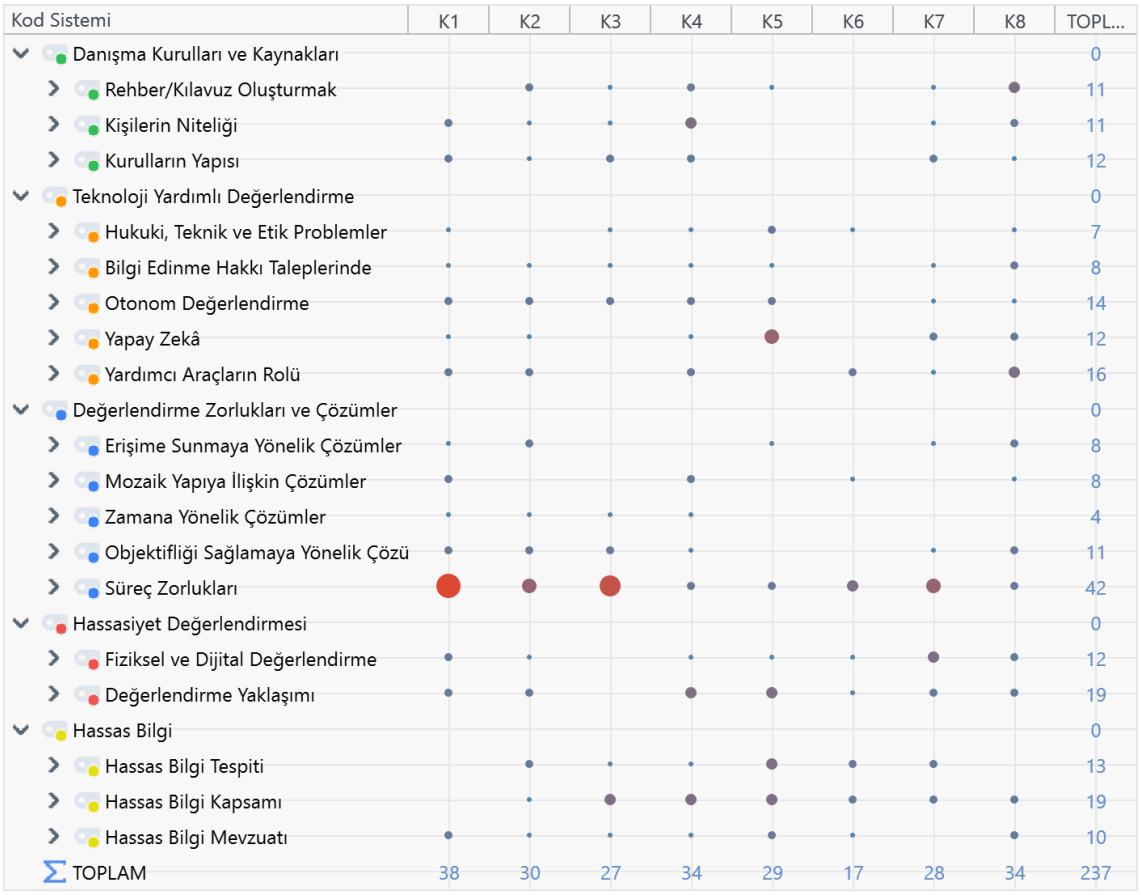
Görsel 13. Görüşme Verilerine Ait Kelime Bulutu

Büyük puntolu kelimeler, araştırmanın odak noktası olan ve metinde daha fazla yer bulan kavramlardır. Görselde sunulan kelimeler doğrultusunda hassas, hassasiyet, gizlilik, bağlam, zaman, dijital, elektronik bağımsız danışma, mevzuat gibi kelimeler çalışmada vurgulanan konular hakkında ipucu vermektedir.

V.6.2. Tema ve Kategorilerin Kod Matrisi

Verilere ilişkin kod matrisi (Tablo 12) katılımcıların her tema ve kategoride katılımlarının nasıl dağıldığını ve hani kategorinin öne çıktığını göstermektedir. Bununla birlikte katılımcıların kod sayılarını (K2- 30 kod) ve toplam kod (237) sayılarını sunmaktadır.

Dairesel noktalamalar her bir katılımcının hangi tema ve kategoride daha çok veya az katılım yoğunluğunu ifade etmektedir.



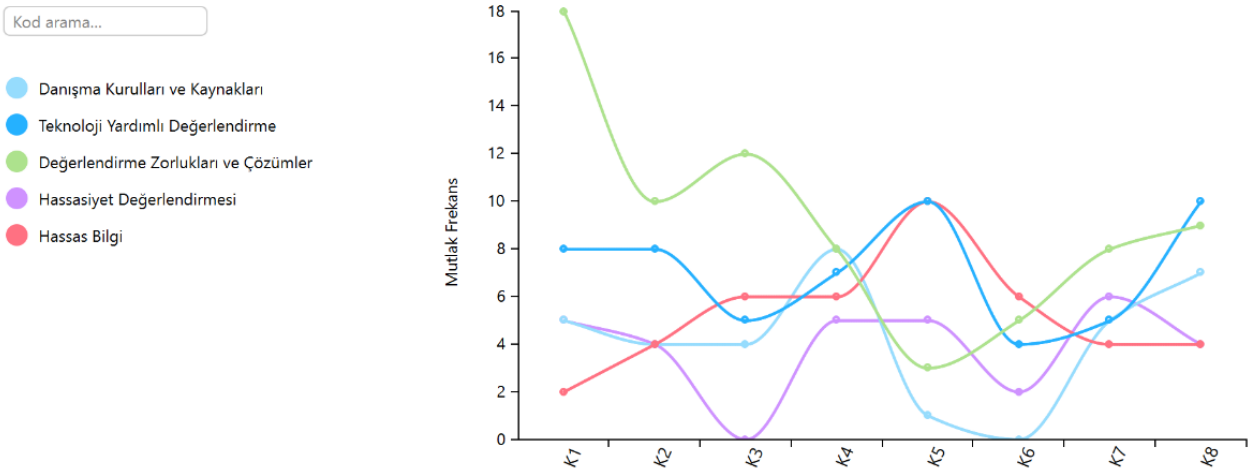
Tablo 12. Temaların ve Kategorilerin Katılımcılara Göre Dağılımı

Örneğin K1 katılımcısı Değerlendirme Zorlukları ve Çözümler teması altında bulunan Süreç Zorlukları kategorisinde büyük katkılar sunarken aynı temada yer alan Objektifliği Sağlamaya Yönelik Çözümler kategorisinde katkıda bulunmuştur. Ayrıca herbir kategoride kaç kodlamanın yer aldığını bilgisi katılımcıların hangi kategoriye yoğun olarak katkı sağladığı bilgisini vermektedir. Katılımcılar Süreç Zorlukları Kategorisine en fazla katkıyı; Zamana Yönelik Çözümler kategorisinde en az katkıyı sağlamışlardır. Kod matrisi ayrıca araştırma sorularına yönelik temalara katılım hakkında bilgi sunmaktadır. Bu bakımdan Değerlendirme Zorlukları ve Çözümler temasına katılımcıların yoğun olarak (73 kod) katıldığı, Hassasiyet Değerlendirmesi temasına düşük katılım sağlandığı (31 kod) ifade edilebilir. Katılımcı bazında da benzer okumayı

yapmak mümkündür. K1 katılımcısının en fazla kod (38); K6 katılımcısının en az kod (17) katkısı sunduğu görülmektedir.

V.6.3. Tema Trendleri

Katılımcıların temalara göre eğilimlerini gösteren (Grafik 2) grafik her bir katılımcıya dair bilgiler sunmaktadır. Mutlak Frekans ekseninde her bir temayı temsil eden renkli çizgiler frekansların zaman içinde nasıl değiştiği görülmektedir.



Grafik 2. Katılımcılara Göre Tema Trendleri

Örneğin hassas bilgi temasına (kırmızı) K5 katılımcısının diğer katılımcılara göre en fazla katkıyı sağladığı; hassasiyet değerlendirmesi temasına K3'ün en az katkıyı sağladığı görülmektedir. Teknoloji Yardımlı Değerlendirme teması grafik boyu eşit bir dağılım gösterirken Değerlendirme Zorlukları ve Çözümler teması dengeli bir eğilim göstermemektedir. Bu durum temaya ait kodların belirli katılımcılar tarafından oluşturulduğu bilgisini vermektedir. Bununla birlikte, Hassasiyet Değerlendirmesi ve Hassas Bilgi temalarındaki artışlar, bu konuların belirli katılımcılar tarafından daha fazla önemsendiğini ve dikkat çekildiğini göstermektedir.

V.6.4. Tema: Hassas Bilgi

"Dünyada ve Türkiye'de veri koruma/gizlilik veya kişisel veri mevzuatında hangi bilgiler hassas olarak nitelendirilmektedir? Bu bilgilerin kapsamı, tespiti ve işlenme koşulları nasıl belirlenmelidir?" araştırma sorusunun cevaplanması amacıyla yöneltilen görüşme sorularına verilen cevaplar, kategori ve kodlar ayrılmıştır.

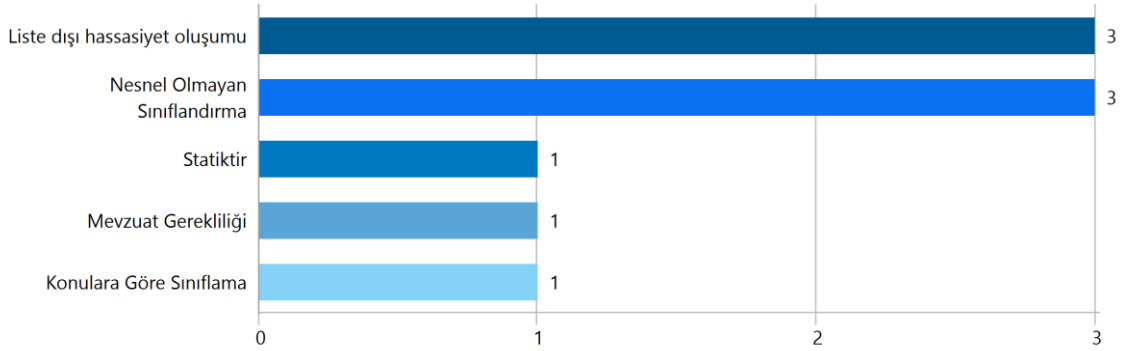
Tablo 13. Hassas Bilgi Temasına Ait Kategori ve Kodlar

Kategori	Kodlar	Katılımcılar
Hassas Bilgi Mevzuatı	Nesnel Olmayan Sınıflandırma	*K1, K3, K8*
	Liste dışı hassasiyet oluşumu	*K4, K6, K8*
	Konulara Göre Sınıflama	*K2*
	Mevzuat Gerekliliği	*K1*
	Statiktir	*K5*
Hassas Bilgi Kapsamı	Kurum Bazlı Sınıflama	*K3, K5, K7, K8*
	Geniştir	*K5, K6, K8*
	Görecelidir	*K2, K3, K6*
	Güncellenebilir Olmalı	*K4, K5, K7*
	Hem Kamusal Hem Kişisel	*K4*
	Süreç Tabanlı Belirleme	*K3*
Hassas Bilgi Tespiti	Formattan Bağımsız	*K1, K2, K3, K4, K5, K6, K7*
	Yardımcı Doküman	*K5, K6, K7*
	Usul ve Esaslara Göre	*K5, K6*
	Tanım Esaslı Tespit	*K5*
	Bağlama duyarlı	*K2*

Tablo 13'te sunulan verilere göre katılımcıların görüşme sorularına verdikleri cevaplar hassas bilgi teması kapsamında üç kategori altında toplanmıştır. Bu kategorilerin altında yer alan kodlar, katılımcıların bakış açılarını özetleyen bir analiz sunmaktadır. Veriler doğrultusunda kategorilere katılımcıların tamamının eşit düzeyde katılım sağlamadığı; hassas bilgi tespiti kategorisinde yer alan "Formattan Bağımsız" koduna hemen hemen her katılımcının katılım sağladığı ve bazı kategorilerin sınırlı sayıda katılımcının görüşleri ile şekillendiği gözlemlenmektedir. Bazı katılımcılar (K5 ve K6) ise tüm kategorilerde en fazla katkı sağlayan kişiler olarak öne çıkmaktadır Bununla birlikte her bir katılımcnın sunulan üç kategoriden en az bir tanesinde görüş beyan ettiği görülmektedir.

V.6.4.1. Kategori: Hassas Bilgi Mevzuatı

Hassas bilgi mevzuatı kategorisinde görüş beyan eden yedi katılımcı tarafından beş farklı görüş (Grafik 3) sunmuştur. Katılımcılara göre mevzuatta ağırlıklı olarak nesnel olmayan sınıflandırma yapılmaktadır.



Grafik 3. Hassas Bilgi Mevzuatı

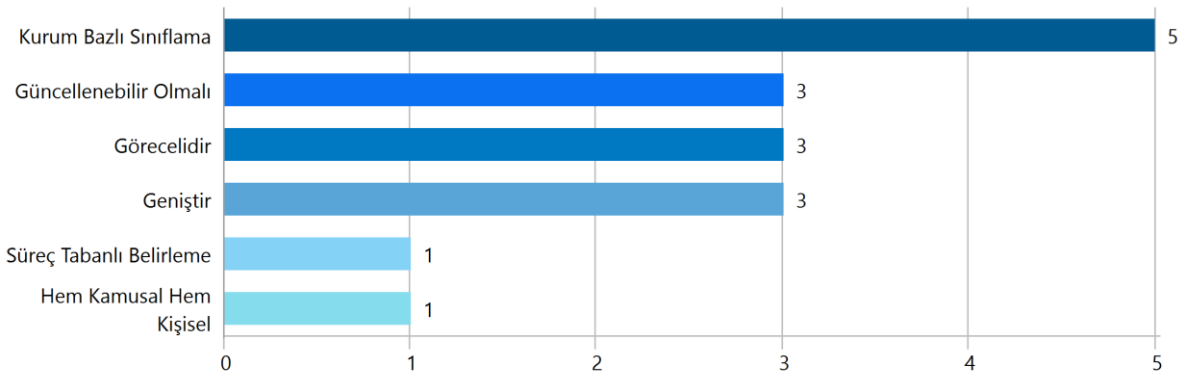
Bu konuda K3, "*Tam nesnel ölçüleri içermese de bu şekilde bilgi sınıflandırılması yapılmaktadır*" ifadesi ile mevzuatın nesnel olmadığına işaret etmektedir. Bilgi sınıflandırmalarının nesnel olmaması mevzuatın dışında oluşabilecek hassasiyetleri ortaya çıkarabilmektedir. Katılımcılar bu konuyu liste dışı hassasiyet oluşumu kodu çerçevesinde değerlendirmektedir. K4, "*Bu türlerin dışında da, listelenen türler dışında da yeni hassasiyetler oluşabilir. Çünkü bunları direkt sınırlamak doğru olmaz*" ifadeleriyle hassasiyetin listelemeler yolu ile sınırlandırılmaması gerektiğini belirtmektedir. Bu görüşü K6, "*Evet, mevzuatın dışında da birçok hassasiyet mevcut, özellikle kültürel hassasiyet şu anda üzerinde düşündüğümüz belirgin bir eksiklik*" ifadeleri ile desteklemiş hassasiyet oluşumunun başka bir yönüne dikkat çekmiştir.

Hassas bilgi mevzuatı kategorisinde K2, mevzuatın konulara göre sınıflandırıldığını ve tüm konuları kapsayabileceğini "*Yasal nedenler sunuyor; bu nedenler bilginin neden sunulamayacağını açıklıyor ve bu nedenler bekleyebileceğiniz tüm konuları kapsıyor"* ifadeleri ile belirtmektedir. K1, bu konuda münferit bir mevzuatın olması gerektiğini "*Bunun bir mevzuatının olması lazım diye düşünüyorum. Hassas bilgi*

için ise böyle bir şey maalesef hiç yok zaten" ifadeleri ile vurgulamaktadır. Bu kategoriye ilişkin son olarak bir katılımcı mevzuatın statik yönünü eleştirmiştir. K5, "*Hassas bilgilerin ne tür bilgiler olduğu her daim dinamik olarak belirlenebilme sistem, öyle bir sistem tasarlanması lazım. Yani ben bugün şu şu bilgiler hassas deyip 3 yıl, 5 yıl, 10 yıl sadece o bilgileri hassas kabul edip diğerlerini es geçiyor ya da görmezden geliyor olmam büyük hata olur"* ifadeleri ile düşüncelerini aktarmıştır.

V.6.4.2. Kategori: Hassas Bilgi Kapsamı

Hassas bilgi kapsamı kategorisinde görüş beyan eden yedi katılımcı altı farklı görüş (Grafik 4) sunmuştur. Katılımcılar önceliklike kapsama dair durum tespiti (geniş, görece, güncellenmeli) niteliğinde görüşler belirtmiş; sonrasında kapsama dair fikirler (kurum bazlı, hem kamusal hem kişisel, süreç tabanlı) beyan etmişlerdir.



Grafik 4. Hassas Bilgi Kapsamı

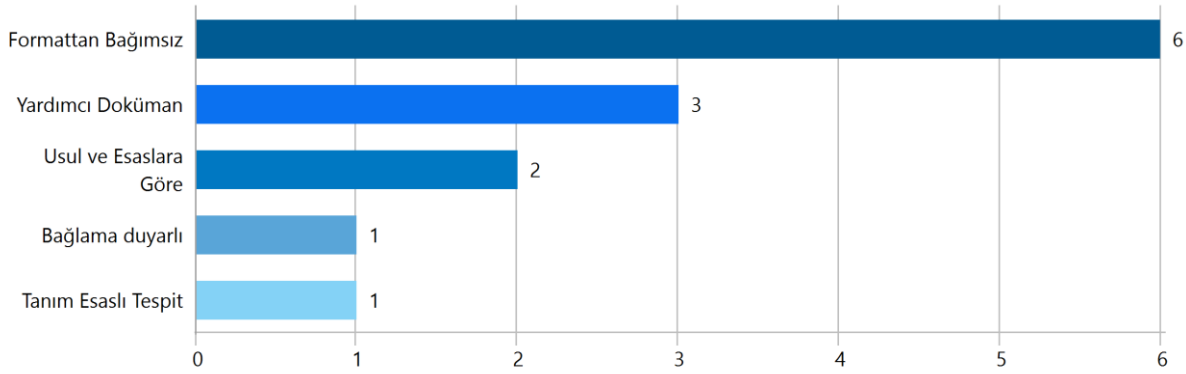
K6, "*Kategoriler her şeyi kapsamıyor ve oldukça geniş olabilir*" ifadeleri ile hassas bilginin kapsamının geniş olduğunu; K3, "*Belirlenmiş ama bu hassasiyetlerin belirlenmesi konusunda yine insanların yetkililerin subjektif görüşlerine yer veriliyor*" ifadeleri ve K2, "*Farklı karar vericiler farklı sonuçlara varabilir*" ifadeleri ile göreceli olduğunu; K4, "*Temel standart anlamda bir tanımlama tespit yaptığımız zaman günün şartlarına göre değişim gerektiren durumlarda bu tanımlamaya bağlı kalırsak eksik*

kalacağını düşünüyorum. O yüzden bu tanım ve tespit kapsamın yenilenebilir, her zaman güncellemeye açık olabilir bir yaklaşımla benimsenmesi gerektiğini düşünüyorum" ifadeleri ile güncellenebilir olması gerektiğini belirtmektedir.

Hassas bilgi kapsamının nasıl belirleneceğine dair katılımcılar ideal olarak olması gerekene dair bazı fikirler sunmuşlardır. K3, "*Kurumsal bazda süreç tabanlı bilgi hassasiyet belirleme süreç prosedürü yapılmasını... Şöyle ki ABD Savunma Bakanlığı'nda bu konuda 6 adımlı bir süreç belirleme prosedürü var*" ifadeleri ile hassas bilgi kapsamının süreç tabanlı olarak belirlenmesi gerektiğini; K4, "*Yani bir kişilere bağlı bir de kişilerin dışında gelişen şeyler var. Hem kurumsal olsun hem kişiler olsun yine bir açık alan bırakmak gerekiyor*" ifadeleri ile hassas bilgi kapsamının hem kamusal hem kişisel çerçevede ele alınması gerektiği belirtmektedir. Bu kategoride katılımcıların üzerinde mutabık kaldığı kod, hassas bilgi kapsamının kurum bazlı sınıflama yolu ile çizilmesidir. K3, "*Kurumsal bazda bir hassasiyet belirleme prosedürlerinin yapılması gerektiğini düşünüyorum*" ve K7, "*Kurumların kendi hassas bilgileri, kendi sektörlerine barındırdıkları kurumlarında barındırdıkları, ürettikleri, işlem aldıkları, üzerinde çalıştıkları, depoladıkları hassas bilgi türlerine göre… mevzuat… geliştirilmesi gerekir*" ifadeleri ile kurum bazlı hassas bilgi envanterinin oluşturulması gerektiğine dikkat çekmişlerdir.

V.6.4.3. Kategori: Hassas Bilgi Tespiti

Hassas bilgi tespiti kategorisinde görüş beyan eden yedi katılımcı beş farklı görüş (Grafik 5) sunmuştur. Katılımcıların görüşleri çeşitli öneriler etrafında toplanmıştır. Bu konuda bir öneri olmayan ancak bir durum tespiti niteliğinde olan "Formattan Bağımsız" kodu, katılımcıların en çok vurguladıkları ve mutabık oldukları görüştür.



Grafik 5. Hassas Bilgi Tespiti

K4, "*Bir belgenin hassas olması bence içeriğiyle ilgili. O yüzden bir belgenin elektrik ya da kâğıt ortamında olması içeriğini değiştirmediği için hassasiyetini değiştireceğini düşünmüyorum açıkçası*" ve K7, "*Mesela X kişinin sağlık dosyası, isterse fiziksel olsun, isterse dijital olsun, hassassa hassastır*" ifadeleri ile formatın hassas bilgi tespiti noktasında bir etkisi olmadığını içerik ile ilgili bir mesele olduğunu belirtmektedir. İçerik konusunda K2, "*Bilgilerin hassas olup olmadığını anlamak için bir bağlamsal anlayışa ihtiyacınız vardır*" ifadeleri ile hassas bilgi tespitinin bağlama duyarlı olduğu tespitinde bulunmuştur. Bununla birlikte katılımcılar hassas bilgi tespitinin nasıl yapılması gerektiği konusunda çeşitli önerilerde bulunmuştur. K5, "*Din, dil, ırk, meslek, maaş, disiplin, güvenlik soruşturması vs. bunları tek tek yazmak yerine kapsamı tanımlamak, tanım üzerinden gidip daha bilgiyle uğraşanlara böyle bir alan ve inisiyatif tanımak daha doğru olur diye düşünüyorum*" ifadeleri ile tespitin tanım esaslı olarak yapılabileceğine işaret etmektedir. K6, "*Prosedürlere sahip olmak son derece faydalıdır*" ifadeleri ile usul ve esasa göre tespit yapılması gerektiğini belirtmiştir. Bu görüşü K5 "*Bence yapılması gereken hassas bilgi nedir? Hassas bilgi nasıl ortaya konur? Yöntemi usulü nedir? Hangi sorular sorulur? Hassas bilginin özellikleri nedir? Bunları biraz daha genel bir kavramla yani bir yaklaşım şeklinde ortaya konursa mevzuatta da direkt hassas bilgi tanımı yerine hassas bilginin belirlenmesi için uygulanacak usul esas yöntem yaklaşım gibi şeyler belirlenirse şey olur daha doğru bir yaklaşım olur*" ifadeleri ile desteklemiştir. Bununla

birlikte tespit işlemlerinde kullanılacak yardımcı dokümanlara duyulan ihtiyaç vurgulanmıştır. K7, "*Kılavuzlarla politikalarla stratejilerle şekillenen bir yaklaşım olması gerekir*" ve K5 "*Yön gösterici yol gösterici bir döküman hazırlanırsa daha doğru olur*" ifadeleri ile bu ihtiyaca dikkat çekmişlerdir.

V.6.5. Tema: Hassasiyet Değerlendirmesi

"Hassas bilgi içerikli belgelere yönelik değerlendirme süreci (hassasiyet değerlendirmesi) nasıl yürütülmelidir? Bu süreç fiziksel ve dijital ortama göre farklılık oluşturur mu?" araştırma sorusunun cevaplanması amacıyla yöneltilen görüşme sorularına verilen cevaplar, kategori ve kodlar ayrılmıştır.

Tablo 14. Hassasiyet Değerlendirmesi Temasına Ait Kategori ve Kodlar

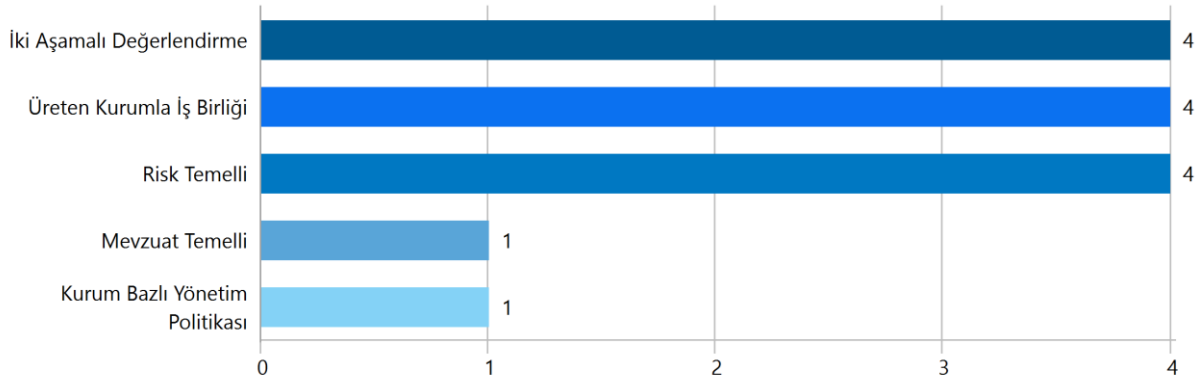
Kategori	Kodlar	Katılımcılar
Değerlendirme Yaklaşımı	Risk Temelli	*K2, K6, K7, K8*
	Üreten Kurumla İş Birliği	*K1, K2, K4, K5*
	İki Aşamalı Değerlendirme	*K1, K2, K4, K5*
	Kurum Bazlı Yönetim Politikası	*K8*
	Mevzuat Temelli	*K7*
Fiziksel ve Dijital Değerlendirme	Dijital Bilginin Riski Yüksektir	*K6, K7, K8*
	Formata Göre Yönetim Farklılığı	*K4, K7*
	Benzer Süreç Yönetimi	*K1*
	Yöntemden Bağımsız Risk	*K2*
	Kâğıt Ortam Daha Kontrolsüz	*K5*
	Dijital Ortam Daha Kontrolsüz	*K7*
	Dijital Belge Miktarının Fazlalığı	*K6*
	Dijital Belge İlişkisini Kurmak Zordur	*K7*

Tablo 14'te sunulan verilere göre katılımcıların görüşme sorularına verdikleri cevaplar hassasiyet değerlendirmesi teması kapsamında iki kategori altında toplanmıştır. Bu kategorilerden ilki olan "değerlendirme yaklaşımı" katılımcıların hassas bilgi içerikli belgeleri değerlendirirken nasıl bir anlayış ve/veya yöntem ile bu işlemin uygulanacağına

dair görüşlerini içermektedir. İkinci kategori olan "fiziksel ve dijital değerlendirme", katılımcıların bilgi taşıyıcısının formatına göre sürece yönelik görüşlerini yansıtmaktadır.

V.6.5.1. Kategori: Değerlendirme Yaklaşımı

Değerlendirme yaklaşımı kategorisinde görüş beyan eden yedi katılımcı beş farklı görüş (Grafik 6) sunmuştur. Hassas bilgi içerikli belgeler değerlendirilirken hangi yaklaşım ile yapılacağı konusunda görüş beyan eden katılımcılar risk üzerine yoğunlaşmaktadır.



Grafik 6. Değerlendirme Yaklaşımı

K6, "*Yüksek riskli belgeler için ayrıntılı değerlendirmeleri saklayarak bir risk yönetimi yaklaşımı kullanıyoruz*" ifadeleri ile görev aldığım kurumda risk temelli bir yaklaşım sergilendiğini belirtmiştir. K7, "*Hassasiyet değerlendirmesi bir risk yönetimine dayalı bir yaklaşım olması gerekir*" ifadeleri ile risk yaklaşımını desteklemiştir.

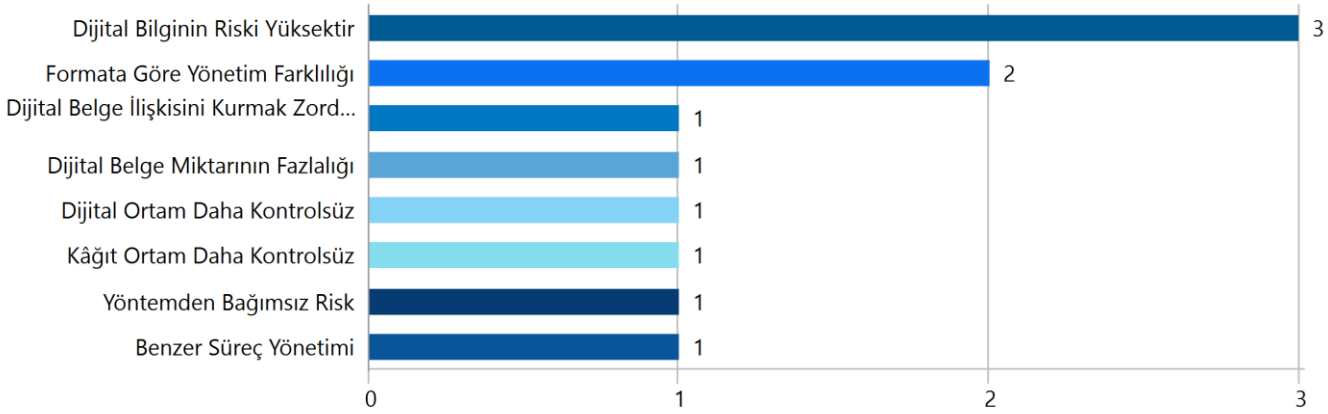
Bazı katılımcılar değerlendirme sürecinde üreten kurum ile iş birliğine gidilmesi gerektiğini belirtmektedir. K2, "*Hangi bilgiyi kamuya açıp açamayacağımızı bilmemiz gerekiyor. Kendi başımıza karar vermek istemeyiz; ideal olan, bilgiyi oluşturanların bu kararları mümkün olduğunca kendi risk iştahlarına ve bağlamlarına dayanarak almalarıdır*" ifadeleri ile üreten kurum ile iş birliği kurulmasına dikkat çekmiştir. K5, "*Yani bir içerik bir kurum için bir bilgi bir birim için ya da ne bileyim bir disiplin için çok önemlidir. Ama biz o veriyi anlamayabiliriz. Atıyorum bir mühendislik çizim. Geldi,*

işte çok hassas çizimler içeriyor. Ben mühendis değilim, nasıl anlayacağım ne kadar değerli olduğunu, hassasiyetini, derecesini" ifadeleri ile bu görüşe örnek sunarak destek vermiştir. Üreten kurum ile iş birliğine yönelik oluşan bir diğer görüş, belgelerin iki aşamalı olarak değerlendirilmesi gerektiğinin ifade edilmesidir. K1, "*Belge üretim aşamasında bunların çok ciddi olarak yetişmiş personel tarafından yapılması kayıt altına alınması gerektiğini düşünüyorum. Çünkü bir belge kurumda üretiliyor. İşte bize 20 yıl 30 yıl sonra geliyor. Biz burda tekrar bunları değerlendirmek durumunda kalıyoruz*" ifadeleri ile ilk değerlendirmenin önemine dikkat çekmiştir. K2, "*Daniel Kahneman'ın "Gürültü İnsan Yargısında Hata" kitabını okumuş biri olarak, bu tür son derece öznel karar verme süreçlerinde oldukça fazla "gürültü" olduğunu tahmin ediyorum. Bu da, neden ilk kararı verenin üstünde bir gözden geçiricinin bulunmasının önemli olduğunun sebeplerinden biri"* ifadesi ile iki aşamalı değerlendirmenin önemine örnek vererek dikkat çekmektedir. Bir diğer görüş hassas bilgi yönetimine dair kurum bazlı yönetim politikası belirlemeye yöneliktir. K8, "*Yetkili kişilere yetkilerin tanımlanması, erişmesi sağlanabilir. Böyle bir politika izlemeliyiz. Yani bir politika oluşturulabilir her kurum için. Bu hassas bilgileri, erişme, işte kimlerin… erişebilir veya kullanılabilir. Hani sadece bunu şimdi görebilir, paylaşabilir, yazdırabilir, silebilir. Bu yetkilerin de tanımlanması lazım. Yani yetkilendirmeler burada da hassas bilgi olduğu için hassasiyetle…, önem teşkil etmesi lazım. Ona göre hazırlanması gerektiğini düşünüyorum"* ifadeleri ile görüşünü beyan etmiştir. Değerlendirme yaklaşımına ilişkin bir diğer görüş bu sürecin mevzuat temelli olarak yapılması gerektiğini ifade etmektedir. K7, "*O ülkenin bu konudaki mevzuatı göz önünde bulundurmanız gerekir. Bu tabii ki belli bir şey. Mevzuatı göz önünde bulundurmanız gerekir*" ifadeleri ile mevzuata dayalı olarak değerlendirmenin yapılması gerektiğini belirtmektedir. K2, "*Elinizde büyük miktarda bilgi bulunuyor ve uyguladığınız süreç, ister makine yardımlı, ister manuel değerlendirmeler veya bunların bir kombinasyonu olsun, kusursuz olmayacak*" görüşü ile

format ve yöntem farketmeksizin sürecin mutlak risk içerdiğini ve hataların olacağına dikkat çekmektedir.

V.6.5.2. Kategori: Fiziksel ve Dijital Değerlendirme

Fiziksel ve Dijital Değerlendirme kategorisinde görüş beyan eden yedi katılımcı sekiz farklı görüş (Grafik 7) sunmuştur. Hassas bilgi içeren belgelerin değerlendirme bağlamında yönetimine ilişkin katılımcı görüşleri bilgi taşıyıcı ortamına yönelik olarak farklılık göstermektedir. Bazı katılımcılar dijital bilginin riskli olduğunu vurgulamıştır.



Grafik 7. Fiziksel ve Dijital Değerlendirme

K7, "*Dijital bilginin riski daha fazla. Mesela bir fiziksel bir dosyayı gözden geçirirsin ki ben… buna şahit oldum. Mesela gözden geçirilir, kamuoyuyla paylaşılır. Sonra iki hafta sonra bir itiraz olur, bir şey olur ya da bir kişi hala yaşadığı ortaya çıkıyor vesaire. O dosyayı kapatıyorsun tekrar. Ama dijital ortamda bunu nasıl yaparsın? Zaten kamuoyuyla paylaştığın zaman çoğu zaman nete düşüyor yani. Nete düşüyor bunu tekrar kapatmak yani kurumunu tekrar geri çekse bile yani bunu geri çekse bile kendi bünyesinde kapatmasa peki mesela bir arşiv diyelim ama bunu nette paylaşmış olabilir. Mesela ben bir vatandaş olarak Japonya'daki arkadaşıma maile göndermiş olabilirim o bilgiyi*" ifadeleri ile örnekler sunarak dijital bilginin daha riskli olduğunu belirtmektedir. K6, "*Dijital belgeler, bazen eski veya özel dosya formatlarında oldukları için erişim*

sorunları yaşayabilir; bu durum, kapsamlı bir değerlendirme yapmayı zorlaştırır. Ayrıca, dijital materyaller genellikle çok daha fazla miktarda gelir, bu nedenle risk yönetimi yaklaşımımıza daha fazla bağımlı kalıyoruz" ifadeleri ile K7'nin erişim kontrolü riskine karşın dijital bilginin formatından ve hacminden kaynaklanan risklerine işaret etmektedir.

K7, "*Yönetim açısından fark vardır, yani belge yönetimi açısından fark vardır, arşivsel süreçler açısından fark vardır*" görüşü ile bilgi taşıyıcı formatın farklılığının yönetim farklılığına sebep olacağını ifade etmektedir. K4, "*Bir oda dolusu belge ile bir hard disk dolusu belgenin incelenmesi aynı şeyde olmuyor. Bu anlamda kâğıt ve elektronik belgelerle ya da hassas bilgileri değerlendirirken belki işlem olarak aynı şey ama süre olarak farklılıklar olacağını düşünüyorum ben. Belgeye o da nüfus etme anlamında fiziki bir belgenin incelenmesiyle örnek veriyorum bir kurumu üreten birim o belgeyi A şehrinde üretmiştir. Ama arşiv olarak şu anda muhafazası B şehrinde yapılıyordur. Fiziki bir belgenin değerlendirilmesinde A şehrinden B şehrine gitme durumları varken ama elektronik bir belgede bunlar direkt sistem üzerinde aynı anda interaktif olarak bile incelenebileceği durumlar olabilir. Bu yüzden işlem olarak aynı olsa da vakit ve zaman olarak farklı olacağını düşünüyorum"* görüşü ile bu farklılıkları yer, zaman ve hız bağlamlarında değerlendirmektedir. K1, "*Elektronik belgelerle kâğıt ortamındaki belgelerin değerlendirme süreci aslında aynı olmalı diye düşünüyorum*" görüşü ile süreç yönetiminin ortamdan bağımsız olarak benzer ilerlediğini ifade etmektedir.

V.6.6. Tema: Değerlendirme Zorlukları ve Çözümler

"Hassasiyet değerlendirmesi sürecinde yaşanan zorluklar nelerdir? Bu zorluklar hangi yöntemler ile çözülebilir?" araştırma sorusunun cevaplanması amacıyla yöneltilen görüşme sorularına verilen cevaplar, kategori ve kodlar ayrılmıştır.

Tablo 15. Değerlendirme Zorlukları ve Çözümler Temasına Ait Kategori ve Kodlar

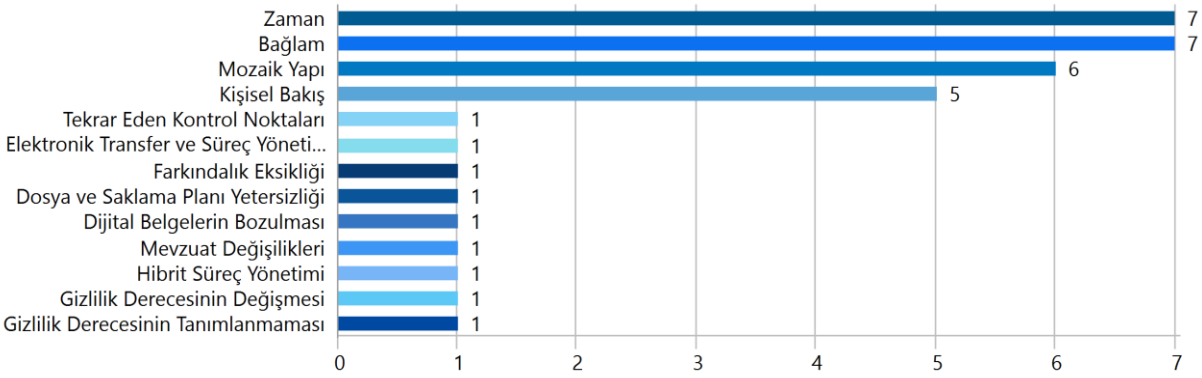
Kategori	Kodlar	Katılımcılar
Süreç Zorlukları	Bağlam	*K1, K2, K3, K4, K6, K7, K8*
	Zaman	*K1, K2, K3, K5, K6, K7*
	Kişisel Bakış	*K1, K2, K3, K4, K7*
	Mozaik Yapı	*K2, K3, K4, K6, K7*
	Gizlilik Derecesinin Tanımlanmaması	*K1, K8*
	Gizlilik Derecesinin Değişmesi	*K3*
	Hibrit Süreç Yönetimi	*K3*
	Mevzuat Değişilikleri	*K3*
	Dijital Belgelerin Bozulması	*K6*
	Dosya ve Saklama Planı Yetersizliği	*K1*
	Farkındalık Eksikliği	*K8*
	Elektronik Transfer ve Süreç Yönetimi	*K5*
	Tekrar Eden Kontrol Noktaları	*K1*
Objektifliği Sağlamaya Yönelik Çözümler	Mevzuat	*K2, K3, K4, K7, K8*
	Eğitim ve Bilgilendirme	*K1, K3, K8*
	Otomasyon	*K2*
	Görüş alışverişi	*K1*
	Görev tanımları ve talimatname	*K1*
Zamana Yönelik Çözümler	Erişime Kapatma	*K2*
	Periyodik Değerlendirme	*K1*
	Süreç Yönetimi	*K3*
	Belge Üretici Kurum Kararı	*K4*
Mozaik Yapıya İlişkin Çözümler	İlişki Kurma	*K1, K4, K8*
	Kurumlararası Koordinasyon	*K4*
	İş birlikçi değerlendirme	*K6*
Erişime Sunmaya Yönelik Çözümler	Anonimleştirme	*K1, K5, K8*
	Redaksiyon	*K2*
	Kamu Yararı	*K2, K7, K8*
	Kriptolu ve yetkilendirilmiş	*K8*

Tablo 15'te sunulan verilere göre katılımcıların görüşme sorularına verdikleri cevaplar değerlendirme zorlukları ve çözümler teması kapsamında beş kategoride toplanmıştır. Bu kategorilerden ilki hassasiyet değerlendirmesi sürecinde yaşanan/yaşanabilecek sorunları özetleyen kodlardan oluşmaktadır. Bu kategori en fazla kodun oluştuğu ve bütün katılımcılarin hassasiyet değerlendirmesi sürecinde tespit ettikleri sorunları/zorlukları içermektedir. İlk dört kod görüşme soruları içerisinde yer alan konular olması bakımından

doğal olarak oluşmuş ve en çok katılımın olduğu kodlardır. Ancak diğer kodlar katılımcıların çeşitli görüşlerini içermektedir. Bu anlamda çeşitlilik olarak en fazla dönüt K3 katılımcısından alınmıştır. Çözümleri içeren geriye kalan kategoriler, katılımcıların çoğunlukla çözüm ürettikleri sorunlara verdikleri yanıtlardan oluşmaktadır. Çözümlere ilişkin "Teknoloji Yardımlı Değerlendirme" teması altında yer alan "yapay zekâ" kategorisinin çeşitli çözümler üretebileceği görüşleri de yer almaktadır. Birden fazla katılımcının işaret etmesi, farklı temalar altında aynı kodun yer alamayacağı düşüncesi ile ilgili konuda kategoriye dönüştürülmüştür.

V.6.6.1. Kategori: Süreç Zorlukları

Süreç zorlukları kategorisinde görüş beyan eden tüm katılımcılar 13 farklı görüş (Grafik 8) sunmuştur. Bu sürece ilişkin hemen hemen tüm katılımcıların tespiti ve görüş olarak sunduğu zorluk "bağlam" meselesidir. Katılımcılar bu sürece ilişkin farklı örneklemeler sunarak düşüncelerini ifade etmişlerdir.



Grafik 8. Süreç Zorlukları

K1, "*Mesela Kore savaşını çalışıyoruz. Şimdi burdan ne beklersiniz siz? Kore savaşını baştan sona, bu savaşın başlaması işte başlangıcından önceki süreç, aldığınız uyguladığınız politikalar ürettiğiniz stratejiler, en nihayetinde oraya asker gönderiyoruz, orda cepheler, çatışmalar, esirler şu bu ve nihayetinde savaş bitiyor. Yani kore savaşını*

özellikle şundan dolayı söylüyorum çalıştığımız bir konu olduğu için. Şimdi burda belgeyi bir bütün olarak değerlendirdiğimizde savaşla ilgili şeyleri öğrenmek anlamak istiyorsunuz. Fakat öyle bir belge geçiyorki. Mesela bir alay komutanı uygunsuz birtakım davranışlar gördüğünü rapor ediyor. Yani aslında savaşın kendisi ile ilgili bir şey değil. Ama bağlam noktasında bağlamından kaynaklanan diyorsunuz ya şimdi öyle bir şey yazıyor ki ya da belge üretiyor ki şimdi bunu o savaşın bağlamından çıkartmak zorunda kalıyorsunuz" görüşleri ile bağlama dair oluşan zorluğu örnek bir vaka üzerinden açıklamıştır. K3, "*Aynı konu grubundan Millî Eğitim Bakanlığı tarafından çıkarılan bir belgeye bu belgeye hizmete özel gizlilik derecesi veya gizlilik derecesi verilmeyebilir. Fakat istihbarat birliklerinde çalışan, dış işlerinde çalışan, millî savunma bakanlığında çalışan kişiler personelin gizliliğini sağlamak adına bu belgeye daha farklı hassasiyetler verebiliyor"* görüşü ile bağlama ilişkin belgenin içerisinde yer aldığı fonun/kurumun hassasiyete etki edebileceğini ifade etmektedir. K7, "*Bağlam genelde siyasî, kültürel, sosyal, hani dinî faktörlere dayalı oluyor. Ama beni ilgilendiren kısım, bir uygulamacı olarak bunlardan ziyade… bu bilgi kırıntılarını ve birleştirdikten sonra kontekstin, bağlamının değiştiğini görmek. Ve değiştiğinde bir hassasiyetin ortaya çıktığını görmek*" görüşü ile bağlamın bilgi kırıntıları ile değişime açık zorluklar içeren bir konu olduğuna dikkat çekmektedir.

Bağlam ile ilişkili ve birbirine etki eden bir diğer mesele zamandır. Katılımcılar zaman zorluğuna ilişkin çeşitli örnekler ile görüşlerini beyan etmişlerdir. K5, "*Bugün hassas olan bilgi yarın olmayabilir ya da bugün hassas olmayan bilgi yarın hassas bilgi olabilir"* görüşü ile zamanın geçmişte veya gelecekte dinamik bir olgu olarak varlığını koruyacağını ifade etmektedir. Zaman zorluğunun bağlam ile olan ilişkisini kuran K2, "*Çok uzun süre boyunca hassas kalan şeyler çok ilginçtir. Örneğin, 1940'lar veya 1950'lerde atom bombası geliştirmeyle ilgili belgeler hâlâ inanılmaz derecede hassastır veya kimyasal ya da biyolojik silah geliştirmeyle ilgili belgeler bugün bile inanılmaz*

derecede hassastır. Uzun vadeli eğilim, zamanla hassasiyetin azalması yönündedir, ancak bağlamdaki değişikliklerin, önceden hassas olmayan şeyleri çok daha hassas hale getirebildiğini görebilirsiniz. Bu, belgede yer alan şeylerle ve belgenin daha geniş bağlamda nasıl oturduğuyla ve bu bağlamın nasıl değiştiğiyle ilgilidir. Yani, evet, hassasiyet kaybedilir ve kazanılır, genellikle kaybedilir ama bazı durumlar vardır" ifadeleri ile görüşlerini bildirmiştir. K7, "*Bazen 80'li yıllarından tarihi kalan dosyaları gözden geçirdiğimiz zaman hassasiyet açısından evlilik dışı ilişkiler, evlilik dışında birlikte yaşayan kişilerin bu ayrıntıyı kararlıyorduk bu ayrıntıyı. Çünkü bu özel hayata giriyor. Bu hala evet, özel hayata giriyor. Ama mesela İngiltere'de artık evlilik dışında, evlilik öncesi birlikte yaşamak bir norm haline gelmiş. Yani bir norm haline gelmiş ve bu ilerideki bu konudaki hassasiyet değerlendirmesini bu konuda etkileyebilir. Hani şöyle ayrıntı varsa tabii ki, nitelikli ayrıntı varsa bence tabii ki hala bu bilgi paylaşılmıyor, ileride de paylaşılmayacaktır. Ama diyelim ki 10 yıl öncesi, 10 sene sonra bir kamu belgesinde iki kişinin birlikte yaşadığını saf bir şekilde ayrıntı vermeden bir belgede geçiyorsa bence artık bu bilgi hassas olarak değerlendirilmeyecektir*" görüşleri ile bir topluma ait zamanla kaybolan hassasiyeti belirtmiştir. Ayrı bir sorun olarak da ifade edilebilen "mevzuat değişikliği" zaman ile doğrudan ilişkli bir zorluk olarak değerlendirilebilir. K3, bu durumu "*Kişisel verileri koruma kanunundan önce kişisel bilgileri içeren belgelere hassasiyetlik kazandırmıyorduk. Bu kanundan sonra KVKK kapsamındaki belgeler hassasiyetlik kazandı. Bu sebeple yeni yapılacak düzenlemeler veya yurttan kaldırılacak düzenlemeler belgelerin hassasiyetlik zamanını değiştirecektir*" görüşleri ile örnek üzerinden bir açıklama getirmiştir.

Hassasiyet değerlendirmesi değerlendiricilerin ideoloji ve entelektüel bakış açılarının istemsizce yer aldığı bir süreç olması bakımında objektifliği sağlamak zordur. Katılımcılar objektifliğin önünde bir engel olan bu zorluğa dair çeşitli görüşler sunmuştur. K7, "*Bazen insan kendi görüşleri, kendi siyasî ya da kültüre, sosyal hayatı ya da değerleri*

insanı daha az objektif kılabilir" ifadeleri ile objektiflik sağlamanın çeşitli yönlerden zorluklar içerebileceğini belirtmektedir. K3, "*Malumunuz, gizlilik derecelerine haiz arşivsel belgelerin araştırmaya açılması kapsamında ve yeniden gizlilik derecelerinin belirlenmesi kapsamında bir kurul oluşturuluyor. Birimlerin ilgili yetkilileri bu kurumun doğal üyesi. Bu yetkililer her zaman aynı kurumda çalışmıyor. 5 yıl sonra değerlendirmeye gelen kişi farklı bir yorumda bulunabilir*" görüşleri ile yönetici veya personel rotasyonları doğrultusunda yaşanabilecek değişikliklerin de kendine mahsus bir öznellik barındıracağını ifade etmektedir.

Belgenin ilgili olduğu bilgi veya belge ile olan ilişkisinden kaynaklanan zorluklar katılımcılar tarafından değerlendirilmiştir. K2, mozaik yapıdan kaynaklanan hassasiyeti "*Bir şeyi gizlemeye çalışıyorsam, bilgiyi saklamaya çalışıyorsam, ne kadar başka bilginin mevcut olduğunu ve bu bilgilerin gizlemeye çalıştığım şeyi hangi güven derecesiyle yeniden üretebileceğini bilmek*" olarak ifade etmektedir. K7, "*En büyük zorluk dijital ortamda farklı yerlerdeki saklanan, depolanan bilginin ilişkisini, arasındaki ilişkiyi kurmak zor ve ilişki kurduğunda da bunu hassasiyet açısından kavrayabilmek yani gerçekten daha zor"* görüşü ile bu ilişkinin dijital ortamda daha büyük problem olduğunu ifade etmektedir. K4, "*Basit bir gaz alım belgesi. Bunlar araştırmaya açılıyor. Araştırmaya açıldığı zaman normal araştırmacı buna bakıyor. Bunu araştırmaya açan … da sıradan bir temel ihale gibi, gaz alım belgesi gibi görünüyor. Ama araştırmacı bunu yıl itibariyle, Sabiha Gökçe'nin yaptığı hava faaliyetleriyle birleştirdiği zaman, bu belgeleri ilişkilendirdiği zaman farklı bir anlam ifade ediyor. Bu da işte idare olarak şeyde kalınabiliyor işte bak diyor o sene demek ki siz bunu yaptınız her sene 3 ton gaz alıyorsunuz bu sene 30 ton gaz almışsınız yıl bazlı bir belgeyi işte farklı bir faaliyette ilişkilendirip yapabiliyor. Bu gerçekten önemli bir konu. Ondan sonra idareye sorumluluğunda, cevap vermeye sorumluluğu da doğuyor işte"* örneği ile mozaik yapıya ilişkin tarihsel süreç içerisinde yaşanmış bir olayı aktarmaktadır. Her iki belge tekil olarak

değerlendirildiğinde hassasiyet içermese bile bu tür bağlantılar kurulduğundan özel bir durum ortaya çıkmaktadır.

Gizlilik derecelerinin belge üzerinde tanımlanması, sadece hassas bilgi içeren belgeler özelinde değil gizlilik içeriğine sahip belgeler için de gereklidir. Ancak içerikte yer alan bilginin hassasiyeti konusunda bilgi düzeyinin yeterli olmaması gizlilik derecesinin tanımlanmamasına sebebiyet vermektedir. K1, "M*esela işte öyle belgelerimiz var ki belgede aslında hiçbir gizlilik kaydı yok. Fakat ticarî sır niteliğinde bir şirketin bir kurumun bütün öz varlıkları ile ilgili ticarî sır sayılacak şeyler var ama belgede gizlilik kaydı yok. İşte şimdi bunu ancak biz tanımlama alanında kayıt altına alabiliriz"* görüşü ile gizlilik derecesinin tanımlanmaması zorluğuna işaret etmektedir. Bu durum bir başka katılımcının sorun olarak ifade ettiği "*Hassasiyet yani şu an ülkemizde tam anlamıyla kullanıldığını yani kurumların bunun farkında olduğunu çok düşünmüyorum. Yani tam olan kurumlar vardır, dikkat eden kurumlar vardır ama genel bir şey var"* (K8) farkındalık eksikliğinin bulunması ile ilgili olduğu düşünülmektedir. Gizlilik derecesinin tanımlanmaması konusunda "dosya ve saklama planları" doğrudan bir etkiye sahiptir. K1, "*Bizim standart dosya planımız, saklama planlarımız maalesef buna dönük bir şey yapmıyor. Yani hassas içerik veya belge bu konuda değerlendirilmelidir gibi böyle bir şey yok*" görüşü ile dosya ve saklama planlarında ilgili konuda alanların yer almadığı, uygulamadaki dokümanların yetersiz olduğu ifade etmektedir.

Birbiri ile ilişkin diğer zorluklar ise "gizlilik derecesinin değişmesi" ve buna bağlı olarak ortaya çıkan "hibrit süreç yönetimi" meseleleridir. K3, "*Yetkili kişi belgenin gizlilik derecesini değiştirdiğinde belgenin ortamı da değişiyor. Bu sebeple sorunlar ortaya çıkıyor"* görüşü ile gizlilik derecesi değişikliklerinin yönetsel sorunları beraberinde getiridiğini ifade etmektedir. K3, "*Malumunuz farklı hassasiyetlik derecesindeki belgeler farklı platformlarda ortamlarda yönetiliyor. Bu da iş yükünü*

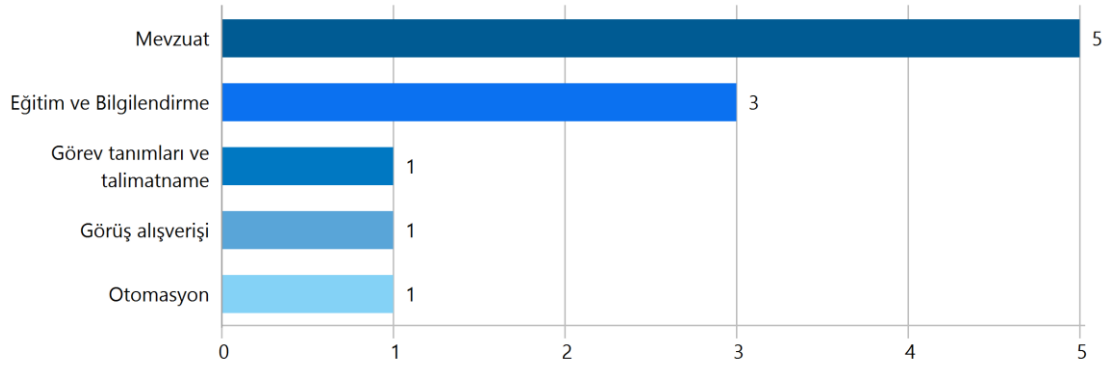
acayip bir şekilde artırıyor" görüşü ile farklı ortamlardaki yönetimin zorluğunu vurgulayarak gizlilik derecesi değişikliği hibrit yönetimi doğurduğunu vurgulamaktadır.

Katılımcılar tarafından ifade edilen bir diğer ilişkili zorluklar "Dijital Belgelerin Bozulması" ve "Elektronik Transfer ve Süreç Yönetimi" meseleleridir. K6, "*Dijital belgeler, bazen eski veya özel dosya formatlarında oldukları için erişim sorunları yaşayabilir*" görüşü ile sürece ilişkin erişim hususundaki zorluğa dikkat çekmektedir. K5, "*Fiziksel arşivde kâğıt veya diğer manyetik ortamdaki belgelerin saklanması biraz daha analog sistemler içeren bir yapı gerektirirken dijital içeriklerin korunması çok daha hassas. Uzun sürede dijital içeriği koruyamıyorsunuz. Burada sık sık veri göçü yaptırılmak zorunda. Şimdi biz arşiv olarak bu hassas veriyi değerlendirmekten ziyade verinin yönetimi konusunda nasıl bir sistem tasarlamalıyız? Bu verilerin yönetilmesi konusunda nasıl bir yapı kurgulamalıyız? Onun üzerinde durmamız lazım. Yani hassas veri bir kurumdan başka bir kuruma verilirken nasıl verilir? Hangi formatta verilir? Hangi kurallar çerçevesinde verilir? İşte erişim yetkileri, düzenleme yetkileri, bakma yetkileri, imha yetkileri falan vesaire bunlar nasıl belirlenir?"* görüşleri ile dijital içeriğin uzun süreli olarak korunması konusundaki sorunları açıklayarak hassas içeriğe sahip belgelerinn elektronik ortamdaki transfer ve yönetim süreçlerinin nasıl olması gerektiğine dair bir dizi soru/sorun belirtmektedir.

Bu kategoriye ilişkin ifade edilen son zorluk kontrol noktalarının döngüye girmesi üzerinedir. K1, "*Bir kontrol mekanizması geliştirip kendi içimizde tekrar bu belgelerin bir daha gözden geçirilmesi. Ama takdir edersinizki şimdi bir kontrol noktası oluşturuyorsunuz. Acaba doğru mu yaptı mı? Bir kontrol noktası daha. Acaba bir kontrol. Bunun sonu yok. Maalesef sonu yok"* görüşü ile değerlendirme sürecinde kontrol noktalarının sürekli olarak tekrarlamanın verimli bir yönetim olmayacağını ifade etmektedir. Önlem olarak çok fazla kontrol noktasının bulunması personel, zaman ve maliyet bakımından olumsuz bir etki oluşturacaktır.

V.6.6.2. Kategori: Objektifliği Sağlamaya Yönelik Çözümler

Objektifliği sağlamaya yönelik çözümler kategorisinde görüş beyan eden altı katılımcı beş farklı görüş (Grafik 9) sunmuştur. Hassasiyet değerlendirmesi sürecinde kişisel bakış objektifliğin önündeki en büyük engel olarak ifade edilmektedir. Daha önce katılımcıların bu durumu destekler nitelikte görüşlerine değinilmiştir. Bu konuda çözüm sunan katılımcılar objektif bir değerlendirmenin olabilmesi için sürecin ağırlıklı olarak "mevzuata" dayalı olarak ilerlemesi gerektiğini savunmaktadır.



Grafik 9. Objektifliği Sağlamaya Yönelik Çözümler

K4, "*Uygulama emri olabilir… kurumlarda yönetmelik olabilir, talimname olabilir. Herkesin o standartı sağlamak açısından idare tarafından koyulacak bir mevzuat. Ve dediğim gibi her zaman bu mevzuata ek yapılacak, güncelleme yapılabilecek bir maddeyi de içeren bir mevzuat*" görüşü ile güncellemelerin saklı tutulduğu bir mevzuata bağlı kalmanın objektifliği destekleyeceğini belirtmektedir. Benzer bir şekilde K3, "*Ulusal çapta nesnel ölçütler yerine kurumsal politikalarla belirlenen, yine temelinde yasal mevzuat bulunan nesnel ölçütlerin belirlenmesi gerektiğini düşünüyorum*" görüşü ile mevzuata dayalı olarak kurum bazlı nesnel ölçüt belirleme çalışmasını vurgulamaktadır. Mevzuat ile ilişkili bir unsur olarak "görev tanımları ve talimatname" hususu çözüm olarak sunulmuştur. K1, "*Bir görev tanımları yapıyoruz bir talimatname oluşturuyoruz onunla ilgili neye dikkat edilecek hangi unsurlar göz önünde bulundurulacak*" görüşü ile

objektifliğin sağlanabileceğini belirtmektedir. Mevzuat içerisinde bu tür görev tanımlarının olması, mevzuata dayalı talimatname ve işleyişin oluşturulması mümkündür.

Objektifliği sağlamaya yönelik bir diğer çözüm önerisi "eğitim ve bilgilendirme" faaliyeti olarak ifade edilmektedir. K3, "*Kurum genelinde bu konuda da eğitim verilmesi veya bilgilendirme yapılması lazım. Çünkü bu şekilde subjektifliği objektifliğe çevirebilirsiniz"* görüşünü sunmaktadır. K8 bu görüşü *"Objektiflik ve hassas bilgilerin konusunda eğitim verilmesi iyi olur"* ifadeleri ile desteklemektedir. Tek yönlü bir faaliyet olan bu uygulamanın yanı sıra K1, "*Birebir ikazlarımız, uyarılarımız, önerilerimiz, karşılıklı görüş alışverişlerimiz de olabiliyor. Tereddüt ettiğiniz konuları komisyona havale edelim, birlikte değerlendirelim gibi*" ifadeleri ile görüş alışverişi" yolu ile objektifliğin sağlanabileceği belirtilmektedir.

Sürecin mekanikleşmesi adına insan faktörünün azaltılarak "otomasyon" yazılımlarının kullanılmasının objektifliği arttıracağı görüşü de bulunmaktadır. K2, "*Otomasyonun arttırılması da bazı işlemleri daha otomatik hale getirmede kesinlikle faydalı olacaktır*" ifadesi ile otomasyonu çözüm olarak sunmaktadır.

V.6.6.3. Kategori: Zamana Yönelik Çözümler

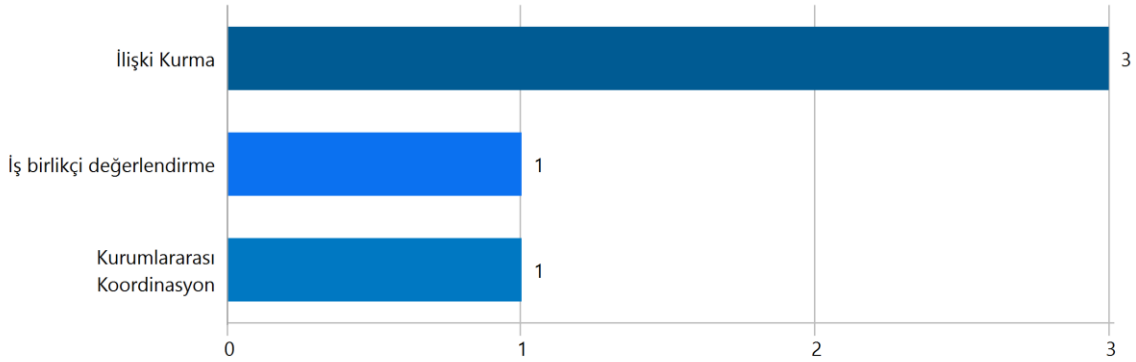
Zaman, hassasiyet değerlendirmesi sürecinde karşılaşılan başlıca zorluklardandır. Bu konuda görüş beyan eden dört katılımcı dört farklı görüş (Grafik 10) sunmuştur.

Grafik 10. Zamana Yönelik Çözümler

K2, "*Bizim yayından kaldırma hakkı gibi çözümlerimiz var; bir şeyi yayınlarız ve sonra yayından kaldırırız. Belki de başka çözümlere ihtiyacımız var*" ifadeleri ile erişime kapatma gibi kısmî bir çözümü belirtmiştir. Ancak kapatma kararının çözüm noktasında yeterli olmadığını ifade etmiştir. Özellikle dijital çağda bu çözümün işlevini yerine getirmesi mümkün görünmemektedir. Belge üretici kurumun zaman konusunda süre belirlemesi gerektiğini ifade eden K4, "*Arşiv faaliyetlerinde cari yıl sonundaki ayıklama ve imhaya tabi tutan kişilerin de belgeye üretim makamı olduğu için onların bu konuda zaman konusunda her belgeye ayrı ayrı bir şey yapmasına süre biçmesi konusunda yani belki bu bir çözüm olabilir"* görüşü ile çözüm sunmuştur. Benzer bir şekilde K1, "*Periyodik olarak bunları tekrar değerlendirmeye alacağımızı bir kayıt altına alabilirsek belki zamanla üstesinden gelebiliriz*" görüşü ile tekrar değerlendirilme tarihinin kurum tarafından kayıt altına alınmasını sağlayarak "periyodik değerlendirme" çözümünü geliştirmiştir. Sunulan çözüm K4'ün belirttiği her belge özelinde ayrı ayrı süre biçme görüşü ile örtüşmektedir. Son olarak bu konuya ilişkin K3, "*Prosedürlerle belirlenen, süreç tabanlı belirlenen nesnel ölçütlerin, yaşayan nesnel ölçütlerin bu sorunu çözeceğini düşünüyorum*" görüşü ile "süreç yönetimi" yaklaşımını önermektedir.

V.6.6.4. Kategori: Mozaik Yapıya İlişkin Çözümler

Mozaik yapıya ilişkin çözümler kategorisi katılımcıların en az katkı sağladığı kategoridir. Bu kategoride görüş beyan eden dört katılımcı üç farklı görüş (Grafik 11) sunmuştur. Mozaik yapı hassasiyet değerlendirmesi sürecinde çözülmesi en zor konulardandır. Katılımcılar bu konuda çeşitli çözümler önerileri geliştirmiştir.



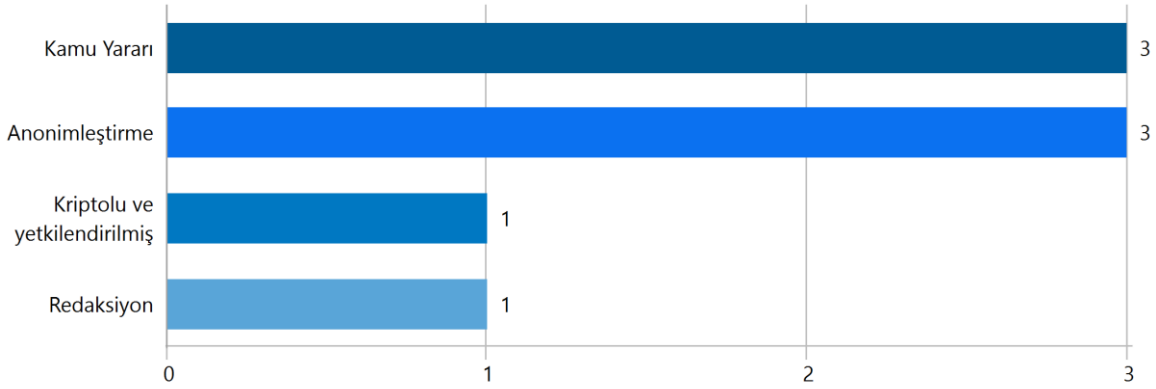
Grafik 11. Mozaik Yapıya İlişkin Çözümler

K1, "*Müstakil olarak bağımsız olarak bir belgeyi her zaman değerlendirme şansımız yok onun başka kurum, kamu belgeleri özellikle başka kurumların başka birimlerin belgelerinin de o anlamda bu ilişkisini kurarak değerlendirme yapmamız gerekiyor. Bunun çözümü olarak şimdiye kadar sadece hani biz tanımlama alanları ile belki bunları klasik kataloglama anlamından çıkararak yani belgelerin birbirleri ile olan ilişkilerini de değerlendirerek yeni bir kataloglama anlayışı geliştirmeye çalışıyoruz"* görüşü ile çözümü belgenin ilişkilerine odaklanan yeni bir kataloglama anlayışı olarak ifade etmektedir. Benzer bir şekilde K8, "*Verilerin ilişki kümesi yapılarak bunlar bir analiz havuzunda belirlenir*" görüşü ile ilişki kurmanın önemine dikkat çekmiştir.

K4, ayrıca çözüm olarak "*Belgenin sahibi kurumda koordineli olarak çalışılması gerektiği yönünü düşünüyorum alınabilecek önlemler kapsamında*" görüşleri ile kurumlararası koordinasyona dikkat çekmektedir. Benzer bir koordinasyonun iş birlikçi değerlendirme yaklaşımı ile çözüleceğini K6 "*Hassasiyet değerlendirmesi sırasında, bireylerin gözden geçirdiği içerikle ilgili sıkça tartışmalar yapılması son derece önemlidir; böylece mozaik hassasiyetlerin kolektif olarak tanımlanması için çok sayıda fırsat sağlanmış olur*" ifadeleri ile belirtmektedir.

V.6.6.5. Kategori: Erişime Sunmaya Yönelik Çözümler

Belgelerin hassas bilgi içermesi tam olarak erişime kapatılması anlamına gelmemektedir. Bu kapsamda erişime sunmaya yönelik çözümler kategorisinde görüş beyan eden beş katılımcı dört farklı görüş (Grafik 12) sunmuştur.



Grafik 12. Erişime Sunmaya Yönelik Çözümler

K5, "*Bilgiyi anonimleştirecek hale getirecek teknikler düşünülebilir*" önerisinde bulunmuştur. K1, bu öneriye dair "*Mesela bir 400 sayfalık bir belge grubu okuyoruz. Bir müfettişin bir bölge ile raporu. Şimdi orda 400 sayfanın içerisine sadece bir cümlede kişileri rencide edebilecek işte olumsuz sonuçlar çıkarabilecek bir ifade var. Ve bu ifadeden dolayı 400 sayfalık bir belgeyi gizlemek zorunda kalıyorum. Halbuki anonimleştirebilirsek bunu yani o satırı karartabilirsek ve bunu da belirtirsek. Yani anonimleştirilmiştir şu satırı diye diğer belgelerin de kamuoyuna açıklanmasında hiçbir sakınca olacağını düşünmüyorum*" görüşü ile anonimleştirmenin özellikle büyük hacimli belgeler için erişime sunmanın önünü açabileceğini örnek ile ifade etmektedir. Benzer bir şekilde K2, "*Bilgi Edinme Yasası kapsamında bu bilgileri isteyen biri olduğunda, bu bilgileri yoğun bir şekilde redakte ederek talebe yanıt verebilir ya da arşive teslim etmeden önce aynı şekilde redakte edebilirsiniz"* ifadesi ile bilgi edinme talepleri bağlamında redaksiyon çözümünü sunmaktadır. Belge/metin üzerinde bilgilerin çeşitli teknikler ile kapatılmasına yardımcı olan bu teknikler aynı amacı taşımaktadır. Erişim hususunda bir diğer yöntem kriptolu ve yetkilendirilmiş erişimdir. K8 bu görüşü "*Dijital*

ortamda bunlar kriptolanarak ve erişim yetkisi olarak şifrelenerek erişilmesi lazım… fiziksel ortamda hani yetkililik kılınan yer ya da özel bir dolap veya yerde bir odada saklanması gerekiyor yani bunların da. Aradaki fark bu yine ikisine de erişim yetkisi" olarak ifade etmektedir. Sunulan öneriler hassasiyet içeren belgelerin erişimine ilişkin yöntemler olarak ifade edilebilir. Bununla birlikte esasında hassas olarak nitelendirilebilen ancak "kamu yararı" bulunan bilgiler de var olmaktadır. Bu konuda K7, "*Bu bilgi kamuoyuyla paylaşılırsa bu dosya içerisinde, bu arşiv belgesi içerisinde, bu kamuoyun yararına mıdır, bu kamuoyun yararına değil midir? Hani bunu sürekli, bu bizim gündemimizdeydi çünkü bu mevzuatta var. Hani kamunun yüksek yararına. Mesela şöyle bir şey, mesela diyelim ki bir memurun bir bilgi edinme hakkı talebi geldi. İşte X kurumda çalışan X kişinin maaşını öğrenmek istiyorum diye bir bilgi edinme hakkı talebi geldiği zaman bu bilgi paylaşılmıyor. Neden? Çünkü o kişinin maaşı, tam olarak aldığı maaşı onun nitelikli kişisel verisi olarak sayılıyor. Ancak birisi, bir vatandaş, bir milletvekilinin hangi ülkede olursa olsun, yani bu fark etmiyor ve İngiltere'de bu çok yaşandı, çok örnekleri var. Mesela bir milletvekilinin, X milletvekilinin geliri nedir? Şimdi bir milletvekili de sonuçta çalışan bir insan ama kamu yararını düşündüğünüz zaman halkın, kamunun hakkı var milletvekilinin ne kadar kazandığını öğrenmesi için*" ifadeleri ile hassas bilgi içeren belgeleri erişime sunma konusunda kamu yararını çözüm olarak belirtmektedir. Konuyu kamu soruşturması bağlamında değerlendiren K2, "*Pandemi sırasındaki karar alma belgelerini siyasî olarak hassas bilgi olarak değerlendirebilirsiniz… Ancak, devlet o olaylara ilişkin açık bir kamu soruşturması yapma kararı alırsa ve bu soruşturma yasal yetkilerini kullanarak departmandan bilgi talep ederse, aynı belgeler kamu yararına açıklanabilir*" ifadeleri ile kamu yararının erişime sunma hususundaki önemini belirtmektedir.

V.6.7. Tema: Teknoloji Yardımlı Değerlendirme

"Dijital hassasiyet değerlendirmesi nedir? Dijital araçların/yazılımların hassasiyet değerlendirmesi sürecinde fonksiyonları/katkıları nelerdir? Bu araçlar hassasiyet değerlendirme sürecinde kullanılmalı mıdır?" araştırma sorusunun cevaplanması amacıyla yöneltilen görüşme sorularına verilen cevaplar, kategori ve kodlar ayrılmıştır.

Tablo 16. Teknoloji Yardımlı Değerlendirme Temasına Ait Kategori ve Kodlar

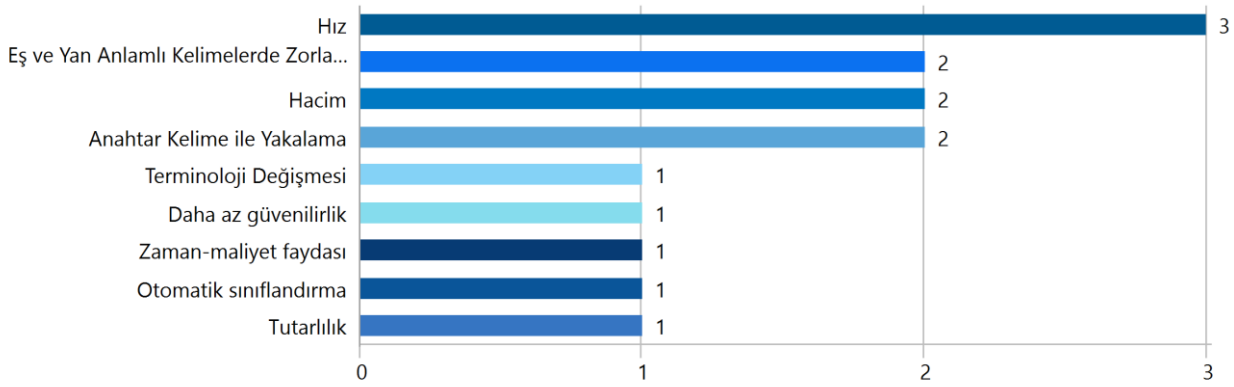
Kategori	Kodlar	Katılımcılar
Yardımcı Araçların Rolü	Anahtar Kelime ile Yakalama	*K4, K6*
	Hız	*K1, K2, K8*
	Tutarlılık	*K2*
	Hacim	*K2*
	Otomatik sınıflandırma	*K8*
	Zaman-maliyet faydası	*K8*
	Daha az güvenilirlik	*K1*
	Eş ve Yan Anlamlı Kelimelerde Zorlanır	*K4, K6*
	Terminoloji Değişmesi	*K7*
Yapay Zekâ	Bağlam tespiti	*K5, K8*
	Zamana karşı duyarlı	*K4, K7, K8*
	Objektiflik	*K1, K5*
	Otonom işlemler	*K2, K5*
	Öğrenebilir Olmalıdır	*K5*
Otonom Değerlendirme	İnsana Bağlı	*K1, K2, K3 K4, K5, K7, K8*
	Merkezî Kural Tabanlı	*K5*
	Yaşam Deneyimi, Sezgi ve Empati	*K2, K3*
	Doğrulanmalı	*K4*
Bilgi Edinme Hakkı Talebi	Gereklilik	*K2, K8*
	Süreci hızlandırır	*K1, K4, K5, K7 K8*
	İnsan eliyle etiketleme işlemi yapıldıktan sonra	*K3*
Hukukî, Teknik ve Etik Problemler	Kurum sorumlu	*K1*
	Kural setlerine bağlı	*K5*
	Hukukî sorumluluk belirsizdir	*K3*
	Sözleşmeye bağlı	*K4, K5, K6*
	Yerli Yazılım	*K8*

Tablo 16'da sunulan verilere göre katılımcıların görüşme sorularına verdikleri cevaplar teknoloji yardımlı değerlendirme teması kapsamında beş kategori altında toplanmıştır. İlk

kategoride hassasiyet değerlendirmesi sürecinde yardımcı araçların rolü ele alınmaktadır. Bu kategoride oluşan ilk altı kod yardımcı araçların pozitif yönlerini son üç kod negatif yönlerini ifade etmektedir. İkinci kategoride pek çok farklı zorluğa yönelik çözüm geliştirdiği ifade edilen yapay zekâ teknolojisini içermektedir. Özellikle bir önceki tema olan "Değerlendirme Zorlukları ve Çözümler" teması altında yer alan konulara dair çözümler bulunmaktadır. Üçüncü kategori genellikle yapay zekâ kullanılarak mümkün olan otonom işlem kabiliyetine yönelik katılımcı cevaplarından oluşmaktadır. Dördüncü kategori yardımcı araçların bilgi edinme hakkı talepleri noktasındaki rolüne ilişkin katılımcı görüşlerini içermektedir. Son olarak beşinci kategori değerlendirme sürecinde kullanılan/kullanılacak yardımcı araçların oluşturabileceği hukukî, teknik ve etik problemlere odaklanmaktadır. Bu kategoride katılımcılar hukukî sorumluluk bağlamında birbirinden farklı yaklaşımlar göstermektedir.

V.6.7.1. Kategori: Yardımcı Araçların Rolü

Yardımcı araçların rolü kategorisinde görüş beyan eden altı katılımcı dokuz farklı görüş (Grafik 13) sunmuştur. Yardımcı araçların rolüne ilişkin katılımcılar tarafından pozitif ve negatif görüşler alınmıştır.



Grafik 13. Yardımcı Araçların Rolü

K4, özellikle dijital ortamda olan belgelerin metin yapısının sunmuş olduğu kolaylıktan dolayı "*Belirli anahtar kelimelerle falan belge hassasiyetleri yakalanabilir*" görüşü ile yardımcı araçların kelime odaklı hassasiyet tespiti yapabileceğini vurgulamaktadır. Kelime tespiti ile birlikte K8, "*Otomatik araçlar belgeleri hassasiyet düzeylerine göre sınıflandırdığında daha hızlı konuşulabilir. İşte hassas bilgi tespiti, otomatik raporlama, izleme mekanizmaları filan bunlar daha iyi kontrol ve kısa sürede erişimleri sağlar*" görüşü ile otomatik sınıflandırmanın süreci hızlandırabileceğini belirtmektedir. Yardımcı araçların etkili olduğu düşünülen unsurların başında "hız" gelmektedir. K2, "*Otomasyon kullanımı… süreci hızlandırabilir*" görüşü ile el yordamına karşılık yardımcı araçların hız kazandırabileceğini belirtmektedir. Hız kazanma konusunda K8, "*Otomatik araçlar manuel veya fiziksel süreçlerin azaltılmasıyla zamanın ve kaynakların daha etkili ve verimli şekilde kullanmasını sağlar. Bu da maliyetlerin düşmesine etkili olur*" görüşü ile hızlı işlem sürecinin zaman-maliyet faydası sunacağını ifade etmektedir.

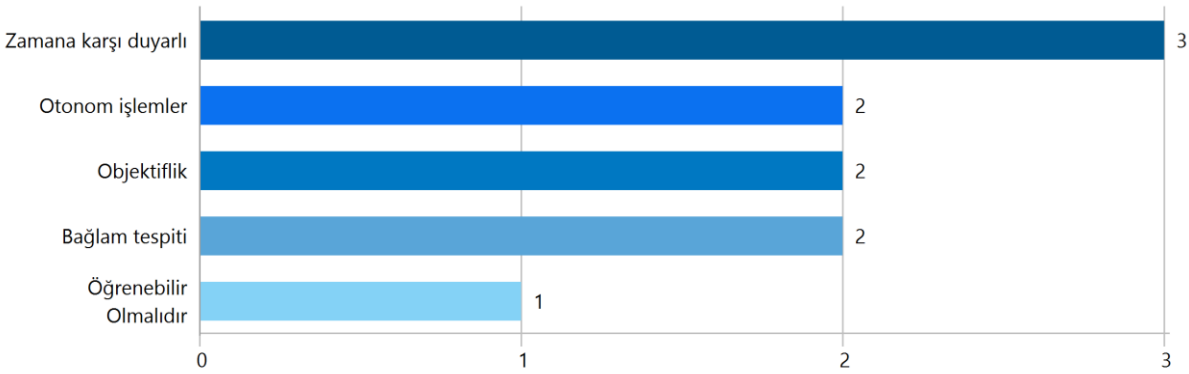
K2, yardımcı araçlara dair "*Daha objektif verilere dayanan durumlarda tutarlılığı sağlamak çok daha kolaydır. Özellikle otomatik araçlardan yararlandığınızda bu avantajı elde edersiniz. Örneğin, isim tanıma gibi araçlar sayesinde bu süreçte çok daha tutarlı sonuçlar elde edilebilir"* görüşü ile tutarlılık; "*Hükümet departmanları, dijital yığın dediğimiz çok büyük miktarda bilgi biriktirdiler ve bu bilgi hacmi, artık insan gücüyle oturup tek tek incelenemeyecek kadar fazla. Bu nedenle, süreçleri ölçeklendirebilmek için otomasyona ve otomatik araçlara başvurmamız gerekiyor*" görüşü ile hacim konusundaki pozitif katkıları ifade etmiştir.

Yardımcı araçların negatif rolüne ilişkin K1, "*Bir şahsın bireysel olarak değerlendirmesiyle bir yazılımın bunu değerlendirmesi arasında fark olur mu diye bir şey soracak olursan ben kendi kendime belki birbirlerine yakın olabilir. Ama burada insan unsurunun daha önemli ve güvenilir olduğu kanaatindeyim*" görüşü ile yardımcı araçların katkı olarak insan düzeyinde bir işlevi olsa bile daha az güvenilir olduklarını ifade

etmektedir. Bir diğer zorluk yardımcı araçların eş ve yan anlamlı kelimelerde zorluk yaşamasından kaynaklanmaktadır. Bu durumu K4, "*Bomba kelimesine anahtar kelime aldım ben. Şimdi bomba kelimesi patlayıcı olarak kullanıldığı zaman tamam, uygun. Ama örnek veriyorum, Deniz Kuvvetleri'ndeki bir erin gittiği limanda, Ukrayna Limanı'ndaki seyirinde müsaade edilen serbest zamanda bir kız görüyor. Arkadaşına bir mektup yazıyor, işte bomba gibi bir kız. Ya da işte İzmir Limanı'nda İzmir bombası yedik şeklinde bir belge var, arkadaşına anlattığı bir belge var. İşte bugün İzmir bombasını deneyimledim, çok güzel bir lezzet olduğunu anladım şeklinde*" görüşü ile yerel kullanım anlamlarına sahip ve çeşitli manalara gelen bir kelime üzerinden açıklamıştır. K6, "*Kelimelerin çeşitli anlamları vardır ve birçok yanlış pozitif sonuç alabilirsiniz; örneğin, "Aids" (virüs) ile "Aids" (fiil) arasındaki fark*" görüşü ile bu durum destekler nitelikte bir örnek sunmaktadır. Dil ve kelime odaklı negatif görüşlerden bir diğeri de belirli konulardaki terminoloji değişimidir. Bu konuyu K7, "*Mesela teknoloji kullanabilirsin ama o tek yazılıma belli terimler işlememişseniz o zaman onları tespit edemez. Mesela cinsel suçlarla alakalı olan terminoloji çok değişti. Mesela son 50-60 yıldır İngiltere'de. Bu konulardaki dosyalarda teknoloji kullanılacaksa eğer bunların da işlenmesi gerekir, kodlanması gerekir yazılıma. Yoksa çok büyük etik ve tabii ki hukukî sorunlar olur*" görüşü ile açıklamıştır. Kullanılacak yardım aracın/yazılımın bu tür kelimelere duyarlı olarak geliştirilmemesi pozitif-negatif sonuçlara doğrudan etki edeceğinden sorun olarak değerlendirilmektedir.

V.6.7.2. Kategori: Yapay Zekâ

Yapay Zekâ kategorisinde görüş beyan eden altı katılımcı beş farklı görüş (Grafik 14) sunmuştur. Katılımcılar, hassasiyet değerlendirmesi sürecindeki pek çok soruna yönelik olarak yapay zekâ çözümünü öne sürmektedir.



Grafik 14. Yapay Zekâ

K8, "*Yapay zekâ sistemleriyle düzenli olarak bunların gözden geçirilmesi*" görüşü ile; K7, "*Teknoloji destekli yapay zekâ hassasiyet değerlendirme araçları kullanıldığında bu yazılımlar geliştirildiğinde zaman faktörün bu yazılımlara işlenmesi gerekiyor*" görüşü ile yapay zekânın belgelerin değerlendirme sürecinde "zaman" odaklı olarak tekrar değerlendirme rolünü üstlenebileceğini ifade etmektedir.

K5 yapay zekânın bağlam[72] sorununa yönelik olarak üstleneceği sorumluluğu "*İçerikten ve bağlamdan bir hassasiyet değerlendirmesi yapmak istiyorsanız bu konuda yapılmış bir çalışmayı yapay zekâya verip öğretmeniz lazım. Yapay zekâ o yapılandırılmış veriden öğrenir. Kendi modelini bulur. Daha sonradan yeni döküman verdiğinizde onu değerlendirmesini sizin bakış açınıza göre yapar. Yani şimdi bu hassas verilerin hassas veri zaten dediğim gibi bu bağlamdan olur. Kişi, zaman, içerik, konu birebir ilişkili"* görüşü ile ifade etmektedir. K8, "*Yapay zekâ ile… bağlamına göre hassasiyet durumları belirlenebilir. Düşükten yükseğe göre sınıflandırma olabilir. Seviye ona göre arttırıp düşürmesi lazım olabilir*" görüşü ile bağlama karşı yapay zekânın rolünü desteklemektedir.

K5, "*Yapay zekâ da hassas bilgiyi tanıyan bir model eğitilebilir. Bu yapay zekâ ile analiz edilerek bu bilginin hassas olup olmadığı %100 objektif değerlendirilebilir*"

[72] Yapay zekânın bağlama bağlı hassas verileri tanımlama konusunda yardımcı olabileceği görüşü Jaillant (2022a) tarafından da ifade edilmektedir.

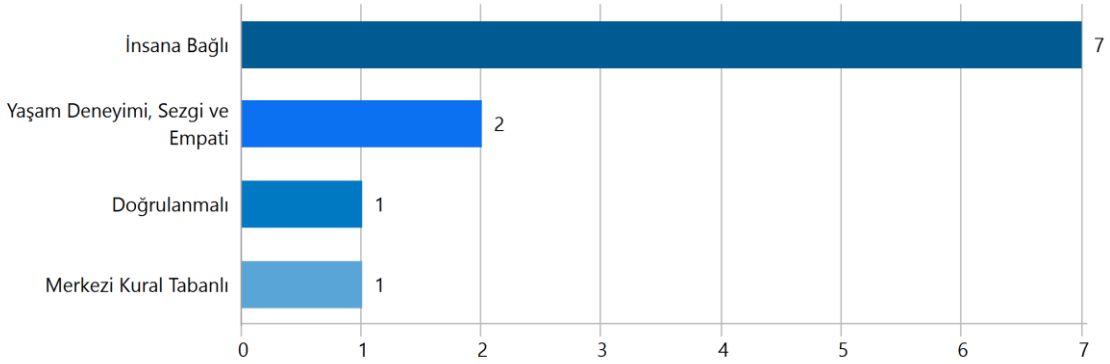
görüşü ile objektif değerlendirme işleminin yapay zekâ ile mümkün olabileceğini ifade etmektedir. K1, "*Hassas içerik veya hassas değerlendirme noktasında ek ilave yazılımların bize ciddi katkılar sağlayacağını yani kişisel ya da şahsi değerlendirmelerin belki biraz daha üstüne çıkarak yapay zekânın bize katkı sağlayacağına inanıyoruz"* ifadeleri ile yapay zekânın kişisel/şahsi değerlendirmelerin üzerinde objektif bir işlev sunacağını belirtmektedir.

Yapay zekânın otonom işlem sunma kabiliyeti konusunda K5, "*İşin en büyük yardımcısı muhtemelen yapay zekâ olacaktır. Yani siz bugün yapay zekâ ile analiz ettiğiniz de dokümanları bir iki tane prompt yazıp ya da bir kural belirleyip dersiniz ki bundan sonra bu tür belgeler yani içeriğinde şu şu şu ifadeler geçen belgeler benim için hassas belgelerdir dersiniz. Yapay zekâ tak sizin arşivinizdeki bütün belgeleri analiz eder… Veri setleriyle sürekli bu yapay zekâyı her gün eğitmek gerekir. Ya da onun dışında sürekli prompt yazmalıyız. Ama %100 otonom olmuyor bu süreçte. İşimizi %80-%90 belki kolaylaştırır, hız kazandırır, doğruluğu kazandırır ve objektifliği sağlar"* görüşü ile hassasiyet değerlendirmesi sürecinin tamamında olmasa da büyük ölçüde otonomlaşabileceğini ifade etmektedir.

Yapay zekânın sunacağı çeşitli çözümlerin yanı sıra kendi kendini eğitebilen "öğrenebilen" bir alt yapıyaya sahip olması gerektiğini K5, "*Şimdi yapay zekâyı eğitip modeli dondurduğunuz anda eğittiğiniz andaki kurallar geçerlidir. Yani modeli aldığınız dışarı çıkarttığınız andaki kurallar geçerlidir. Ondan sonra yeni bir kural ekleme veya çıkarma yaptığınızda yapay zekâ buna cevap vermez. Bu sefer işin içine öğrenebilir sistemler girer. Öğrenebilir sistemlerin girebilmesi için de bu yapay zekâ ile ilgili değerlendirilen verilerin daha sonradan bir belli kişiler tarafından tekrar değerlendirilerek ya da değerlendirilmeyen veriler tekrar değerlendirilerek eğitim veri setine yeni veriler atılır*" görüşü ile ifade etmektedir.

V.6.7.3. Kategori: Otonom Değerlendirme

Otonom değerlendirme kategorisinde görüş beyan eden yedi katılımcı dört farklı görüş (Grafik 15) sunmuştur. Hemen hemen tüm katılımcılar %100 otonom işlem kabiliyetinin mümkün olmadığını ve sürecin "insana bağlı" olduğu görüşünü savunmaktadır.



Grafik 15. Otonom Değerlendirme

K5, "*Kuralları siz sisteme verirsiniz sistem bu kurallar çerçevesinde işlem yapar. Dolayısıyla %100 otonomlu bir şeyden bu sistemde bahsedemeyiz*" görüşü ile yapay zekâ ve türev yardımcı araçların kurallar çerçevesinde ilerdiğinden otonomlaşmanın mutlak surette olmayacağını ifade etmektedir. K7, "*Hassasiyet değerlendirme konusunda teknoloji uygulandığında ama şöyle bu teknoloji kullanılsa bile yine de mutlak kararının bir kişinin, bir uzmanın vermesi gerekmektedir*" görüşü ile uzman denetimi ile kontrolün sağlanması gerektiğini bu sebepten ötürü tam otonom bir işlemin olmayacağını belirtmektedir. K2, "*Benim tahminim, insanların ve toplumların yaşamlarını etkileyen her türlü karar verme sürecinde yasal bir gereklilik olarak insanın döngü içinde bulunması gerektiğini görmeye devam edeceğiz. Toplumlar ve topluluklar da bunu etik açıdan talep edecektir*" görüşü ile hassasiyet değerlendirmesi başta olmak üzere insanı ilgilendiren ve doğrudan bir etkiye sahip durumlarda mutlaka süreç içerisinde insan faktörünün yer alması gerektiğini ifade etmektedir.

Otonomlaştırma konusunda K3, "*Değerlendirme araçlarının insan deneyiminden ve sezgisinden yoksun olması sebebiyle hassasiyetlik derecesi belirleme kapsamında bu*

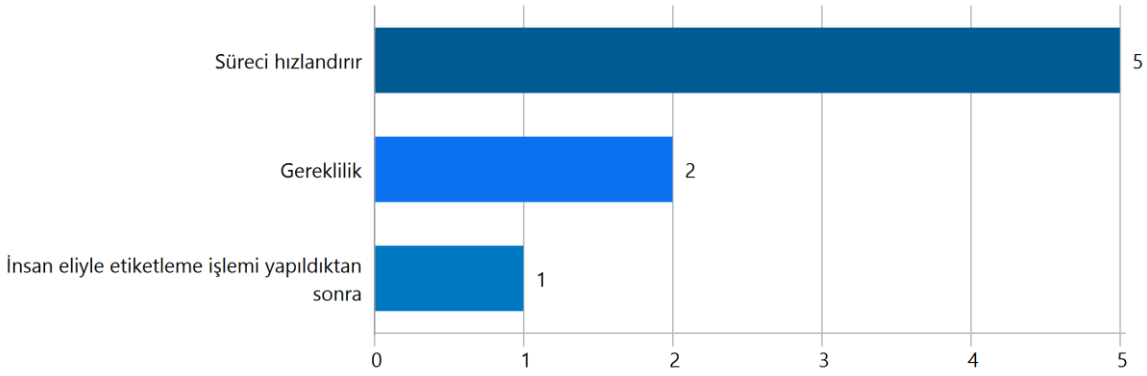
işlerin tam olarak bu araçlara bırakılmaması gerektiğini düşünüyorum" görüşü ile; K2, "*İnsanların en büyük gücü, sahip olduğumuz yaşam deneyimimiz ve empati yeteneğimizdir; bir insan olarak başka birine ne tür bir etkisi olabileceğini anlamamızdır. Tamamen otomatikleştirilmiş bir sistemde bu tür bir yetenek bulunmaz*" görüşü ile "yaşam deneyimi, sezgi ve empati" unsurlarına dikkat çekmektedir.

K5, "*Merkezî bir uygulama, daha doğrusu merkezde bir kurallar tanımlanacak. Bu kurallara erişen bir uygulama olacak. Bu uygulama gidip o kuralları merkezden çekecek. Daha sonra oluşturulan her belgeyi bu kurallar çerçevesinde analiz edecek. Ondan sonra da bu belgeye bir hassaslık derecesi verecek. Atıyorum 1 ile 10 arasında. 1 hassas belge içermez. 10 çok hassas belgedir*" görüşü ile otonomlaştırma konusunda merkezî bir kural tabanlı sistem önerisinde bulunmuştur.

K4, otonomlaşma konusunda "*Doğrulamaya ihtiyaç var*" görüşü ile mevcut teknolojinin henüz mutlak otonom işlem kabiliyetine sahip olmadığını, teyit edilmesi gerektiğini ifade etmektedir.

V.6.7.4. Kategori: Bilgi Edinme Hakkı Talebi

Bilgi edinme hakkı talebi kategorisinde görüş beyan eden yedi katılımcı üç farklı görüş (Grafik 16) sunmuştur. Demokratik, hesap verebilir, şeffaf toplumlarda bilgi edinme hakkı kapsamında vatandaşlar kamu kurumlarına başvuruda bulunmaktadır. Bilgi edinme taleplerinde hassasiyet değerlendirmesi gerekebileceğinden yardımcı araçların bu süreçlerde kullanımı ile ilgili katılımcılar tarafından farklı görüşler alınmıştır.



Grafik 16. Bilgi Edinme Hakkı Talebi

K2, "*Bunun gerekli olduğunu düşünüyorum ve bilgisayarların iyi olduğu konularda, daha tutarlı olacaklar ve kararların daha tutarlı bir şekilde uygulanmasına yardımcı olacaklar*" görüşü ile bilgi edinme hakkı taleplerinde yardımcı araçların gerekliliğine vurgu yaparak tutarlı sonuçlar verebileceğini ifade etmektedir.

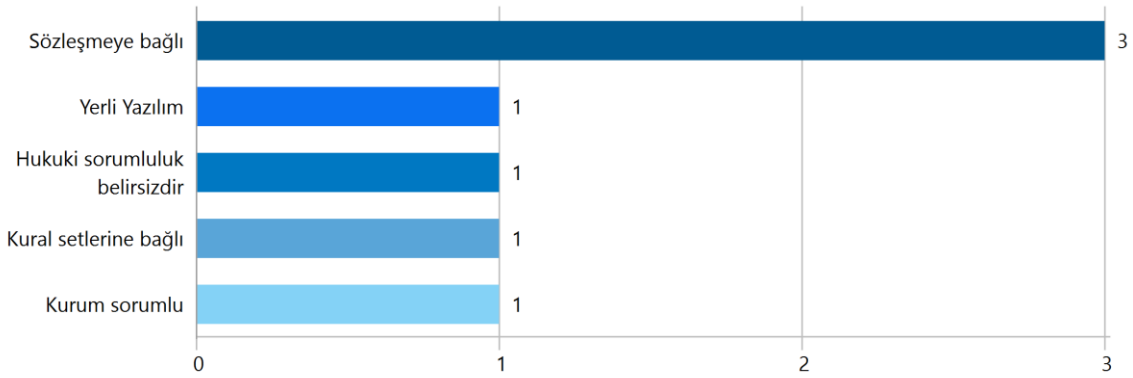
Katılımcılar bu konuda çoğunlukla yardımcı araçların süreci hızlandırabileceğini düşünmektedir. K1, "*Biz bu otomatik araçları tabiri caizse bu şekilde kullanabilirsek bu bilgi edinme taleplerinin hacmini de miktarını da azaltabiliriz"* görüşü ile bilgi taleplerinin hacmini azaltarak hızlandırabileceğini belirtmektedir. K7, "*Bilgi edinme talepleri için bence harika bir çözümdür. Yani bir çözümdür teknoloji sistemi kullanmak. Çünkü gerçekten çok zaman alıyor bu talepleri değerlendirmek ve bilgiyi bulmak özellikle dijital çağda gözden geçirmek zor olabilir*" görüşü ile bilgi edinme taleplerini değerlendirmenin özellikle dijital çağda zor bir süreç olduğunu yardımcı araçların bu süreci hızlandırabileceğini ifade etmektedir. K4, "*Mesela geçmişe yönelik tarımsal faaliyetlerin işte buğday ihraç oranlarını araştıran bir vatandaş Tarım Bakanlığı'na işte yıl yıl işte son 50 yıldaki bütün buğday ihraç rakamlarına yönelik bir bilgi talebinde bulunduğunda kişi bazlı insan tek tek arşivlerden gidip bu şeye bakıp raporlaştırma durumunda. Ama yazılımla bunu yakaladığı zaman belirli algoritmalarla çok kısa sürelerde bu soruların cevabını verebilecek şekilde hazırlığını yapabilir yani. O yüzden*

bu konu katkı sağladığını düşünüyorum" ifadeleri ile örnek vaka üzerinden sürecin hızlanabileceğini belirtmektedir.

K3, "*Belge üzerinde bulunan bilgi tanımlarının insan çıkarımıyla ve sezgisiyle yapılması gerektiğini ve bunların etiketlenmesi gerektiğini, ve bundan sonra bu etiketlemeden sonra otomatik olarak sistemler tarafından cevap verilmesi gerektiğini düşünüyorum. Etiketlenme, hassas bilgi yerlerinin etiketlenmesi bilgi taleplerinin karşılanma oranını da arttıracaktır ve hızını da arttıracaktır*" görüşü ile hassas bilgi noktalarının öncelikli olarak etiketlenmesi gerektiğini ifade etmektedir. Katılımcı etiketleme pratiğinin süreci hızlandırabileceğini düşünmektedir.

V.6.7.5. Kategori: Hukukî, Teknik ve Etik Problemler

Hukukî, teknik ve etik problemler kategorisinde görüş beyan eden altı katılımcı beş farklı görüş (Grafik 17) sunmuştur. Yardımcı araçların hassasiyet değerlendirmesi sürecinde kullanılması, insan-makine iş birliğine veya belirli işlemlerin otonomlaştırılmasına yönelik hukukî, teknik ve etik konuları gündeme getirmektedir. Katılımcılar hukukî sorumluluğun çoğunlukla sözleşmeye bağlı olduğunu belirtse de farklı düşünceler veya çözümsüzlükler de ifade edilmektedir.



Grafik 17. Hukukî, Teknik ve Etik Problemler

K5, "*Tamamen sözleşmeye bağlıdır. Hiçbir şirket bu tür sorumluluğun altına girmez*" görüşü ile sözleşmenin hukukî olarak hem kurumu hem de üretici/geliştirici firmayı bağlayacağını belirtmektedir. Benzer bir şekilde K4, "*Yüksek ihtimalle bir sözleşmeyle bunun belirlenmesi lazım*" görüşü hukukî hakların sözleşmeye dayandırılması gerektiğini ifade etmektedir. Bu görüşlerin aksine K1, "yazılımcılara yükleme şansınız yok. Kurumun sorumluluğunda olacaktır tabiki" görüşü ile kurumun sorumlu olduğunu; K3, "*Herhangi bir yanlış değerlendirme kapsamında sorumluluğun kim olacağı belli değil. Yasal düzenlemeler yapılsa bile, yapılan yasal düzenlemeler buna cevaz verse bile yanlış değerlendirme yapıldığında sorumluluğu kim üstlenecek? Ben hukukî sorunlara sebep olabileceğini düşünüyorum"* görüşü ile hukukî sorumluluğun belirsiz olduğunu ifade etmektedir. Bu bakımdan hukukî sorumluluk durumuna yönelik üç farklı görüş bulunmaktadır. K5, "*Şimdi kural setleri insanlar yazdığı için oradaki kuralların işletilmesi makine yakalı. Dolayısıyla kural ne kadar doğru, ne kadar etik, ne kadar hukukî ise o araçta ancak o kadardır*" görüşü ile kural setlerine ve dolayısıyla geliştiricilere dikkat çekmektedir.

Hukukî sorumluluğun dışında K8, "*Ulusal yerli bir yazılım daha iyi olur. Çünkü bu uluslararası belirlenmiş bir şey yok. Mevcut politika veya şey olmalı. Her ülkenin farklılık gösterebildiği için ondan dolayı Ulusal olması hem ülke veri bütünlüğü açısından hani şimdi ortak bir şey olduğunda bu veriler diğer ülkeler yani başka ülkelerin verilerine erişebilir orada çok sıkıntılı durumlar yaratabilir ülkeler için*" görüşü ile ulusal veri güvenliğine dikkat çekerek bu tür yardım araçların yerli geliştiriler tarafından tasarlanması gerektiğimi ifade etmektedir.

V.6.8. Tema: Danışma Kurulları ve Kaynakları

"Hassasiyet değerlendirmesi sürecinde danışma/gizlilik kurullarının ve kaynaklarının (rehber, kılavuz, talimatname vs.) rolü ve niteliği ne olmalıdır?" araştırma sorusunun

cevaplanması amacıyla yöneltilen görüşme sorularına verilen cevaplar, kategori ve kodlar ayrılmıştır.

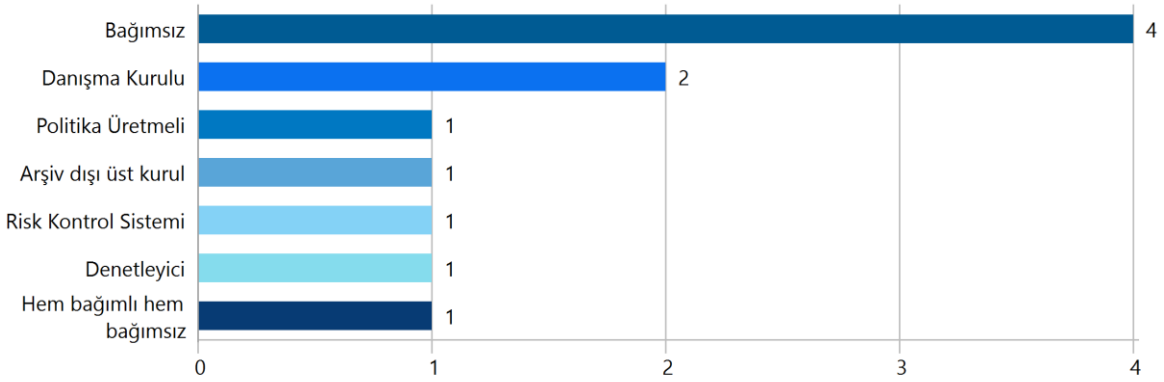
Tablo 17. Danışma Kurulları ve Kaynakları Temasına Ait Kategori ve Kodlar

Kategori	Kodlar	Katılımcılar
Kurulların Yapısı	Bağımsız	*K1, K4, K7, K8*
	Hem bağımlı hem bağımsız	*K3*
	Denetleyici	*K7*
	Danışma Kurulu	*K1, K4*
	Risk Kontrol Sistemi	*K5*
	Arşiv dışı üst kurul	*K1*
	Politika Üretmeli	*K3*
Kişilerin Niteliği	Arşiv Uzmanlığı	*K4, K8*
	Farklı Disiplin ve Kurum Yöneticilerinden Oluşmalı	*K1, K3, K4, K8*
	Yeni Nesil Teknoloji Becerisi	*K4*
	Sivil Olmalı	*K7*
	Amprik ve Matematiksel Yaklaşım	*K2*
Rehber/Kılavuz Oluşturmak	Kurumlararası İş birliği	*K3, K7, K8*
	Bilgi ve Tecrübelere Dayalı	*K2*
	Genel ve Kurum Bazlı	*K4, K5, K8*
	Problem çözer hız artar	*K8*
	Sistematik ve verimli işleyiş	*K8*

Tablo 17'de sunulan verilere göre katılımcıların görüşme sorularına verdikleri cevaplar danışma kurulları ve kaynakları teması kapsamında beş kategori altında toplanmıştır. İlk kategoride hassasiyet değerlendirmesi sürecinde danışma kurullarının ideal yapısı, işleyişi ve yönetimi konusundaki katılımcı görüşlerini içermektedir. İkinci kategori bu kurullarda yer alacak kişilerin niteliğine ve taşıması gereken becerilere dair görüşlerden oluşmaktadır. Üçüncü kategori, kamu kurumlarında hassasiyet değerlendirmesi sürecinde kullanılacak bir rehbere olan ihtiyacı ve ideal rehberin oluşturulmasına yönelik katılımcı görüşlerini içermektedir.

V.6.8.1. Kategori: Kurulların Yapısı

Kurulların yapısı kategorisinde görüş beyan eden altı katılımcı yedi farklı görüş (Grafik 18) sunmuştur. Hassasiyet değerlendirmesi sürecinde kurumlarda/birimlerde yer alan değerlendirme komisyonlarının dışında ulusal arşivlerde gizlilik konusunda kurullar/komisyonlar bulunmaktadır. Bu kurulların yapısına ilişkin katılımcılar tarafından çeşitli roller biçilmiştir. Öncelikle kurulların bağımsız olup olmaması konusunda katılımcılar çoğunlukla bağımsız olması gerektiğini ifade etmektedir.



Grafik 18. Kurulların Yapısı

İki katılımcı bu soruya cevap vermemiş (K6), bir katılımcı ise böyle bir kurulun olmaması gerektiğini (K7) ifade etmektedir. K1, "*Bağımsız bir yapı. Kurumun içerisinde yani ulusal arşiv kurumunun içerisinde ama bağımsız bir noktada"* görüşü ile kurulların bağımsız olması gerektiğini ifade etmektedir. K3, "*Devlet Arşivleri Başkanı, bu kurulun başkanlığını yürütmesi gerektiğini düşünüyorum. Malumunuz da devlet arşivleri başkanı doğrudan Cumhurbaşkanlığına bağlı. Bu şekilde hem bağımsızlık hem de bağımlılığın olabileceğini düşünüyorum. Çünkü malumunuz bu kurul birçok kamu kurumunun yetkililerini bünyesine barındıracaktır"* görüşü ile kurulun en üst yönetim kademesine bağlı olmasının hem bağımlı hem bağımsız bir yapıyı bünyesinde barındıracağını belirtmektedir. Arşiv personelinin veya yöneticisinin kurul içerisinde yer almasına karşın K1, "*Arşiv çalışanları olarak değil de belki böyle bir üst kurul veya işte bir kurul*

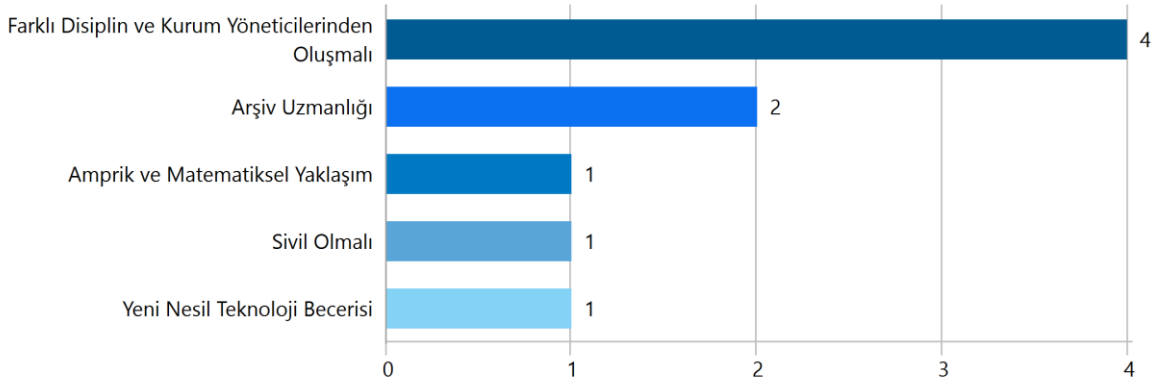
vasıtasıyla değerlendirilmesinin ben daha doğru olacağı kanaatindeyim. Hem bu geniş katılım olacağı için belki bazı algıları da giderecektir diye düşünüyorum" görüşü ile üst kurul olarak görev yapması gerektiğine dikkat çekmektedir.

K2, "*Bu kurullar danışma kurulları gerekirse… denetleyici yani kamu yararına o kamu yararına devleti hesap verilebilirlik şeffaflık konusunda denetleyen, yani denetim kurulları oluyorlar. Hani birebir belgeleri hassasiyet devredilmesinde geçirmiyorlar. Kamu kurum ve kuruluşlarının bu hassasiyet konusundaki aldığı kararları gözden geçiriyorlar… Kamu kurumlarının hesap verilebilirlik ve şeffaflık konusunda bir denetim sağlayabilirler*" görüşü ile bu kurulların denetleyici bir role sahip olması gerektiğini ifade etmektedir. K4, "*Tek aşamalı karar verme sürecinden ziyade aslında bir danışma gibi işte bu o da kurumun belgeyi üreten kuruma yol göstereceği yani böyle bir belge var biz bununla ilgili bize göndermişsin şu anda muhafaza ediyoruz. Bununla ilgili hassasiyet belirleme noktasında kendimiz bir çalışma yaptık. Bu şekilde düşünüyoruz. Siz bu belgeyle ilgili bizim yaptığımız çalışma bu. Bu konuda siz ne düşünüyorsunuz diye işte aslında bir danışma gibi*" görüşü ile denetleme ile birlikte uzlaşmazlıkların olması durumunda danışma kurulu vazifesi olması gerektiğini ifade etmektedir. Denetim ve danışma rolüne paralel bir yaklaşım gösteren K3, "*Danışma komitelerinin oluşturulmasında dikkate alınması gereken faktörler arasında risk ve risk iştahı önemli bir yer tutar. Erişim şekilleri ve risklere karşı kontrol sistemleri üzerine çok sayıda tartışma yapılması gerekmektedir"* görüşü ile kurulların risk kontrol sistemine sahip işlevi olması gerektiğini belirtmektedir.

K3, "*Bu kurul politika üretmeli… hassas belgelerin yönetimi ve denetimi hakkında işte güvenlik eğitimleri hakkında şikayetler hakkında veya bu Türkiye'de olmayan olması gerektiğini belirtmiş olduğum ikincil gizlilik dereceli belirleme prosedürü kapsamında yetkin ve yetkili bir kurulu olmalı ve bu konuda politikalar geliştirmeli*" görüşü ile kurulların politika geliştiren bir işleve sahip olması gerektiğini vurgulamaktadır.

V.6.8.2. Kategori: Kişilerin Niteliği

Kişilerin niteliği kategorisinde görüş beyan eden altı katılımcı beş farklı görüş (Grafik 19) sunmuştur. Katılımcılar farklı disiplin ve kurum yöneticilerinin bir arada olduğu çok yönlü bir kurul oluşturulması gerektiğini ifade etmektedir.



Grafik 19. Kişilerin Niteliği

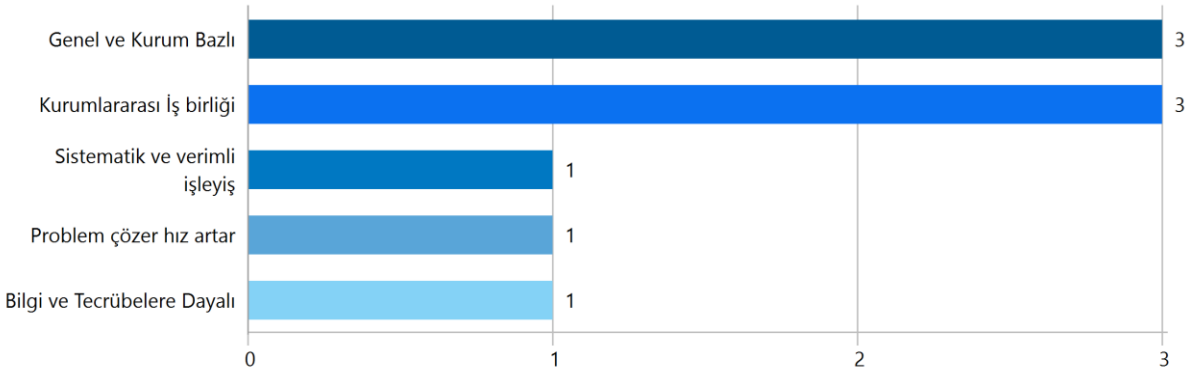
K4, "*İşte alanda yetkin kişilerin olması gerektiği bir kamu kurumunda temel, en önemli kamu kurumlarında millî eğitim, millî güvenlik… bu tarz temel ana kurumların temsilcilerinin olması gerektiğini düşünüyorum*" görüşü ile temel kurum temsilcilerinin olması gerektiğini belirtmektedir. K3, "*Bilgi belge mezunları işte hukukçular işte BT yazılım uzmanları bilgi güvenliği uzmanları veri analizcileri bu kişilerden oluşan ve kamu temsilcilerinden oluşan bir kurul oluşturulması daha faydalı olacaktır*" görüşü ile kamu kurumu temsilcilerinin yanı sıra çeşitli uzmanlık becerilere dikkat çekmiştir. K4, farklı kurum yöneticilerinin yanı sıra "*Arşiv anlamında, tasnif, meta anlamında en iyi şey yapacak, yetkin bu bilgileri en iyi şekilde ulaşacak, işleyecek kişilerin olması gerektiğini düşünüyorum*" görüşü ile arşiv uzmanlığını; "*Teknolojiyi son dönemde yakalayan, işte bu yapay zekâdır, son dönemde gelişen teknolojilerdir. Bunları en iyi şekilde kullanan, yetkin kişilerden oluşan bir kurul olması gerektiğini düşünüyorum*" görüşü ile yeni nesil teknoloji becerilerine sahip nitelikli kişilerin kurul içerisinde yer alması gerektiğini ifade

etmektedir. K2, kişilerin niteliğine dair "*Daha bilimsel daha ampirik ve daha matematiksel bir bakış açısıyla*" görüşünü sunmaktadır.

K7, "*Bu kuruldaki kişiler genellikle üst düzey olur ve sivil olurlar. Mesela eski bir emekli bir vali vardı, bir gazeteci vardı, kurumda üst rütbe bir emekli olan bir general vardı, askeriyede bir akademisyen vardı… Kesinlikle devlette hala çalışan memurlardan, kişilerden, uzmanlardan oluşturulmamalı*" görüşü ile kurullardaki kişilerin niteliğine dair aktif görevde olmayan üst düzey siviller olması gerektiğini ifade etmektedir.

V.6.8.3. Kategori: Rehber/Kılavuz Oluşturmak

Rehber/Kılavuz oluşturmak kategorisinde görüş beyan eden altı katılımcı beş farklı görüş (Grafik 20) sunmuştur. Katılımcılar rehber/kılavuz gereksinimi ve oluşturulma yöntemlerine dair çeşitli görüşler sunmaktadır.



Grafik 20. Rehber/Kılavuz Oluşturmak

K8, "*Bu kılavuzlar, prosedürler hassasiyetin veya hassas bilgilerin değerlendirme sürecinin hızlı ve sorun çözme rehberi olarak sürecin daha problemsiz işlemesine yardımcı olur*" görüşü ile rehberlerin problem çözücü rolüne; "*Kamu kurumlarında kılavuz ve rehberlerin, prosedürlerin, talimatların kullanılması süreçlerin sistematik, verimli ve uyumlu bir şekilde yürütülmesinde önemli katkı sağlar*" görüşü ile kurumlara sistematik ve verimli işleyiş sunma rolüne dikkat çekmektedir. Bu rehberin oluşturma

yöntemi konusunda K2, "*Bildiklerimizi ya da öğrendiklerimizi yazılı hale getirerek, kılavuzlar ve rehberler oluşturarak kodlamak için zaman ayırırsak, kolektif olarak en hızlı şekilde ilerleyeceğiz… Tüm yaklaşımlarımızı giderek daha fazla revize etmek ve uyarlamak zorundayız. Bu nedenle, öğrendiklerimizi kodlamak, öğrendiklerimizi daha iyi paylaşmak ve pratiğimizi hızlı bir şekilde geliştirmek için gerçekten çok önemlidir"* görüşü ile bu rehberin bilgi ve tecrübelere dayalı olarak oluşturulması gerektiğini vurgulamaktadır. Bazı katılımcılar rehber oluşturulurken kurumlararası iş birliğini öne çıkarmaktadır. K3, "*Kurumlar arasında iletişimle bu belgeden ikincil ve türev belge oluşturulurken de dikkat edecek hassasiyetlere dikkat edilmesi ve uygun gizlilikleri derecesi verilmesi gerektiğini düşünüyorum. Ve bu politikalar oluşturulmalı bence ve kılavuzlar yapılmalı. Kurumlar birbirleri arasında iletişim sağlamalı"* görüşü ile kurumlararası iş birliği ve koordinasyona dikkat çekmiştir. Benzer bir şekilde K8, "*İletişim ve koordinasyon kurumlar arasında bir iş birliği veya bir şirket veya kurum içerisinde ise de departmanlar arasında iş birliğini artırarak hassasiyet değerlendirmesi süreçlerinde daha iyi bir sonucun ulaşmasına koordinasyonunu sağlamak*" ifadeleri ile bu görüşü desteklemektedir.

Bazı katılımcılar oluşturulacak olan rehberin hem genel hem de kuruma özgü olmasını gerektiğini savunmaktadır. K5, "*Genel çerçeveyi çizecek bir yapı oluşturduktan sonra onun içini doldurmak kurumlara, birimlere kalır. Onlar da bu usul çerçevesi içerisinde kendi değerlemesini yapar. Daha mantıklı olur. Merkezî bir kılavuz rehber kesinlikle faydalı olur*" görüşü ile hem genel hem de kurumlara özgü hassasiyetlerin yer aldığı rehber olması gerektiğini belirtmektedir.

VI. BÖLÜM: DEĞERLENDİRME, SONUÇ VE ÖNERİLER

Çalışmanın bu bölümünde yapılan analizler ve araştırma sürecinde elde edilen bulgular bütüncül bir bakış açısıyla değerlendirilecek, ortaya çıkan sonuçlar ışığında tartışma ve öneriler sunulacaktır.

Hassas bilgi mevzuatı incelenen ülkeler ve uluslarüstü kuruluşlar değerlendirildiğinde hassas olarak ifade edilen listelemelerin odağında genellikle nitelikli kişisel veriler yer almaktadır. Türkiye'de özel nitelikli kişisel veri olarak adlandırılan bu veri türleri son dönem yapılan düzenlemeler ile AB GVKT ile uyumlu hale getirilmiştir. Hassasiyetin kişisel verilere odaklanan güçlü ve yaygın bir yönünün bulunması, kişilere bağlı hassasiyet ifşasının ciddi problemlere (hukukî, psikolojik, sosyal maddi ve manevi) sebebiyet vermesi düzenlemelere etki etmiştir. Kişilerin dışında var olan hassas bilgi olgusu düzenlemelerde bilgi edinme hakkı kapsamında sınırlılıklar (IV.9 bölümde belirtilen) veya muafiyetler olarak ifade edilmektedir. Bu bakımdan hassas bilgi kavramına yönelik doğrudan kişileri tanımlayan ve kişilere bağlı olmayan bir yaklaşım ortaya çıkmaktadır. Çalışmada hassas bilgi türlerine yönelik bu yaklaşım kişisel tanımlanabilir bilgiler, kamu kaynaklı bilgiler, ihtisas alanı ve sektör bilgileri olmak üzere üç yönlü bir sınıflama[73] olarak geliştirilmiştir. Özellikle kamu kurumlarının farklılaşan hizmet alanları ve üretilen belge çeşitliliği değerlendirildiğinde, hassasiyetin yalnızca kişilere ait verilerle sınırlı kalmadığı görülmektedir. Bu sınıflamanın temel amacı, belgelerin yönetim ve özellikle arşivleme süreçlerini kolaylaştırmaktır. Arşiv işlemleri mevzuat ve bağlı düzenlemeler çerçevesinde yürütülmektedir. Ulusal arşivler, mevzuata uyumlu kılavuzlar oluşturarak kamu kurumlarına direktifler vermektedir. Dolayısıyla mevzuatın kapsayıcı olması gerekmektedir. Örneğin, TNA tarafından 2015'te yayımlanan ve 2019'da revize edilen "*Personal information: a guide for justification*

[73] Bu sınıflama II.4 Hassas Bilgi Türleri başlığında "Şema 2. Hassas Bilgi Sınıflaması" olarak yer almaktadır.

wording" adlı kılavuz, hangi bilgi türlerinin hassas kabul edildiği, bu bilgilere dair açıklamalar ve kapatma süreleri hakkında mevzuata dayalı sınırlar çizmektedir. Ancak bu kılavuz sadece kişilere bağlı hassasiyetlere odaklı olarak geliştirilmiştir. Bununla birlikte TNA tarafından 2015 yılında yayımlanan "*Access to public records*" adlı kılavuz kamu kurumları için hassasiyet değerlendirmesi sürecinde kişisel verilerin dışındaki bilgi edinme hakkı muafiyetleri hakkında direktifler sunmaktadır. Kılavuz, ulusal güvenlik, savunma, uluslararası ilişkiler, ekonomi, ticarî sır gibi konularda mutlak kapatma ya da kamu yararı testi uygulamalarından hangisine başvurulması gerektiğine ve bunun sonucunda kapatma sürelerine ilişkin bir çerçeve sunmaktadır. Bu bakımdan kişisel hassas bilgiler ile birlikte kişilere bağlı olmayan konuların da hassasiyet değerlendirmesi sürecinde göz önünde bulundurulması gerektiği açıkça görülmektedir. Kamu belgelerindeki hassasiyetin çoğunlukla kişisel hassas verilerden oluşması değerlendirme sürecinde daha çok dikkate alınmasına sebep olmaktadır. Her ne kadar kurum/fon bazlı bir belge çeşitliliği olsa da doğrudan gerçek kişileri ilgilendiren hassas bilgilerin özel bir koruma ve işleme gerekçelerine tabi tutulması mevzuat ile garanti altına alınmıştır.

Çalışma kapsamında arşivcilik alanında öncü kurumların faaliyetleri (IV. Bölüm) incelenmiştir. İncelenen ulusal arşivler, arşiv uygulamalarında hassasiyet değerlendirmesi sürecine yer vermiştir. Özellikle TNA sürece dair her aşamaya (transfer, imha, redaksiyon, kapatma süreleri, teknoloji yardımlı değerlendirme vs.) yönelik bir uygulama kılavuzu yayınlamıştır. Diğer ulusal arşivler web sitelerinde, strateji belgelerinde, arşiv mevzuatında hassas bilgilerin yönetimine ilişkin kurallar yayınlamışlardır. Kurumlar, çoğunlukla kataloglarında (çevrimiçi) hassasiyet gerekçesi ile kapalı tuttukları belge ve belge gruplarına dair yasal gerekçeler sunmuş, üst veri alanlarını bu doğrultuda tanımlayarak kamu erişimine açmışlardır. Bazı kurumlar belgeleri sınırlı olarak (redaksiyon veya maskeleme) erişime sunmuşlardır. Türkiye özelinde yapılan incelemeler doğrultusunda DAB kataloğu (BETSİS) erişime kapalı

belgeler ile ilgili herhangi bir üst veri bilgisi sunmamaktadır. Nitekim Arşivlerden Yararlanma Usul ve Esasları Hakkında Yönetmelik (2021, 9/2), özel nitekli belgelerin bilimsel araştırmalar için gerekli olması durumunda korunarak verilebileceğine işaret etmektedir. Bu madde daha önce anılan Bilgi Edinme Hakkı Kanunu'nun 9. maddesi ile desteklenmiştir. Ancak katalogta belge veya belge grubunun var olduğuna dair üst veri alanlarının dahi yer almaması erişimin önünde bir engel olarak varlık göstermektedir. Bununla birlikte her yıl TBMM tarafından yayımlanan bilgi edinme genel raporlarında – özellikle "gizli ya da sır niteliğindeki bilgiler çıkarılarak veya ayrılarak bilgi ve belgelere erişim sağlanan başvurular" – DAB'ın veri sağlayıcı kurumlar arasında yer almaması dikkate değer bir başka eksikliktir. Arşiv belgelerine yönelik olarak bu kapsamda yapılan başvuruların olup olmadığı, red veya kabul durumları açıklanmamaktadır. DAB'ın hassasiyet değerlendirmesi sürecinin yanı sıra gizlilik dereceleri belgelerin arşivleme sürecine ilişkin kamu kurumlarını yönlendirici bir rehberi bulunmamaktadır. Bu konuda gizlilik yönetmeliğine bağlı oluşturulan kılavuzun dışından bir yaklaşım gösterilmemiştir. Türkiye'deki mevzuatın belirli kısımlarında hassas bilgilere yönelik göndermeler yapılmıştır. Ancak uygulama noktasında gerek DAB gerekse kamu kurumlarında yönlendirici bir doküman eksikliğinden kaynaklanan bir belirsizlik bulunmaktadır. Hassas bilgi içeren gizlilik dereceli belgelere yönelik kapatma süreleri ve gizlilik derecesinin değişmesi durumunda yönetim faaliyetlerinin nasıl ilerleyeceği konusunda eksiklikler bulunmaktadır. Gizlilik derecesine sahip belgelerin farklı güvenlik düzeylerinde yönetilmesi ve gizlilik derecelerindeki değişikliklerin kurumlarda hibrit yönetim ve arşivleme süreçlerini gerektireceği düşünülmektedir (Kaymak ve Külcü 2024, s. 274). Bu görüş, katılımcıların süreç zorluğu olarak ifade ettiği bir yön olması bakımından literatür ile örtüşmektedir. Hibrit yapı arşivlenen belgelerin dinamik bir süreç yönetimine tabi tutulacağını, hassas belgelerin/bilgilerin özellikle zaman ve bağlamsal faktörlerden dolayı pozitif veya negatif durumlara sebep olacağını göstermektedir.

Bununla birlikte, kapatma sürelerinin belirsizliği, daha önce anılan Devlet Sırrı Kanun Tasarısı'nda önerilen süreler temelinde değerlendirilmesi gereken ayrı bir konu ve önemli bir eksiklik olarak öne çıkmaktadır.

Hassasiyet değerlendirmesi işleminin bir süreç yönetimi olması, etkili olabilecek her yaklaşımın incelenmesini gerekli kılmaktadır. Bu sebeple, görüşme verileri katılımcıların sürece etki eden çeşitli temalarda oluşan görüşlerinin incelenmesine olanak sağlamıştır. Katılımcılar hassas bilgi, hassasiyet değerlendirmesi, değerlendirme zorlukları ve çözümler, teknoloji yardımlı değerlendirme, danışma kurulları ve kaynakları temaları/konuları doğrultusunda düşüncelerini aktarmıştır. Elde edilen bulgular olduğu gibi yansıtılmıştır.

Hassas bilgi mevzuatı, kapsamı ve tespiti konularında soruların yöneltildiği ilk temada katılımcıların vurguladığı bazı alanlar öne çıkmaktadır. Çoğu katılımcı hassas bilginin hangi ortamda/formatta bulunduğunun tespitini etkilemeyeceğini belirtmiştir. Hassasiyet değerlendirmesinin içerik ile ilgilenen bir alan olmasından dolayı formatın ancak yönetim süreçlerine etki eden bir faktör olacağı anlaşılmıştır. Ancak format artan dijital hacim sebebiyle tespiti güçleştiren bir meseledir. Mevzuatın hassasiyeti belirli kalıplar, konular, kelimeler, ifadeler bağlamında değerlendirmesi sınırlı bir hareket alanı oluşturacağından içerikteki bağlamın dikkate alınarak nesnel ölçütlerin ancak kurum bazlı iş süreçlerine dayalı bir sınıflama ile mümkün olacağı düşünülmektedir. Bu durum araştırmanın ikinci bölümünde oluşturulan hassas bilgi türleri sınıflamasının tutarlılığına işaret etmektedir. Mevzuatın statik, ait olduğu zamana ve öncesine ait izler barındıran bağlayıcı bir unsur olması toplumsal değişimlerin hassas bilgi anlayışındaki güncellemelere yanıstılamamasına sebep olmaktadır. Bu bakımdan katılımcılara göre tanım ve tema anlayışını geniş kapsamda yansıtan bir mevzuat iradesi ortaya konulmalı; kurumların bağlı yönerge ve yardımcı dokümanlarını güncellemelerine olanak sağlayacak şekilde düzenlemeler yapılmalıdır. Bu temada katılımcıların dikkat çektiği bir başka yön

ise kurum bazlı hassasiyetlerin oluşturulmasıdır. Her kurumda benzer içerik ve amaca hizmet eden belgeler üretilse de farklılaşan belge ve form türleri de bulunmaktadır. Kuruma özgü hassasiyetlerin üretilen belgelere yansıması nedeniyle, hassas bilgi kapsamına yönelik genel bir dokümanın oluşturulması kurumlardan alınacak geri bildirimler doğrultusunda gerçekleştirilmelidir.

Hassasiyet değerlendirmesi konusunda soruların yöneltildiği ikinci temada katılımcılar bu sürecin risk ile olan bağlantısını kurmuşlardır. Hassasiyet değerlendirmesi sürecinde belgelerin üretildiği ortam farketmeksizin bir risk yönetimi uygulanmaktadır. Bu konuda bazı katılımcılar kâğıt bazı katılımcılar elektronik ortamın daha fazla risk içerdiğini ifade etmişlerdir. Farklılaşan bu görüşlerin katılımcıların deneyimlerine bağlı olduğu söylenebilir. Bununla birlikte dijital bilgi hacminin fazla, dağınık ve kontrolsüz olması hassasiyet değerlendirmesi sürecini negatif yönde etkilediği bilinmektedir (McDonald ve diğerleri, 2014, s. 500; The National Archives, 2016, s. 6; McDonald, McDonald ve Ounis, 2019, s. 337; Whyte ve Walsh, 2024, s. 13). Bu bağlamda elektronik ortamın hassasiyet değerlendirmesini olumsuz yönde etkilediği (risk, miktar, kontrol,) tespiti literatür ile uyumlu olarak katılımcıların çoğunluğu tarafından ifade edilmiştir. Literatürden farklı olarak katılımcıların formata göre yönetim farklılıklarına değinmesi gizlilik derecelerine bağlı süreç yönetimine işaret etmektedir. Bu konuda ayrıca zorlukların ifade edildiği üçüncü tema kapsamında da (hibrit yönetim) yer almaktadır. Hassasiyet değerlendirmesi sürecinde üreten kurum ile iş birliğinin gerekliliği ve iki aşamalı değerlendirme yaklaşımı farklılaşan diğer önemli noktalardır. Kurum bazlı hassassiyetlerin ifade edildiği ilk temadaki görüşler, iki aşamalı iş birlikçi değerlendirme yaklaşımı ile bağlantılı bir anlayış göstermektedir.

Hassasiyet değerlendirmesi sürecinde yaşanan zorluklar ve çözüm önerileri konusunda soruların yöneltildiği üçüncü temada katılımcılar literatürde var olan zorluklara ek olarak farklılaşan yaklaşımlar göstermişlerdir. Katılımcılar değerlendirme

zorluklarından bağlam, zaman, kişisel bakış ve mozik yapı zorluklarına yönelik literatür ile bağdaşan görüşler bildirmişlerdir. Bu zorlukların dışında katılımcılar gizlilik derecelerinin tanımlanmaması sorunu ile bu konudaki farkındalık eksikliğine dikkat çekmişlerdir. İçerikteki bilginin hassas olduğunun farkında olunmaması gizlilik kapsamında değerlendirilmemesine sebep olmaktadır. Bununla birlikte gizlilik derecelerinin değişmesi sonucu hibrit süreç yönetimine işaret edilmiştir. Süreç yönetimi konusunda özellikle elektronik ortamda üretilen hassas belgelerin transfer yönetiminin nasıl yapılacağı konusu benzer bir zorluk olarak ifade edilmiştir. Dosya ve saklama planında gizli ve hassas belgelere yönelik alan eksikliğine dikkat çekilmiştir. Çeşitli zorlukların ifade edildiği bu temada katılımcılar bazı konularda çözüm önerileri geliştirmiştir. Erişim hususunda sınırlı erişim yöntemlerinin katılımcılar tarafından önerilmesi literatür ile bağdaşmaktadır. Hassasiyet değerlendirmesi sürecinde objektifliği sağlamaya yönelik çözümün otomasyon olduğunun ifade edilmesi dijital araçların kullanımına yönelik pozitif bir görüş olarak değerlendirilebilir. Ancak subjektifliğin otomasyon ve yardımcı araçların tasarlanma/kodlanma süreçlerine veya algoritmaların eğitim verilerine yansımayacağı düşünülmeyebilir. Bununla birlikte mevzuat ve mevzuata bağlı eğitim ve bilgilendirme faaliyetlerinin dikkate alınmasının objektifliği arttıracağı düşünülmektedir. Ancak, gerek mevzuat gerekse mevzuata dayalı eğitimler, görev tanımları ve talimatnameler uygulama aşamasında kişilere bağlı olarak gerçekleşeceğinden, objektif bir sürecin garanti altına alınması güçtür. Bir diğer zorluk olan zaman konusunda çözüm geliştiren katılımcıların her biri, kendi içinde geçerli olabilecek önemli noktalar üzerinde durmaktadır. Ancak bazı çözüm önerilerine dijital çağda, daha dinamik ve esnek çözümler gerekli olabilir. Örneğin yayından kaldırmak çözümü, belgenin hala erişilebilir olmasını engellemeyebilir. Bununla birlikte periyodik değerlendirme önerisi, belgelerin belirli aralıklarla gözden geçirilmesini sağlamak adına faydalı bir çözüm sunabilir. Bu yaklaşım, periyodik değerlendirme sürelerinin doğru bir

şekilde belirlenmesi ve kuruma özgü ihtiyaçlara göre uyarlanması ile sistematik bir sürecin oluşturulmasına olanak sağlayabilir. Son olarak katılımcıların mozaik yapıya dair görüşleri, bilgi yönetimi ve kataloglama süreçlerini geliştirmeye yönelik ilişki kurma (ilişkili belge kümesi oluşturma) ve iş birliği odaklı yaklaşımlar sunmaktadır. İlişkili kataloglama anlayışı belgeler arası anlamlı ilişkiler kurulmasını sağlayabilir. Ancak uygulanması zaman ve kaynak gerektirecektir. Bununla birlikte koordineli çalışma önerileri, bilgi paylaşımını ve iş birliğini teşvik ederek, belgelerin daha kapsamlı değerlendirilmesine yardımcı olabilir. Ancak farklı belge grupları arasında kurumlar arasında ilişki kurmaya yönelik bir uyumdan bahsetmek mümkün görünmemektedir. Hangi belgenin ilişkili veya ilişkisiz belgeler ile bir araya getirilince hassasiyet oluşturacağını belirlemek zordur. Bu durumu zamana bağlı olarak değişen hassasiyetler negatif yönde etkileyecektir. Çözüm önerileri konusunda, teknoloji yardımlı değerlendirme teması altındaki yapay zekâ kategorisi, bu teknolojinin çoğu sorunu (bağlam, objektiflik, zaman) çözmek için kullanılacağına dair katılımcı görüşlerinden oluşmaktadır. Nitekim bazı sorunların çözümündeki karmaşıklık ve çoğu parametriyi aynı anda değerlendirme gereksinimi günümüzde ve gelecekte yardımcı araçlara – özellikle yapa zekâya – ihtiyaç duyulacağını göstermektedir.

Hassasiyet değerlendirmesi sürecinde teknoloji yardımlı değerlendirme konusunda soruların yöneltildiği dördüncü temada katılımcılar bu sürecin büyük ölçüde insana bağlı olacağını belirtmektedir. Yardımcı araçlar iş süreçleri hem pozitif yönde (hızlı, tutarlılık, hacim, otomatikleştirme) hem negatif (güvenilirlik, teminoloji ve eş/yan anlam) yönde etkilemektedir. Henüz bu araçların kullanımı konusunda güven düzeyinin yeterli olmadığı[74] ve doğrulamaya ihtiyaç olduğundan dolayı otonom işlemler küçük ölçekte var olabilir. Bununla birlikte yapay zekânın çözüm olarak ifade edildiği alanlarda

[74] Wyte ve Walsh (2024, s. 17) tarafından yapılan çalışmada katılımcılar hassas bilgileri tespit etmek için kullanılan yazılım araçlarının güvenilirliği ve doğruluğu konusunda endişelerini dile getirmektedir. Bu bakımdan benzer sonuçlara ulaşılmıştır.

(bağlam, zaman, objektiflik vb.) öngörüsel olarak fayda sağlayacağı düşünülmektedir. Katılımcıların bu yaklaşımı, gelecekte hassasiyet değerlendirmesi sürecinin her safhasında bir yapay zekâ izinin olabileceğini düşündürmektedir. Otonom işlemlerin değerlendirme sürecinde rol alması, katılımcılar arasında tartışmalı bir konu olarak öne çıkarken bazı katılımcıların teknolojinin belirli kurallar çerçevesinde insan katkısıyla otonom hale gelebileceğini savunmaktadır. Diğer taraftan insan sezgisi, empati ve deneyimin mutlak bir otonom sistemle karşılanamayacağı belirtilmektedir. Bu eleştirel yaklaşım, teknolojinin insan deneyimini ve etik duyarlılığı günümüz teknolojisi ile tam anlamıyla ikame edemeyeceğini ortaya koymaktadır. Özellikle, etik açıdan önemli ve doğrudan insanları ilgilendiren kararlar söz konusu olduğunda insan müdahalesi gerekliliği vurgulanmaktadır. Yardımcı araçların etkili olabileceği bir diğer alan bilgi edinme hakkı talepleridir. Bilgi edinme süreçlerinde yardımcı araçların hız ve tutarlılık sağlaması, katılımcılar tarafından desteklenmektedir. Ancak, belge üzerindeki hassas bilgilerin doğru tanımlanması ve etiketlenmesi[75] süreçte hız ve tutarlılık elde etme açısından gerekli olacağı ifade edilmiştir. Sürecin doğru işletilebilmesi tanımlamanın ve bağlı olarak hassas bilgi etiketlemelerinin niteliği ile doğru orantılı olmaktadır. Bu durum olumlu bir katkı sunmasına rağmen sürecin insan müdahalesine bağlı olması sebebiyle tam anlamıyla otonom bir yapının eksik kalabileceğini ortaya koymaktadır. Hukukî sorumluluğun belirlenmesi konusunda katılımcıların görüş ayrılıkları dikkat çekicidir. Kimi katılımcılar, hukukî sorumluluğun yazılımlar ve kurumlar arasında bir sözleşme çerçevesinde paylaşılması gerektiğini ifade ederken, bazı katılımcılar sorumluluk belirsizliğinin hukukî sorunlara yol açabileceğini öne sürmektedir. Bazı katılımcılar ulusal veri güvenliğine dikkat çekerek, bu tür teknolojilerin yabancı kaynaklı olması durumunda riskli hale gelebileceğini belirtmektedir. Bu eleştiriler, hukukî ve etik

[75] Jaillant (2022b, s. 418) hassasiyet değerlendirmesinde yapay zekâ ve makine öğrenmesi kullanılarark otomatik etiketleme yapılacağını ifade etmektedir. Özellikle bilgi edinme hakkı taleplerinde bu işlemin el yordamı olarak yapılacağı konusundaki katılımcı görüşünün aksine bir yaklaşım göstermiştir.

sorumluluğun yalnızca yasal düzenlemelerle değil, yazılımların geliştirilmesi ve kullanımında da çok yönlü değerlendirmelere ihtiyaç duyulduğunu göstermektedir. Son dönemlerde AB ülkelerinin yapay zekâ ve türev teknolojilerine yönelik hukukî düzenlemelerde[76] bulunması bu alanda dikkate alınacak düzenlemenin önemine ve gerekliliğine işaret etmektedir.

Hassasiyet değerlendirmesi sürecinde danışma kurulları ve kaynakları konusuna ilişkin soruların yöneltildiği beşinci temada, katılımcılar danışma kurullarının genellikle bağımsız olması gerektiğini belirtmektedir. Ulusal arşivlerde bu yapı, tamamen bağımsız olmamakla birlikte bağlı bir yapı olarak yer almaktadır. Bağımsızlık, kurulların özgürce karar alabilmesini, aynı zamanda kamu yararı doğrultusunda hesap verebilir olmasını sağlayan bir dengeyi ifade etmektedir. Karar verici rolünden ziyade kurulun denetim, danışma ve politikalar üreten bir üst yapıya sahip olması hem objektif hem de bağımsız hareket kabiliyetini desteklemektedir. Bağımsızlığı destekleyici bir etken olarak kişilerin sivil emekli üst yöneticilerden seçilmesi uygun olabilir. Hassasiyet değerlendirme süreci, bir risk yönetimi olarak, kurulun yalnızca pasif bir danışma merci olmasının ötesinde, uzun vadeli stratejiler oluşturan aktif bir fonksiyon üstlenmesini gerektirmektedir. Bununla birlikte ilk temada kurum bazlı hassasiyet sınıflandırma yaklaşımı ile danışma kurulunda yer alacak kişilerin farklı disiplin ve kurum temsilcilerinden oluşması gerektiği fikri örtüşmektedir. Literatürde, danışma kurullarının farklı alanlardan uzmanların bir araya geldiği çok yönlü bir yapıya sahip olması gerektiği vurgulanmaktadır (Keskin, 2012, s. 8). Bu kurulların özünde arşiv biliminin genel teori ve esasları konusunda bilgili ve tecrübeli uzmanların yanı sıra – özellikle yardımcı araçların değerlendirme sürecindeki katkısı ve rolü göz önünde bulundurulduğunda – yeni nesil teknoloji becerilerine sahip

[76] AB parlementosu Haziran 2024'te dünyanın ilk kapsamlı yapay zekâ kanununu (Artificial Intelligence Act) onaylayarak yürürlüğe koymuştur. Bu kanun, yapay zekâ uygulamalarının risk düzeyine göre sınıflandırılmasını ve yüksek riskli teknolojilere sıkı denetimler uygulanmasını öngörmektedir. Bkz. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

kişilerin yer alması gerekmektedir. Katılımcıların görüşü bu durumu desteklemektedir. Benzer bir şekilde, kamu kurumlarının hassasiyet değerlendirmesi sürecinde bağlı kalacakları bir rehberin oluşturulmasında, her kurumun görüşünün alınması katılımcı bir dokümanın ortaya çıkmasına katkı sağlayacaktır. Bu bağlamda, kurumlar arası iş birliği ile genel yaklaşımlar belirlenecek ve her kurum, bu genel rehbere bağlı olarak kendi iç hassasiyetlerini yansıtacak politika ve yönergeleri oluşturabilecektir.

Bu çalışmada, hassas bilgi içerikli kamu belgelerinin arşivsel değerlendirme süreci araştırılmıştır. İncelenen mevzuat, literatür, ulusal arşivlerin faaliyetleri ve yapılan görüşmeler doğrultusunda "*Türkiye'de hassas bilgi güvenliğini sağlamak amacıyla, T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı başta olmak üzere kamu kurumlarında hassasiyet değerlendirmesi sürecinin doğru yönetimi için yasal düzenlemeler, kapsamlı politika belgeleri, rehberler, kontrol listeleri, danışma kurulları oluşturulmalı ve güçlü bir dijital altyapı geliştirilmelidir*" hipotezi (H1) sorgulanmıştır. Türkiye'de yürürlükte olan mevzuat, hassas bilginin sınıflandırılması, arşivlenmesi ve erişime sunulması konusunda diğer ülkelere göre yetersiz değildir; ancak uygulama[77] aşamasında bilgi ve farkındalık eksikliği mevcuttur. Bu eksikliğin başlıca sebebi, ulusal arşivin (DAB) bu konudaki farkındalığının düşük olmasıdır. Hassas bilgi kavramı ve bu kavram etrafında gelişen kamu belgelerine yönelik yaklaşımlar, konunun net bir şekilde tanımlanmasına yardımcı olmamaktadır. Dolayısıyla belirsiz bir şekilde tanımlanan ve yaygın olarak yorumlanan bir kavram etrafında politika geliştirmek zordur (Dressler ve Kearns, 2023, s. 175). Ancak ulusal arşivlerin bu konudaki yaklaşımları yeni değildir. Bu alanda ağırlıklı olarak yurtdışında yürütülen bilimsel araştırmalar başta olmak üzere incelenen kaynaklar ve kurumsal uygulamalar konunun anılan unsurlar çerçevesinde Türkiye'de geliştirilmesi gerektiği hipotezinin doğrulamaktadır.

[77] Türkiye'deki kurumlar üzerine yapılan bir araştırmaya göre (Cengiz-Mater, 2022) hassasiyet değerlendirmesi çoğunlukla uygulanmamaktadır.

Mevzuat, hassas bilgilerle ilgili belirli yönlerdeki hassasiyetlere odaklanmakta, donuk bir yapıya sahip olduğu ve tanımlara dayalı bir yaklaşım sergilemediği için yetersiz kalmaktadır. Bundan dolayı "*hassasiyet değerlendirmesi sürecinde, yürürlükte olan gizlilik/koruma mevzuatında listelenen hassas bilgi türleri, belge içeriklerinde bulunan yeni veya gelişen hassas veri türlerini tanımlamakta yetersiz kalmaktadır*" alt hipotezi (H1.1) doğrulanmıştır. Katılımcı görüşleri (V.6.4. Tema: Hassas Bilgi) ve literatür (II.4. Hassas Bilgi Türleri) bu durum destekler niteliktedir.

Mevzuat, yasal yükümlülükleri ve bunların sonuçlarını belirlerken; kılavuzlar ve politikalar, sürecin adımlarını ve uygulama yöntemlerini tasarlayan bir el kitabı işlevi görmektedir. Hassasiyet değerlendirmesi sürecinin yüksek risk içermesi nedeniyle, değerlendiricilere yardımcı olacak kontrol listeleri ve kılavuzlar gibi rehber dokümanların hazırlanmasının sürecin etkinliğini artıracağı öngörülmektedir. Bu doğrultuda, "*Hassasiyet değerlendirmesi sürecinde, değerlendiricilere yardımcı olacak kontrol listeleri ve kılavuzlar gibi rehber dokümanların hazırlanması sürecin etkinliğini artıracaktır*" (H1.2) alt hipotezi öne sürülmüştür. İncelenen ulusal arşivler bu tür belgeleri mevzuata dayalı olarak oluşturdukları rehberler doğrultusunda değerlendirmektedir. Nitekim bu konuda en fazla reber yayınlayan TNA, arşiv genel süreç yönetiminin her safhasında hassasiyet değerlendirmesi ilişkisi kuran otorite bir kurumdur. Katılımcı görüşleri (V.6.8.3. Kategori: Rehber/Kılavuz Oluşturmak) ve ulusal arşiv uygulamaları (IV. Bölüm) hassasiyet değerlendirmesi sürecinde yardımcı dokümanların kullanılması süreci olum yönde etkileyecektir hipotezini doğrulamaktadır.

Dijital çağda bilgi ve belgelerin yönetimi gizlilik unsuruna bağlı olmaksızın zor bir süreçtir. Hassas ve gizli bilgi içeren belgeler bu süreci daha da zorlaştırmaktadır. Bu sebeple "*Dijital araçlar ve yazılımlar, hassasiyet değerlendirme sürecinde tespit, belge hacmini yönetme, uzman bilgisi sağlama, danışma ve uyarı mekanizmalarını geliştirme bakımından yönetimi olumlu yönde etkliyecektir*" (H1.3) alt hipotezi öne sürülmüştür.

Yapılan araştırmalar sonucu ulaşılan literatür (III.4. Dijital Değerlendirme ve Yardımcı Araçlar), ulusal arşivlerin çalışmaları (The National Archives, 2016) ve katılımcı görüşleri (V.6.7. Tema: Teknoloji Yardımlı Değerlendirme) çeşitlilik arz ederek bu hipotezi doğrulamıştır.

Bu araştırmada belirlenen model doğrultusunda kapsamlı analizler yapılmış ve çeşitli bulgulara ulaşılmıştır. Literatür incelemesinde ağırlıklı olarak yabancı kaynaklardan yararlanılması ve araştırma grubunda uluslararası katılımcıların bulunması, Türkiye'de yürütülen bu çalışmaya önemli bir katkı ve zenginlik sağlamıştır. Elde edilen sonuçlar, literatüre özgün katkılar sağlarken ilgili alan için de geniş bir perspektif sunmaktadır. Bu bağlamda, araştırma; Türkiye'deki uygulamalar için farkındalık ve gizlilik konularında bir yaklaşım paradigması sunarak hem hassasiyet değerlendirmesi konusunda mevcut durumu iyileştirecek hem de gelecek araştırmaları destekleyecek öneriler sunmaktadır. Öneriler literatür, incelenen ulusal arşivler ve görüşmeler doğrultusunda elde edilen bulgular doğrultusunda geliştirilmiştir.

1. Hassas bilgi mevzuatında (KVKK, BEHK) belirtilen/listelenen unsurlara ek olarak, hassasiyeti sınırlamayan, tanım temelli bir çerçeve oluşturulmalıdır. Bu çerçeve, bağlama duyarlı olarak hassasiyet derecesini belirleyebilecek kriterler içermeli ve kamu kurumları ile çeşitli sektörlerin ihtiyaçlarını karşılayacak şekilde genişletilebilir ve güncellenebilir olmalıdır.
2. Kurumsal bağlama dayalı olarak oluşan veya oluşması muhtemel hassas belge, form ve/veya dokümanlar, kamu kurumlarının olağan iş akış süreçlerinde kurum idarelerince tespit edilerek "Kurum Bazlı Hassasiyet Envanterleri" oluşturulmalıdır. Bununla birlikte DAB kurum bazlı hassasiyetleri kategorize

ederek hangi hassas bilgi türünün ne kadar süre[78] ile kapalı kalacağına yönelik bir sınıflama cetveli yayınlamalıdır.

3. Millî gizlilik derecelerinin üçlü düzeyde sınıflandırılması, gizli veya hassas belgelerin bağlamlarına göre farklılaşabileceğinden, mevcut derecelendirme yaklaşımlarının yeniden değerlendirilmesi gerekmektedir. Bu kapsamda, gizlilik derecelerinin daha az hassastan daha hassasa doğru bir sıralama ile (Örneğin H1, H2..., H10) belirlenmesi, aynı zamanda belgelerin kapatma sürelerini de etkileyebilecektir. Bu durum, belgenin bağlam unsurlarına bağlı olarak olası zararını ve dolayısıyla hassasiyetini, aynı gizlilik derecesi sınıflamasında eşit şekilde değerlendirilmesini engellemektedir. Örneğin, uluslararası ilişkiler konusunda, bir ülkenin diplomatik görüşmelerine ilişkin bir belgenin ifşası, iki devlet arasında kriz yaratabilecek kritik bir duruma yol açabilir. Ancak aynı gizlilik derecesine sahip, bir ticaret anlaşmasının genel detaylarını içeren bir belge, daha az hassas kabul edilebilir. Bu sebep aynı gizlilik derecesine sahip belgelerin bağlamlarına göre farklılaşan bir derecelendirme anlayışı gerekmektedir.
4. Hizmete özel gizlilik derecesine sahip – elektronik ortamda – hassas belgeler, başka bir bilgi ile birleştirildiğinde veya zamanla gizli ya da çok gizli nitelikteki belgelerle örtüştüğünde, gizlilik derecesi yükseltilebilir. Buna karşın, gizli veya çok gizli belgelerin zamanla hassasiyetlerinin azalması da söz konusu olabilir. Bu durumda, belgelerin fiziksel veya elektronik ortama aktarılması ve dolaşımlarının kontrol edilerek hibrit bir yönetim modelinin uygulanması gerekmektedir. Ayrıca, tanımlama ve erişim durumlarına etki eden bu yönetim anlayışına yönelik planlamaların yapılması önemlidir. Bununla birlikte DAB ulusal arşivde gizliliği

[78] Kapatma sürelerine ilişkin olarak daha önce anılan Devlet Sırrı Kanun Tasarısı örneğine benzer bir yaklaşım dikkate alınabilir. Süreye ilişkin belirsizliklerin bulunduğu veya herhangi bir sınırlamanın öngörülmediği durumlarda, periyodik değerlendirme sürelerinin belirlenmesi önerilmektedir.

düşürülen, yükseltilen veya kaldırılan belgelere yönelik olarak istatistiksel ve betimsel verileri paylaşması gerekmektedir. Nitekim gizlilik dereceli belgelere yönelik olarak sadece kaldırma işleminin uygulanması ve bu durumun DAB gizlilik yönergesinde de belirtilmesi 2022 yılında yayınlanan gizlilik yönetmeliği çerçevesine uygun değildir. Mevzuata uygun yönetsel faaliyetlerin DAB başta olmak üzere gözden geçirilerek ilgili düzenlemelerin yeniden yapılandırılması gerekmektedir.

5. Türkiye'de belge ve arşiv yönetiminde denetleyici ve yönlendirici bir misyona sahip olan DAB, kamu kurumlarına yönelik hassas bilgilerin yönetimi konusunda yol gösterici kılavuzlar yayınlamalıdır. Bu kılavuzlar her konu için (tespit, erişim sınırlama, kapatma, transfer vb.) ayrı ayrı düzenlenmelidir. Örneğin, hassas bilgi içeren belgelere erişim sınırlaması amacıyla redaksiyon işlemlerinin nasıl yapılması gerektiğine dair (TNA *redaction toolkit* örneğinde olduğu gibi) ayrıntılı bir kılavuz oluşturulmalıdır. Ayrıca Türkiye'de dijital belgelerin arşive transferi/devri konusunda gerçekleşmiş bir faaliyet bulunmamaktadır. Hassas bilgi içeren kamu belgelerinin devri, diğer belgelere göre farklı uygulamalar gerektireceğinden, bu konuda kamu kurumlarını aydınlatıcı kılavuzlar hazırlanmalıdır. Oluşturulan kılavuzlar iş ve işlemler için uygulama adımları sunan genel bir yapıda olmalıdır.
6. DAB, Türkiye'de hassas bilgi içeren belgelere yönelik bir kamu yararı testi[79] oluşturmalıdır. Bu test, bilginin kamusal yararı ile gizlilik gerektiren unsurlar arasında denge kurarak, hangi belgelerin hangi düzeyde erişime açılabileceğine dair objektif bir değerlendirme mekanizması sunmalıdır. Özellikle BEHK kapsamında, DAB ve diğer kamu kurumlarına yapılan başvuruların açıklığının

[79] Kamu yararı testi, gizlilik ve şeffaflık arasında bir denge kurarak, bilgi paylaşımının kamu yararına olup olmadığını değerlendirme işlemidir. Kamu yararı testine örnek olarak İngiltere Bilgi Komiserliği Ofisi detaylı bilgiler sunmaktadır. Bkz. https://ico.org.uk/for-organisations/foi/freedom-of-information-and-environmental-information-regulations/the-public-interest-test/

sağlanması ve bu başvuruların standart hale getirilmesi, kamu yararı testi ile kamusal şeffaflığı ve hesap verebilirliği artıracaktır.

7. İş süreçlerinin verimliliğini artırmak amacıyla, teknoloji destekli değerlendirme araçlarının tasarlanması gerekmektedir. Özellikle hassasiyet değerlendirme süreçlerinde, yapay zekâ araçları belirli işlemleri otonomlaştırarak veya otomasyona bağlı hale getirerek çeşitli çözümler sunmaktadır. Bu araçlar, hassasiyetlerin öğretildiği yapay zekâ uygulamaları sayesinde, zamana bağlı olarak hangi durumlarda hassasiyetin meydana geleceğini, kapatılan veya sınırlandırılan belgelerin ne zaman erişime açılacağını ve hangi belgelerin ilişkili diğer konular veya belgelerle bir araya geldiğinde hassasiyet kazanacağını öngörebilir. Aynı zamanda, bilgi edinme hakkı taleplerinin hassasiyet değerlendirmesinden geçirilmesi gibi işlemlerde hız ve tutarlılık kazanarak zaman ve maliyet avantajı sağlayacaktır. Kamuda kullanılacak teknoloji destekli değerlendirme araçları, merkezi ve kural tabanlı bir yaklaşımla tasarlanmalıdır. Bu araçlar kamu yönetişimi çerçevesinde gelecek geribildirimlere ve zaman içinde yapılacak güncellemelere açık olacak şekilde geliştirilmelidir.
8. DAB çatısı altında, denetleyici ve politika geliştirici yetkiye sahip, bağımsız bir danışma kurulu oluşturulmalıdır. Bu kurulda, başta arşiv uzmanlığı olmak üzere farklı uzmanlık alanlarına sahip, geniş kurum temsiliyeti sağlayabilecek, teknoloji konusunda donanımlı ve yenilikçi üst düzey sivil nitelikte kişiler yer almalıdır. Böyle bir yapı, kamu arşivlerinin yönetiminde etkili kararlar alınmasını ve güncel teknolojiye uyumlu politikalar geliştirilmesini sağlayacaktır. Bununla birlikte kurumların gizlilik değerlendirme komisyonları[80] ulusal arşive transfer öncesi gerekli hallerde hukukî desteğe başvurmalıdır.

[80] "Çok Gizli Gizlilik Dereceli Belgeleri Değerlendirme Komisyonu" ve "Gizli ve Hizmete Özel Gizlilik Dereceli Belgeleri Değerlendirme Komisyonu" üç kişiden oluşur. Bu kişiler, üst yönetici veya yetkili yönetici, belgeyi üreten birimin yöneticisi ve bir personeldir. Komisyon, sınırlı sayıda kişiden oluşması ve gizli bilgileri içermesi nedeniyle, üyelerinin niteliklerinde çeşitlilik sağlanamamaktadır.

9. Hassasiyet değerlendirme sürecinin bir tür risk yönetimi olması, katılımcı ve iş birliğine dayalı çözümler geliştirilmesini zorunlu kılmaktadır. Bu doğrultuda, kurum gizlilik değerlendirme komisyonları ile ulusal arşiv danışma kurullarının gerekli durumlarda koordinasyon sağlaması ve birimler arası bilgi akışı ile iş birliğini artırması gerekmektedir. İş birliğine yönelik çevrimiçi kataloglarda, kullanıcılardan gelecek öneri ve uyarıların alınması, sürecin doğru bir şekilde yürütülmesine ve olası hataların giderilmesine katkı sağlayacaktır.
10. Araştırma kapsamında incelenen ulusal arşivlerin kataloglarında olduğu gibi DAB, BETSİS üzerinden erişime kapalı belgeler hakkında bilgi sağlamalıdır. Tamamen kapatılmaması gereken belgelere çeşitli sınırlama teknikleri uygulanarak erişimin önü açılmalıdır. Ayrıca, BEHK aracılığıyla yapılan erişim başvurularında kamuoyunu aydınlatacak şekilde hesap verebilir ve şeffaf bir yaklaşım benimsenmelidir.
11. Değerlendiricilere, kararlarını daha bilinçli vermelerine yardımcı olmak amacıyla fayda sağlayabilecek uyarılar ve bilgilendirmeler[81] sunulmalıdır. Gizlilik değerlendirme komisyonları ve değerlendiriciler tarafından, her belge özelinde dikkate alınacak bir kontrol ve tanımlama listesi oluşturulmalıdır. Bu listeye yönelik örnek bir yaklaşım Tablo 18'de sunulmuştur. Buna göre değerlendiriciler, hassas içerik kontrolüne yönelik sorular doğrultusunda belgeleri incelemeli ve tespit ile karar süreçlerini yürütmelidir. Ayrıca, daha önce sunulan (IV. Bölüm) arşiv kataloglarında olduğu gibi, tanımlama[82] alanlarının eksiksiz doldurulması ve

[81] Hassasiyet değerlendirmesi sürecinde, değerlendiricilere belgeyi okumadan önce içerdiği olası hassasiyetler hakkında bilgi verilmesinin, kararlarını daha hızlı almalarını sağlayacağı düşüncesi McDonald (2019, s. 153) tarafından ifade edilmektedir.

[82] Oluşturulan Kontrol ve Tanımlama Listesi'nde yer alan üst veri alanları, hem örnek kataloglarda hem de daha önce anılan ISAD-G standardına uyumlu bir yaklaşım sergilemektedir.

belge içeriğinin ilişkili olduğu hukuki düzenlemelere[83] atıfta bulunulması gerekmektedir.

Tablo 18. Hassasiyet Değerlendirmesi Kontrol ve Tanımlama Listesi[84]

Kontrol ve Tanımlama Listesi
A. Bu belge Kişisel Verilerin Korunması Kanunu'nun (KVKK) ve diğer[85] yükümlü mevzuat düzenlemelerinin belirtmiş olduğu özel nitelikli kişisel/hassas kişisel veri içeriyor mu?
B. Bu belge başka bir belge/veri ile birleştirildiğinde hassasiyet meydana gelir mi? Gizlilik derecesinde bir değişiklik olur mu?
C. Bu belge bir kişiye, gruba veya kuruma zarar, hasar, utanç veya itibar zedenlenmesine sebep olabilir mi?
D. Bu belgeye uygun gizlilik derecesi (elektronik ve fiziksel ortam bakımından uygun derece) seçildi mi?
E. Hassas Bilgi İçermesi Durumunda;
1. Hangi türde hassas bilgi içermektedir?
2. KVKK ve diğer yükümlü mevzuat düzenlemelerinden hangi özel nitelikli/hassas veriye işaret etmektedir?
F. Erişim Kısıtlamaları Tercih Edilmesi Durumunda;
Sınırlı Erişim • Redaksiyon • Maskeleme

[83] Özellikle EBYS'lerde gizli ve/veya hassas bilgi içerikli belgelere yönelik üst veri alanının olmaması ve zorunlu tutulmaması hangi kanunun hangi maddesine göre tespit işleminin yapıldığını belirsiz kılmaktadır (Cengiz-Mater, 2022, s. 63). Bu durum gerek anahtar kelime araması yolu ile tespitini gerekse devir sonrası erişim uçlarının eksik kalmasına sebep olmaktadır.

[84] Kontrol ve Tanımlama Listesine dair iş akışı Şema 3'te görselleştirilmiştir.

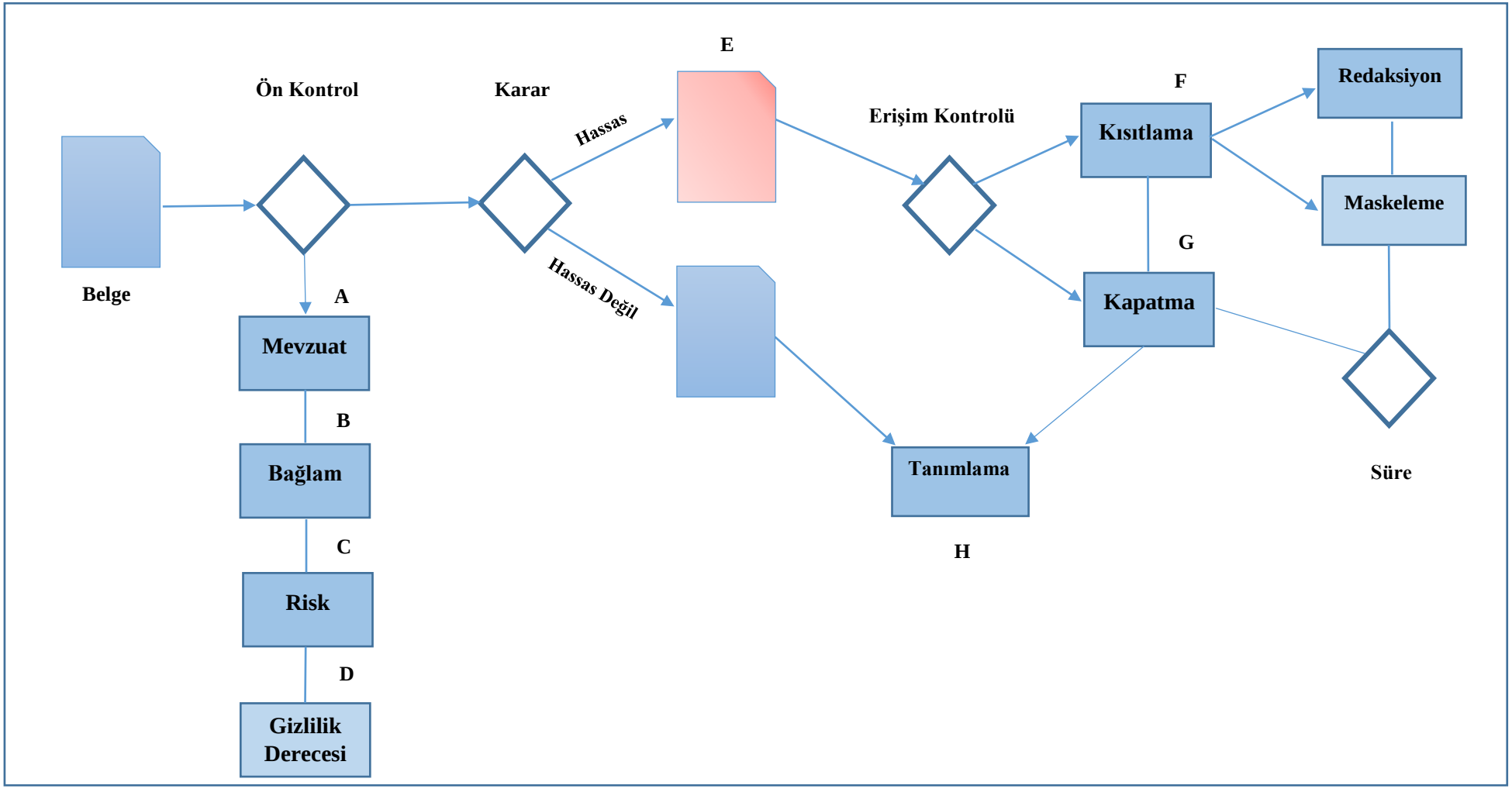
[85] Bu konudaki diğer yükümlü düzenlemeler: Türk Ceza Kanunu, Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ve Bilgi Edinme Hakkı Kanunu'dur.

G. Kapatma Kararı Alınması Durumunda;

- Süreli
    - Ne kadar süre kapalı kalacak? (Mevzuata göre)
- Süresiz

H. Tanımlama

1. Fon/koleksiyon ve seri bilgisi:
2. Üst veri ve özet bilgisi:
3. Üretim tarihi:
4. Format türü:
5. Gizlilik derecesi:
6. Erişim durumu:
7. Yasal durum:
8. Değerlendirici:
9. Değerlendirme tarihi:
10. Tekrar değerlendirme tarihi:
11. Erişime açılma tarihi:
12. Not:



Şema 3. Hassasiyet Değerlendirmesi Kontrol ve Tanımlama İş Akış Şeması

12. Özellikle hassas bilgi dolaşımının yoğun olduğu kamu kurumları başta olmak üzere, tüm kurumlarda "Hassas Bilgi İçerikli Belgelerin Değerlendirme, Arşivleme ve Devir Süreçleri" konulu hizmet içi eğitim planlamalarının yapılması ve bu eğitimlerin, DAB tarafından hazırlanacak politika ve kılavuzlar doğrultusunda verilmesi gerekmektedir. Bu bağlamda, uluslararası hukukî düzenlemeleri dikkate alması gereken Dışişleri Bakanlığı gibi kurumlara yönelik mevzuat bilgilendirmeleri ayrı bir öneme sahiptir.
13. 11 sayılı Cumhurbaşkanlığı Kararnamesinde, anılan [Bütünleşik Arşiv Yönetim Sistemi (BAYS) Projesi kapsamında gerçekleştirilecek] "Devlet Arşiv Ağı" ve "Devlet Arşiv Veri Merkezi" (4/h, 4/ı) uygulamaları, kamu kurumlarının hassas bilgilerini yönetme noktasında standardizasyonun sağlanması ve ilişkili belge yapısının oluşturulması açısından büyük önem taşımaktadır. Hazırlık aşamasındaki BAYS yazılımının, kamu belgelerinde gizlilik konusunu "Tanımlama ve Kontrol" Modülü altında yer alan "gizlilik türü" ve "hassas içerik" üst veri alanları aracılığıyla ele alması planlanmaktadır.[86] Bununla birlikte söz konusu sistemlerin teknoloji destekli araçlarla entegre edilmesi, belgelerin daha verimli bir şekilde sınıflandırılması, izlenmesi ve erişilmesi için genel bir altyapı sağlanması faydalı olacaktır. Nitekim kamu kurumlarının transfer edeceği belgelerin BAYS yazılımında DAB tarafından önizleme ve onay süreçlerine tabi tutulması, özellikle gizlilik dereceli belgeler için sağlama (*accession*) ve geri/kesin iade (*deaccession*) işlemlerinin kontrollü bir şekilde yürütülmesine olanak sağlayacaktır. Böylece, kamu kurumları arasında denetimli bir şekilde, ortak dil, uygulama birliği ve standartlar çerçevesinde gizli ve hassas bilgi yönetimi etkin bir şekilde gerçekleştirilebilir.

[86] BAYS projesi ile ilgili verilen bilgiler 11.12.2024 tarihinde DAB ile yapılan görüşmeler doğrultusunda elde edilmiştir.

Hassasiyet değerlendirmesi, yüksek risk ve çeşitli zorluklar içeren bir süreçtir. Yapılan araştırmalar, çözüm olarak gelecek çalışmaların dijital araçların bu süreçlere olan katkılarına odaklanılması gerektiğini ortaya koymaktadır. Hassas belgelerin, ilgili uzmanlığa sahip değerlendiricilere yönlendirilmesi, değerlendirme önceliklerinin hassasiyete göre belirlenmesi ve geçmiş değerlendirmelere dayalı yönlendirmelerin sistematik araçlarla desteklenmesi, sürecin doğru ve hızlı bir şekilde yönetilmesine katkı sağlayabilir. Bu doğrultuda, Türkiye'deki araştırmacıların, dijital araçların veri yönetimi, bilgi güvenliği ve gizlilik ilkeleriyle entegrasyonunu derinlemesine incelemeleri önemlidir. Yapay zekâ ve makine öğrenmesi gibi yeni nesil teknolojilerin hassasiyet değerlendirmesinde nasıl etkili olabileceği ile blokzincir gibi araçların veri güvenliği ve izlenebilirlik üzerindeki potansiyeli araştırılmalıdır. Hassasiyet değerlendirmesi Türkiye'deki araştırmacılar için henüz derinlemesine keşfedilmemiş bir çalışma alanıdır. Bu alanda literatürdeki tartışmalar genellikle makine öğrenmesi algoritmalarına odaklanmakta olup, dijital dönüşüm sürecine dair yeni sınıflandırma ve analiz yöntemlerinin geliştirilmesi üzerinde durmaktadır. Ayrıca, ulusal arşivleme sistemleri, dijital yedekleme çözümleri ve bulut tabanlı veri güvenliği gibi pratik uygulamalara yönelik çalışmalar, Türkiye'nin dijital arşivleme altyapısını güçlendirecek ve küresel bilgi güvenliği standartlarıyla uyum sağlayacaktır. Bu tür araştırmalar, yerel ve uluslararası düzeyde bilgi yönetimi ve gizlilik politikalarının daha etkin bir şekilde uygulanmasına katkı sunacaktır.

Son olarak dijital araçların ve yenilikçi teknolojilerin hassasiyet değerlendirmesi süreçlerine entegrasyonu, Türkiye'nin bilgi yönetimi kapasitesini artıracak ve küresel düzeyde rekabetçi bir konum elde etmesine yardımcı olacaktır. Bu bağlamda, dijital dönüşüm sürecinin güçlendirilmesi, sadece güvenlik ve verimlilik sağlamakla kalmayacak, aynı zamanda ulusal ve uluslararası düzeyde daha etkin bir veri yönetimi sağlanmasına da katkıda bulunacaktır.

KAYNAKÇA

Act on Data Protection and the Processing of Personal Data (2018). Erişim adresi: https://www.personuvernd.is/media/uncategorized/Act_No_90_2018_on_Data_Protection_and_the_Processing_of_Personal_Data.pdf

Act Regulating Archives Containing Personal Data from Medical Records (2016). Official Gazette of the Republic of Slovenia, No. 85/16. Erişim adresi: https://www.gov.si/assets/organi-v-sestavi/Arhiv-RS/Angleska-stran/Zakonodaja/ZAGOPP-2016_ang.pdf

Ajayi, O. O. ve Adebiyi, T. O. (2014). Application of Data Masking in Achieving Information Privacy. *IOSR Journal of Engineering*, 4(2), 13-21.

Al-Fedaghi, S. (2007). How sensitive is your personal information? *Proceedings of the 2007 ACM Symposium on Applied Computing* içinde (s. 165-169), New York: Association for Computing Machinery.

Allan, A. (2014). *Records Review*. London: Cabinet Office

Altunışık, R., Boz, H., Gegez, E., Koç, E., Sığrı, Ü., Yıldız, E. ve Yüksel, A. (2022). Sosyal Bilimlerde Araştırma Yöntemleri: Yeni Perspektifler. Ankara: Seçkin Yayıncılık.

American Board for Certification in Homeland Security. (2016). Sensitive Security Information, Certified (SSI) Body of Knowledge. CRC Press.

Andrews, P. M. (1998). Changing Attitudes in Government to Record Closures. *Journal of the Society of Archivists,* 19(1), 17-24.

Arşiv Terimleri (2023). Hazırlayanlar Fatih Rukancı, Hakan Anameriç ve Alparslan Başar. İstanbul: Devlet Arşivleri Başkanlığı.

Arşivlerden Yararlanma Usul ve Esasları Hakkında Yönetmelik. *T.C. Resmî Gazete* (2.10.2021 -31616)

Association of Canadian Archivists (2017). Association of Canadian Archivists Code of Ethics and Professional Conduct. Erişim adresi: https://www.archivists.ca/Policies-and-Codes

Association of Records Managers and Administrators. (2007). Glossary of Records and Information Management Terms (3. Baskı). Lenexa KS: ARMA International.

Australia Privacy Act. (1988). https://www.oaic.gov.au/_old/assets/about-us/access-our-information/foi-disclosure-log/foireq20-00051.pdf

Baron, J. R., Sayed, M. F. ve Oard, D. W. (2022). Providing more efficient access to government records: a use case involving application of machine learning to improve FOIA Review for the deliberative process privilege. *ACM Journal on Computing and Cultural Heritage* (JOCCH), 15(1), 1-19.

Baron, J. R., Rollings N. W. ve Oard, D. W. (2023). Using ChatGPT for the FOIA Exemption 5 Deliberative Process Privilege. In Proceedings of the 3rd International Workshop on Artiicial Intelligence and Intelligent Assistance for Legal Professionals in the Digital Workplace held in Conjunction with the 19th International Conference on Artiicial Intelligence and Law içinde (s. 32-48). CEUR Workshop Proceedings.

Bartliff, Z., Kim, Y. ve Hopfgartner, F. (2024). Towards Privacy-Aware Exploration Of Archived Personal Emails. *International Journal on Digital Libraries*, 1-35.

BBC Türkçe. (2025, Ocak 9). Edward Snowden'ın ifşa ettiği ABD Ulusal Güvenlik Ajansı'nın gizli belgeleri. Erişim adresi: https://www.bbc.com/turkce/articles/cgr608rdd42o

Belen-Saglam, R., Nurse, J. R. C. ve Hodges, D. (2022a). An investigation into the sensitivity of personal information and implications for disclosure: A UK

perspective. Frontiers in Computer Science, 4. https://doi.org/10.3389/fcomp.2022.908245

Belen-Saglam, R. B., Nurse, J. R. ve Hodges, D. (2022b). Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications*, 66, 103163. https://doi.org/10.1016/j.jisa.2022.103163

Belge Yönetimi ve Arşiv Terimleri Sözlüğü. (2009). Hazırlayanlar: H. Sekine Karakaş, Fatih Rukancı ve Hakan Anameriç. Ankara: T. C. Başbakanlık Devlet Arşivleri Genel Müdürlüğü.

Berardi, G., Esuli, A., Macdonald, C., Ounis, I. ve Sebastiani, F. (2015). Semi-automated text classification for sensitivity identification. *Proceedings of the 24th ACM International on Conference on Information and Knowledge Management* içinde (s. 1711-1714), New York: Association for Computing Machinery.

Berg, B. L. ve Lune, H. (2019). Sosyal Bilimlerde Nitel Araştırma Yöntemleri (4. baskı). Konya: Eğitim Yayınevi.

Bilgi Edinme Hakkı Kanunu. *T.C. Resmî Gazete* (24.10.2003 -25269).

Birleşmiş Milletler Genel Sekreterlik Bülteni. (2007/6). Information Sensitivity, Classification and Handling. Erişim adresi: https://hr.un.org/content/information-sensitivity-classification-and-handling

Birleşmiş Milletler Geliştirme Grubu. (2017). Data Privacy, Ethics and Protection. Guidance Note on Big Data for Achievement of the 2030 Agenda. Erişim adresi: https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf

Birleşmiş Milletler. (2024a). Veri Koruma ve Gizlilik Yasaları. Erişim adresi: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Birleşmiş Milletler. (2024b). Understanding Information Sensitivity. Archives and Records Management Section. Erişim adresi:

https://archives.un.org/sites/archives.un.org/files/RM-Guidelines/quick_reference_information_sensitivity.pdf

Borden, B. B. ve Baron, J. R. (2016). Opening up dark digital archives through the use of analytics to identify sensitive content. *IEEE international conference on big data içinde* (s. 3224-3229). IEEE.

Branting, K., Brown, B., Giannella, C., Guilder, J. V., Harrold, J., Howell, S. ve Baron, J. R. (2023). Decision support for detecting sensitive text in government records: Anonymous submission. *Artificial Intelligence and Law*, 1-27.

Braun, V. ve Clarke, V. (2019). Psikolojide tematik analizin kullanımı. S. N. Şad, N. Özer ve A. Atli (Çevirenler). *Eğitimde Nitel Araştırmalar Dergisi – Journal of Qualitative Research in Education,* 7(2), 873-898.

Brown, C. (2018). Archival Futures. London: Facet Publishing.

Bulut, M. (2020). Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler. *Ankara Barosu Dergisi*, 78(3), 99-150.

Califonia Privacy Right Act. (2020). Erişim adresi: https://thecpra.org/

Canada Access to Information Act. (2024). Erişim adresi: https://laws-lois.justice.gc.ca/eng/acts/A-1/

Canada Privacy Act. (2023). Erişim adresi: https://laws-lois.justice.gc.ca/eng/acts/P-21/

Cengiz Mater, E. (2022). Dijital Çağda Doğuştan Dijital Belgelerin Bilgi Yönetim Süreçleri: Kurumdan Arşive Giden Yol (Doktora Tezi). Marmara Üniversitesi, Türkiyat Araştırmaları Enstitüsü, İstanbul.

Centel, N. ve Zafer, H. (2008). Ceza Muhakemesi Hukuku. İstanbul: Beta Basım Yayım.

Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun. *T.C. Resmî Gazete* (12.03.2024 -32487).

Cook, T. (1991). The Archival Appraisal of Records Containing Personal Information: A RAMP Study with Guidelines. General Information Programme and UNISIST United Nations Educational, Scientific and Cultural Organization Paris: Unesco.

Cook, T. (2011). 'We are what we keep; we keep what we are': archival appraisal past, present and future. *Journal of the Society of Archivists*, 32(2), 173-189.

Colorado Privacy Act. (2023). Erişim adresi: https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf

Connecticut Data Privacy Act. (2023). Erişim adresi: https://portal.ct.gov/AG/Sections/Privacy/The-Connecticut-Data-Privacy-Act

Cox, R. ve Samuels, H. (1988). The archivist's first responsibility: A research agenda to improve the identification and retention of records of enduring value. *The American Archivist, 51*(1-2), 28-42.

Čtvrtník, M. (2021). Closure periods for access to public records and archives. Comparative-historical analysis. *Archival Science,* 21(4), 317-351.

Council of European. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Erişim adresi: https://www.coe.int/en/web/conventions/

Council European. (2000). Recommendation No. R (2000) 13 of the Committee of Ministers to member states on a European policy on access to archives. Erişim adresi: https://rm.coe.int/16804cea4f

Council of European. (2001). Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows. Erişim adresi: https://rm.coe.int/1680080626

Council of European. (2009). Council of Europe Convention on Access to Official Documents. Erişim adresi: https://rm.coe.int/1680084826

Creswell, J. W. (2013). *Nitel Araştırma Yöntemleri Beş Yaklaşıma Göre Nitel Araştırma ve Araştırma Deseni* (Çev. Edt. Mesut Bütün ve Selçuk Beşir Demir, 3. Baskıdan Çeviri). Ankara: Siyasal Kitabevi.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2020). Bilgi Ve İletişim Güvenliği Rehberi. Erişim adresi: https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf

Çakır, K. (2012). 5237 Sayılı Türk Ceza Kanunu'nda Gizliliğin İhlali Suçu ve Ceza Muhakemesi Hukuku İle İlişkisi. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 18(1), 227-266.

Devlet Arşivleri Başkanlığı 2023 Yılı Faaliyet Raporu. Erişim adresi: https://www.devletarsivleri.gov.tr/varliklar/goruntuler/haberler/image/idarefaaliyetraporu.pdf

Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi. (11 Sayılı Kararname). *T.C. Resmî Gazete* (16.7.2018 -30480).

Devlet Arşiv Hizmetleri Hakkında Yönetmelik. *T.C. Resmî Gazete* (18.10.2019 -30922).

Devlet Sırrı Kanun Tasarısı (2008). Erişim adresi: http://www2.tbmm.gov.tr/d24/1/1-0484.pdf

Dressler, V. ve Kearns, J. (2023). Probing archivists' perceptions and practices in privacy. *Archives and Records*, 44(2), 175-201.

Elliot, M., Mackey, E. ve O'Hara, K. (2020). The Anonymisation Decision-making Framework (2. baskı). UKAN Manchester.

Entrikin, J. L. (2020). Family Secrets and Relational Privacy: Protecting Not-So-Personal, Sensitive Information, *University of Miami Law Review*, 74, 781-897.

Eroğlu, Ş. ve Külcü, Ö. (2014). TS 13298 Çerçevesinde Kurumsal Bilgi Sistemleri ve Elektronik Belge Yönetimi Standartlarının Değerlendirilmesi: İçişleri Bakanlığı Örneği. *Bilgi Dünyası*, 15(2), 327-352.

Etzioni, A. (2014). A cyber age privacy doctrine: More coherent, less subjective, and operational. *Brooklyn. Law Review,* 80 (4), 1263-1308.

European Archives Group. (2018). Guidance on Data Protection for Archive Services. Erişim adresi: https://commission.europa.eu/system/files/2018-10/eag_draft_guidelines_1_11_0.pdf

European Commission. (2014). *Factsheet on the "right to be forgotten" ruling. Erişim adresi:*http://ec.europa.eu/justice/dataprotection/files/factsheets/factsheet_data_protection_en.pdf

European Parliament. (2016). Regulation (EU) (2016) 2016/679 of the European Parliament and of the Council of 27 April on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union.

European Parliament and Council. (2001). Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. Erişim adresi: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32001R1049

Federal Act on Data Protection. (2023). Erişim adresi: https://www.fedlex.admin.ch/eli/cc/2022/491/en

Federal Act on Archiving. (2023). https://www.fedlex.admin.ch/eli/cc/1999/354/en#art_7%20VE%20https://www.fedlex.admin.ch/eli/cc/1999/371/en#art_6

Federal Archives Strategy 2021-2025. Erişim adresi: https://www.bar.admin.ch/bar/en/home/about-us/the-federal-archives/strategy.html

Fule, P. ve Roddick, J. F. (2004). Detecting privacy and ethical sensitivity in data mining results. *Proceedings of the 27th Australasian conference on Computer science-Volume içinde* (s. 159-166), Dunedin: Australian Computer Society.

Geng, L., You, Y., Wang, Y. ve Liu, H. (2011). Privacy Measures For Free Text Documents: Bridging The Gap Between Theory and Practice. *Trust, Privacy and Security in Digital Business: 8th International Conference Proceedings içinde* (s. 161-173). Berlin Heidelberg: Springer.

Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik. *T.C. Resmî Gazete* (26.4.2022 -31821).

Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik Kılavuzu. (2022). Erişim adresi: https://www.tccb.gov.tr/resmiyazisma/gizlilik-kilavuzu/

Gollins, T., McDonald, G, Macdonald, C. ve Ounis, I. (2014). On using information retrieval for the selection and sensitivity review of digital public records. Proceeding of the 1st International Workshop on Privacy-Preserving IR: When Information Retrieval Meets Privacy and Security içinde (s. 39-40), Gold Coast, Australia. Erişim adresi: http://ceur-ws.org/Vol-1225/pir2014_submission_9.pdf

GOV. UK. (2021). Ethics, Transparency and Accountability Framework for Automated Decision-Making. Erişim adresi: https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making

Greene, M. ve Meissner, D. (2005). More Product, Less Process: Revamping Traditional Archival Processing. *The American Archivist*, 68(2), 208-263.

Güler, A., Halıcıoğlu, M. B. ve Taşğın, S. (2015). Sosyal Bilimlerde Nitel Araştırma (2. baskı). Ankara: Seçkin Yayıncılık.

Henkoğlu, T. (2015). Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi (Doktora Tezi). Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Henttonen, P. (2017). Privacy as an Archival Problem and a Solution. *Archival Science*, 17(3), 285-303.

IFLA-ICA Statement on Privacy Legislation and Archiving (2020). Erişim adresi: https://www.ifla.org/publications/ifla-ica-statement-on-privacy-legislation-and-archiving/

Information Commissioner's Office (2022). Special category data. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/

International Council on Archives. (1996). Code of Ethics. Erişim adresi: https://www.ica.org/resource/ica-code-of-ethics/

International Council on Archives. (1999). ISAD(G): General International Standard Archival Description (Second Edition). Erişim adresi: https://www.ica.org/resource/isadg-general-international-standard-archival-description-second-edition/

International Council on Archives. (2012). Principles of Access to Archives. Committee On Best Practices And Standards Working Group On Access. Erişim adresi: https://www.ica.org/sites/default/files/ICA_Access-principles_EN.pdf

Italian Personal Data Protection Code. (2003). Erişim adresi: https://www.privacy.it/archivio/privacycode-en.html

Jaillant, L. (2022a). More Data, Less Process: A User-Centered Approach to Email and Born-Digital Archives. *The American Archivist,* 85(2), 533-555.

Jaillant, L. (2022b). How can we make born-digital and digitised archives more accessible? Identifying obstacles and solutions. *Archival Science*, 22(3), 417-436.

Jaillant, L. ve Rees, A. (2023). Applying AI to digital archives: trust, collaboration and shared professional ethics. *Digital Scholarship in the Humanities*, 38(2), 571-585.

Johns, R. (2017). Appraisal and Disposal. Erişim adresi: https://silo.tips/embed/04-appraisal-and-disposal.html?sp=0

Johnson, C., Badger, L., Waltermine, D., Snyder, J. ve Skorupka, C. (2016). Guide to Cyber Threat Information Sharing, NISTS Special Publication, 800(150).

Kaya, C. (2011). Avrupa birliği veri koruma direktifi ekseninde hassas (kişisel) veriler ve işlenmesi. *Journal of Istanbul University Law Faculty*, 69(1-2), 317-334.

Kaymak, A. ve Külcü, Ö. (2024). Kamusal Bilgi ve Veri Yönetimi Politikaları Çerçevesinde Gizli ve Özel Güvenlik Gerektiren Belgelerin Yönetimi. İstanbul: Hiperyayın.

Kaczmarek, J. ve West, B. (2018). Email preservation at scale: Preliminary findings supporting the use of predictive coding. International Conference on Digital Preservation (iPRES). Erişim adresi: https://osf.io/yau3c

Keskin, İ. (2012). Türkiye İçin Bir Arşiv Kanunu Yazmak: Bir Model Önerisi. *Arşiv Dünyası,* (13), 5-19.

Kılınç, D. (2012). Anayasal bir hak olarak kişisel verilerin korunması. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 61(3), 1089-1172.

Kindt, E. J. (2016). *Privacy and Data Protection Issues of Biometric Applications*. New York: Springer.

Kişisel Verileri Koruma Kanunu. *T.C. Resmî Gazete* (7.4.2016 -29677).

Kişisel Verileri Koruma Kurumu. (2019). Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü. Ankara: KVKK Yayınları.

Lee, C. A. ve Woods, K. (2012). Automated redaction of private and personal data in collections. Editörler Luciana Duranti eve Elizabeth Shaffer, *In The Memory of the World in the Digital Age: Digitization and Preservation*. İçinde (s. 298-313). Vancouver: UNESCO.

Lemieux, V. L. ve Werner, J. (2024). Protecting Privacy in Digital Records: The Potential of Privacy-Enhancing Technologies. *ACM Journal on Computing and Cultural Heritage*, 16(4), 1-18.

Library and Archives Canada. (2024). Restrictions on viewing and copying material. Erişim adresi: https://library-archives.canada.ca/eng/services/public/using-lac-material/material-restrictions/pages/material-restrictions.aspx

Martin, K. ve Nissenbaum, H. (2017). Privacy interests in public records: An empirical investigation. *Harv. JL & Tech.*, 31, 111-125.

Mathers, J. (2000). Providing access to sensitive records: the Personal History Index (PHIND). *Archives and Manuscripts*, 28(2), 58-70.

Melik, J. ve Košir, M. (2013). Sensitive Archives. *Atlanti*, Özel Sayı, 129-136.

Mexico Federal Law on Protection of Personal Data Held by Private Parties (2010). Erişim adresi: https://www.duanemorris.com/site/static/Mexico_Federal_Protection_Law_Personal_Data.pdf

McCardwell, K. (2014). Intellectual Propoerty Concerns in Undocumented Corporate Collections – *Case Studies in Archival Ethics*. Chicago: Society of American Archivist.

McCarville, J. (2004). Balancing Access and Privacy in Archives: New Challenges in the Face of Canadian Privacy Legislation, *Feliciter* 50(4), 149–53.

McCullagh, K. (2007). Data sensitivity: proposals for resolving the conundrum. *Journal of International Commercial Law and Technology*, 2 (4), 190-201

McDonald, G., Macdonald, C., Ounis, I. ve Gollins, T. (2014). Towards a classifier for digital sensitivity review. Advances in Information Retrieval: 36th European Conference on IR Research, ECIR 2014, Amsterdam, The Netherlands, April 13-16, 2014. Proceedings içinde (s. 500-506). Springer International Publishing.

McDonald, G., García-Pedrajas, N., MacDonald, C. ve Ounis, I. (2017). A study of SVM kernel functions for sensitivity classification ensembles with POS sequences. *Proceedings of the 40th international ACM SIGIR Conference on Research and Development in Information Retrieval içinde* (s. 1097-1100), Newyork: ACM.

McDonald, G., Mcdonald, C. ve Ounis, I. (2017). Enhancing sensitivity classification with semantic features using word embeddings. Editörler Joemon M. Jose, Claudia Hauff, Ismail Sengor Altıngovde, Dawei Song, Dyaa Albakour, Stuart Watt, and John Tait. In *Advances in Information Retrieval: 39th European Conference on IR Research, Proceedings içinde* (s. 450-463). Springer International Publishing.

McDonald, G., MacDonald, C. ve Ounis, I. (2018a). Active learning strategies for technology assisted sensitivity review. *European Conference on Information Retrieval* içinde (s. 439-453). Cham: Springer International Publishing.

McDonald, G., Macdonald, C. ve Ounis, I. (2018b). Towards maximising openness in digital sensitivity review using reviewing time predictions. In *European Conference on Information Retrieval* içinde (s. 699-706). Cham: Springer International Publishing.

McDonald, G, MacDonald, C. ve Ounis, I. (2019). The FACTS of Technology-Assisted Sensitivity Review. Erişim adresi: https://arxiv.org/pdf/1907.02956.pdf

McDonald, G. (2019). A Framework For Technology-Assisted Sensitivity Review: Using Sensitivity Classification to Prioritise Documents for Review (Doktora Tezi) School of Computing Science College of Science and Engineering University of Glasgow. New York, USA: ACM.

McKechnie, J. ve McDonald, G. (2024). SARA: A Collection of Sensitivity-Aware Relevance Assessments. arXiv preprint arXiv:2401.05144.

Moss, M. S. ve Gollins, T. J. (2017). Our Digital Legacy: An Archival Perspective. *Journal of Contemporary Archival Studies*, 4(2), 3.

NARA Bulletin. (2014-04). Format Guidance for the Transfer of Permanent Electronic Records. Erişim adresi: https://www.archives.gov/records-mgmt/bulletins/2014/2014-04.html

NARA Bulletin. (2020-02). Guidance on Scheduling the Early and Late Transfer of Permanent Records. Erişim adresi: https://www.archives.gov/records-mgmt/bulletins/2020/2020-02

NARA Strategic Plan 2022-2026. (2022). Erişim adresi: https://www.archives.gov/about/plans-reports/strategic-plan/strategic-plan-2022-2026

Narvala, H., McDonald, G. ve Ounis, I. (2022a). Sensitivity review of large collections by identifying and prioritising coherent documents groups. In *Proceedings of the*

31st ACM International Conference on Information & Knowledge Management içinde (s. 4931-4935).

Narvala, H., Mcdonald, G. ve Ounis, I. (2022b). The role of latent semantic categories and clustering in enhancing the efficiency of human sensitivity review. *Proceedings of the 2022 Conference on Human Information Interaction and Retrieval* içinde (s. 56-66). https://doi.org/10.1145/3498366.3505824

Narvala, H. (2024). Identifying Latent Relationship Information in Documents for Efficient and Effective Sensitivity Review (PhD Thesis). School of Computing Science College of Science and Engineering, University of Glasgow.

National Archives of Estonia. (2024). Frequently Asked Questions. Erişim adresi: https://www.ra.ee/vau/index.php/en/helpdesk/faq/index?dialog=0

National Records of Scotland. (2019). Access to High Court record. Erişim adresi: https://www.nrscotland.gov.uk/files//record-keeping/legislation/nrs-foi-request-foi-19-00595-access-to-high-court-record-1935-jc26-1935-45.pdf

National Records of Scotland. (2021). Guidance to the Form and Content of the Model Records Management Plan. Erişim adresi: https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/Guidance_Document_v2.0_-_21_February_2024.pdf

NATO Act Personal Information and Privacy Protection Directive (2022). Erişim adresi: https://www.act.nato.int/wp-content/uploads/2023/05/rfi022059-privacy-directive.pdf

Naugler, H. (1984). The Archival Appraisal of Machine- Readable Records: A RAMP Study with Guidelines. General Information Programme and UNISIST United Nations Educational, Scientific and Cultural Organization Paris: Unesco.

Nettleton, D. F. ve Abril, D. (2014). An Information Retrieval Approach to Document Sanitization. Advanced Research in Data Privacy içinde (s. 151-166). Cham: Springer International Publishing.

OECD. (2002). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Publishing, Paris, https://doi.org/10.1787/9789264196391-en.

OECD. (2013). The OECD Privacy Framework. Erişim adresi: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

OECD. (2021). Report on the Implementatıon of the Recommendatıon Of The Councıl Concernıng Guıdelınes Governıng the Protectıon of Prıvacy and Transborder Flows of Personal Data. Erişim adresi: https://one.oecd.org/document/C(2021)42/en/pdf

Ohm, P. (2014). Sensitive information. Southern California Law Review, 88(5), 1125-1196. Erişim adresi: https://ssrn.com/abstract=2501002

Ordinance to the Federal Act on Archiving. (2024). Erişim adresi: https://www.fedlex.admin.ch/eli/cc/1999/371/en

Özdemir, L. (2009). The National Archives and the Lord Chancellor's Advisory Council on National Records and Archives in the freedom of information era. *Journal of the Society of Archivists*, 30(2), 137-145.

Özdemir, L. (2019). The inevitability of digital transfer: How prepared are UK public bodies for the transfer of born-digital records to the archives?. *Records Management Journal*, 29(1/2), 224-239.

Özdemir, L. ve Cengiz, E. (2019). Türk Kamu Sektöründe Dijital Süreklilik Ne Kadar Mevcut: Teorik Bir Çerçeve. Editörler Bahattin Yalçınkaya, M. Altay Ünal, Burcu Yılmaz ve Fahrettin Özdemirci. *Bilgi Yönetimi ve Bilgi Güvenliği: e-Belge-*

eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ içinde (273-294). Ankara: Ankara Üniversitesi Bilgi Yönetim Sistemleri Belgelendirme ve Bilgi Güvenliği Merkezi.

Özkan, O. (2020). Kişisel Verilerin Korunması (Yüksek Lisans Tezi). Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Parlar, A. ve Hatipoğlu, M. (2008). 5271 Sayılı Ceza Muhakemesi Kanunu Yorumu. Ankara: Yayın Matbaacılık, 1.

Patton, M. Q. (2018). Nitel Araştırma ve Değerlendirme Yöntemleri (3. bs. Çeviri). Ankara: Pegem Akademi.

Pearce-Moses, R. (2005). *A Glossary of Archival and Records Terminology*. Chicago, IL: The Society of American Archivists.

Personal Information Protection and Electronic Documents Act. (2000). Erişim adresi: https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf

Personal Information Protection Law of the People's Republic of China. (2021). Erişim adresi: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

Peterson, T. H. (2007). Attitudes and access in the United States of America. Japan-US Friendship Association Seminar 9-11 Mayıs 2007 Tokyo, Japan içinde (s. 1-8). Chicago: Society of American Archivists. Erişim adresi: https://www2.archivists.org/sites/all/files/11_Trudy_PETERSON.pdf

Presidência da RepúblicaSecretaria-Geral Subchefia para Assuntos Jurídicos. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD). Erişim adresi: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Ponemon Institute. (2017). 2017 Cost of Data Breach Study. Research Report. Erişim adresi: https://documents.ncsl.org/wwwncsl/Task-Forces/Cybersecurity-Privacy/IBM_Ponemon2017CostofDataBreachStudy.pdf

Poole, A. H. (2020). An ethical quandary that dare not speak its name: Archival privacy and access to queer erotica. *Library & Information Science Research*, 42(2), 101020.

Photopoulos, C. (2011). Managing catastrophic loss of sensitive data: A guide for IT and security professionals. Burlington: Elsevier.

Proteccion De Los Datos Personales (2000). Erişim adresi: https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

Protection of Documents and Archives and Archival Institutions Act (2014). Official Gazette of the Republic of Slovenia, No. 30/06 and 51/14 Erişim adresi: https://www.gov.si/assets/organi-v-sestavi/Arhiv-RS/Angleska-stran/Zakonodaja/PDAAIA-2014.pdf

Public Record Office. (2022). A guide to accessing 'closed' records. Erişim adresi: https://www.gov.im/media/1377168/20220725-accesstoclosedrecords-v1-2.pdf

Pugh, M. J. (1992). Providing Reference Services for Archives and Manuscripts. Chicago: The Society of American Archivists.

Quinn, P. ve Malgieri, G. (2021). The difficulty of defining sensitive data—The concept of sensitive data in the EU data protection framework. *German Law Journal*, 22(8), 1583-1612.

Ranade, S. (2018). Access Technologies for the Disruptive Digital Archive. Edt. Caroline Brown. Archival Futures içinde (s. 79-98). London: Facet Publishing.

Redwine, G., Barnard, M., Donovan, K., Farr, E., Forstrom, M., Hansen, W., John, J. L. Kuhl, N., Shaw, S. ve Thomas, S. (2013). Born digital: Guidance for donors, dealers, and archival repositories. Washington: Council on Library and Information Resources.

Reed, B. (2014). Reinventing Access. *Archives and Manuscripts*, 42 (2), 123-132.

Rukancı, F., Anameriç H. ve Başar, A. (2021). *Arşiv ve Arşivcilik: Kuram, Strateji ve Uygulamalar*. İstanbul: Türkiye Cumhuriyeti Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı Yayınları.

Rukancı, F., Anameriç H. ve Başar, A. (2023). *Bellek Yönetimi: Arşivsel Dönüşüm ve Paradigma.* Ankara: Türkiye Cumhuriyeti Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı Yayınları.

Rules for Archival Description. (2008). Bureau of Canadian Archivists (revised version – July 2008). Ottawa, Canada. Erişim adresi: https://archivescanada.ca/wp-content/uploads/2022/08/RADComplete_July2008.pdf

Rumbold, J. M. ve Pierscionek, B. K. (2018). What are data? A categorization of the data sensitivity spectrum. *Big data research*, 12, 49-59.

Saldana, J. (2019). Nitel Araştırmacılar İçin Kodlamanın El Kitabı, 3.bs (Çev. Aysel Tüfekçi Akcan ve Süleyman Nihat Şad). Ankara: Pegem Akademi.

Sánchez, D., Batet, M. ve Viejo, A. (2012). Detecting sensitive information from textual documents: an information-theoretic approach. In *Modeling Decisions for Artificial Intelligence: 9th International Conference Proceedings 9* içinde (s. 173-184). Berlin Heidelberg: Springer.

Sayed, M. F. (2021). Search Among Sensitive Content (Doctoral Thesis). Faculty of the Graduate School of the University of Maryland.

Schneider, J., Adams, C., DeBauche, S., Echols, R., McKean, C., Moran, J. ve Waugh, D. (2019). Appraising, processing, and providing access to email in contemporary literary archives. *Archives And Manuscripts*, 47(3), 305-326.

Sesigür, E. (2023). Devlet Arşivlerinde Araştırma Hizmetlerinin Yapılandırılması (Doktora Tezi). Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Sillitoe, P. J. (1998). Privacy in a Public Place: managing public access to personal information controlled by archives services. *Journal of the Society of Archivists*, *19*(1), 5-15.

Simitis, S. (1999). Revisiting sensitive data. Erişim adresi: https://rm.coe.int/16806845af%3E

Sloyan, V. (2016). Born-Digital Archives at the Wellcome Library: Appraisal And Sensitivity Review Of Two Hard Drives. *Archives and Records*, 37(1), 20-36.

Society of American Archivist. (2011). SAA Core Values Statement and Code of Ethics. Erişim adresi: https://www.concernedhistorians.org/content_files/file/et/231.pdf

Society of American Archivists. (2020). SAA Code of Ethics. Society of American Archivists, tarafından Şubat 2005'de onaylandı; Ocak 2012 ve Ağustos 2020'de gözden geçirildi. Erişim adresi: https://www2.archivists.org/statements/saa-core-values-statement-and-code-of-ethics

Society of American Archivists. (2024). Dictionary of Archives Terminology. Erişim adresi: https://dictionary.archivists.org/index.html

Stein, Z. G. (2021). Privacy in Public Archives: Managing Personally Identifiable Information in Special Collections. *RBM: A Journal of Rare Books, Manuscripts, and Cultural Heritage*, *22*(2), 85.

Summary of Annual FOIA Reports for Fiscal Year 2022. US Department of Justice. Erişim adresi: https://www.justice.gov/oip/page/file/1581856/dl?inline=

Şişman, N. (2019). Mahremiyet, Hayatın Sırları ve Sınırları. İstanbul: İnsan Yayınları.

TBMM. 2023 Yılı Bilgi Edinme Genel Raporu. Erişim adresi: https://cdn.tbmm.gov.tr/TbmmWeb/Pdf/Bilgi_Edinme_Kurul_Rapor/2023_Y%C4%B1l%C4%B1_Bilgi_Edinme_Genel_Raporu.pdf

T.C. Anayasası. *T.C. Resmî Gazete* (9.11.1982 – 17863).

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *KSÜ Doğa Bilimleri Dergisi*, 11(1), 132-137.

The National Archives. (2012). Disposal scheduling. Erişim adresi: https://cdn.nationalarchives.gov.uk/documents/information-management/sched_disposal.pdf

The National Archives. (2015). Access to public records. Erişim adresi: https://cdn.nationalarchives.gov.uk/documents/information-management/access-to-public-records.pdf

The National Archives. (2016). The Application of Technology-Assisted Review to Born-Digital Records Transfer, Inquiries and Beyond. Erişim adresi: www.nationalarchives.gov.uk/documents/ technology-assisted-review-to-born-digital-records-transfer.pdf

The National Archives. (2018). Guide to archiving personal data. Erişim adresi: https://cdn.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf

The National Archives. (2019a). Personal information: a guide for justification wording. Erişim adresi: https://cdn.nationalarchives.gov.uk/documents/information-management/personal-information-justification.pdf

The National Archives. (2019b). Procedures for closure on transfer. Erişim adresi: https://cdn.nationalarchives.gov.uk/documents/information-management/procedures-for-closure-on-transfer.pdf

The National Archives. (2021a). Access at transfer – Sensitivity Review Overview. Erişim adresi: https://cdn.nationalarchives.gov.uk/documents/information-management/access-at-transfer-sensitivity-review-overview.pdf

The National Archives. (2021b). Closure periods. Erişim adresi: https://cdn.nationalarchives.gov.uk/documents/information-management/closure-periods.pdf

The National Archives. (2022). Redaction Toolkit: Editing exempt information from paper and electronic documents prior to release. Erişim adresi: https://cdn.nationalarchives.gov.uk/documents/information-management/redaction_toolkit.pdf

The National Archives. (2023). Sensitivity Review. Erişim adresi: https://www.nationalarchives.gov.uk/information-management/manage-information/public-inquiry-guidance/sensitivity-review/

The National Archives. (2024). Step 3: Sensitivity review records. Erişim adresi: https://www.nationalarchives.gov.uk/information-management/manage-information/digital-records-transfer/digital-transfer-steps/step-3-sensitivity-review/

Thompson, E. D. ve Kaarst-Brown, M. L. (2005). Sensitive information: A Review and Research Agenda. *Journal of the American Society for Information Science and Technology*, 56(3), 245-257.

Tipton, H. F. (1998). Purposes of Information Security Management. *Handbook of Information Security Management.* CRC Press.

Tough, A. G. (2018). The Scope and Appetite for Technology-Assisted Sensitivity Reviewing of Born-Digital Records in a Resource Poor Environment: A Case Study From Malawi. Editör P. Ngulube. *Handbook of Research on Heritage Management and Preservation* içinde (s. 175-182). Hershey: IGI Global.

Transportation Security Administration. (2008). TSA Management Directive No. 3700.4 Handling Sensitive Personally Identifiable Information. Erişim adresi: https://www.tsa.gov/sites/default/files/foiareadingroom/handling_sensitive_personally_identifiable_information_3700.4.pdf

TSE K 523. (2016). Bilgi Varlıklarının Gizlilik Derecelerine Göre Sınıflandırılması Kriteri. Ankara: TSE.

TS 13298. (2015). Elektronik Belge ve Arşiv Yönetim Sistemi Standardı. Ankara: TSE.

Türk Ceza Kanunu. *T.C. Resmî Gazete* (12.10.2004 – 25611).

Türk Medeni Kanunu. *T.C. Resmî Gazete* (22.11.2001 – 24607).

UNESCO. (2023). A Steady Path Forward: UNESCO 2022 Report on Public Access to Information (SDG 16.10.2).). Paris: UNESCO Publishing.

Virginia Consumer Data Protection Act. (2023). Erişim adresi: https://www.oag.state.va.us/consumer-protection/files/tips-and-info/Virginia-Consumer-Data-Protection-Act-Summary-2-2-23.pdf

Yeo, G. (2018). Can We Keep Everything? The Future Of Appraisal in a World Of Digital Profusion. Edt. Caroline Brown. Archival Futures içinde (s. 45-64). London: Facet Publishing.

Yıldırım, A. ve Şimşek, H. (2021). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri* (12. baskı). Ankara: Seçkin Yayıncılık.

Wacks, R. (1989). *Personal Information: Privacy and the Law*. Oxford: Clarendon Press.

Wang, M. ve Jiang, Z. (2017). The defining approaches and practical paradox of sensitive data: An investigation of data protection laws in 92 countries and regions and 200 data breaches in the world. *International Journal of Communication*, 11, , 3286–3305.

Wadsworth, C., Vera, F. ve Piech, C. (2018). Achieving fairness through adversarial learning: an application to recidivism prediction. arXiv preprint arXiv:1807.00199.

Whorley, T. M. (2006). The Tuskegee Syphilis Study: Access and Control over Controversial Records (Doktora Tezi). University of Pittsburgh. The School of Information Sciences.

Whyte, J. ve Walsh, T. (2024). "Carefully and Cautiously": How Canadian Cultural Memory Workers Review Digital Materials for Private and Sensitive Information. *The Canadian Journal of Library and Information Practice and Research*, 19(1), 1-26.

EKLER

EK 1: Etik Kurul İzni

T.C
ANKARA ÜNİVERSİTESİ REKTÖRLÜĞÜ
Etik Kurulu Başkanlığı

17.07.2024

Sayı : 85434274-050.04.04 / 1444722
Konu : Etik Kurul Kararı

Sayın Hasan ÖZTÜRK

İlgi: 07.06.2024 tarihli başvurunuz.

"Hassas Bilgi İçerikli Belgelerin Değerlendirme Süreci" başlıklı tez çalışması ile ilgili olarak Ankara Üniversitesi Etik Kurulunun 05/07/2024 tarihli toplantısında alınan 16/187 sayılı kararın bir örneği ilişikte gönderilmektedir.

Bilgilerinizi saygılarımla rica ederim.

Rektör a.
Rektör Yardımcısı

EKLER:
Karar Örneği (1 sayfa)

Ankara Üniversitesi Rektörlüğü 06100 - Tandoğan/ANKARA
Telefon : 0 (312) 212 60 40 / 2085-2183

Ayrıntılı Bilgi İçin

ANKARA ÜNİVERSİTESİ
ALT ETİK KURULU
KARAR ÖRNEĞİ

Karar Tarihi : **05.07.2024**
Toplantı Sayısı : **16**
Karar Sayısı : **187**

187- Üniversitemiz Dil ve Tarih-Coğrafya Fakültesi öğretim üyelerinden **Prof.Dr.Fatih RUKANCI**'nın danışmanlığını yaptığı **Hasan ÖZTÜRK**'ün "Hassas Bilgi İçerikli Belgelerin Değerlendirme Süreci" başlıklı doktora tezi ile ilgili 07.06.2024 tarihli "İnsan Üzerinde Yapılan Klinik Dışı Araştırmalar Başvuru Formu" Etik Kurulumuzca incelendi.

Üniversitemiz Dil ve Tarih-Coğrafya Fakültesi öğretim üyelerinden **Prof.Dr.Fatih RUKANCI**'nın danışmanlığını yaptığı **Hasan ÖZTÜRK'**ün "Hassas Bilgi İçerikli Belgelerin Değerlendirme Süreci" başlıklı doktora tezi ile ilgili araştırma protokolüne uyulması ve etik onay tarihinden itibaren geçerli olması koşuluyla uygulanmasının etik açıdan uygun olduğuna oy birliği ile karar verilmiştir.

ASLININ AYNIDIR
05/07/2024

[redacted]

Ankara Universitesi
Etik Kurulu Başkanı

EK 2: Aydınlatılmış Onam Formu

T.C.

ANKARA ÜNİVERSİTESİ

Aydınlatılmış Onam Formu

Araştırmacı: Hasan Öztürk

Araştırmanın Adı: Hassas Bilgi İçerikli Kamu Belgelerinin Değerlendirilmesi

Sayın gönüllü,

Doktora tezi kapsamında planlanmış olan yukarıda adı yazılı araştırmaya katılmak üzere davet edilmiş bulunuyorsunuz. Bu araştırmada yer almayı kabul etmeden önce, araştırmanın ne amaçla yapılmak istendiğini anlamanız ve kararınızı bu bilgilendirme çerçevesinde özgürce vermeniz gerekmektedir. Aşağıdaki bilgileri lütfen dikkatlice okuyunuz, sorularınız olursa sorunuz ve açık yanıtlar isteyiniz.

Bilgilendirme Bölümü

Çalışmanın Amacı: "Hassas Bilgi İçerikli Belgelerin Değerlendirme Süreci" başlıklı araştırma kapsamındaki amaçlar şu şekildedir:

1- Dünyada ve Türkiye'de veri koruma/gizlilik veya kişisel veri mevzuatında hangi bilgiler hassas olarak nitelendirilmektedir? Bu bilgilerin kapsamı, tespiti ve işlenme koşulları nasıl belirlenmelidir?

2- Hassas bilgi içerikli belgelere yönelik değerlendirme süreci (hassasiyet değerlendirmesi) nasıl yürütülmelidir? Bu süreç fiziksel ve dijital ortama göre farklılık oluşturur mu?

3- Hassasiyet değerlendirmesi sürecinde yaşanan zorluklar nelerdir? Bu zorluklar hangi yöntemler ile çözülebilir?
4- Dijital hassasiyet değerlendirmesi nedir? Dijital araçların/yazılımların hassasiyet değerlendirmesi sürecinde fonksiyonları/katkıları nelerdir? Bu araçlar hassasiyet değerlendirme sürecinde kullanılmalı mıdır?
5- Hassasiyet değerlendirmesi sürecinde danışma/gizlilik kurullarının ve kaynaklarının (rehber, kılavuz, talimatname vs.) rolü ve niteliği ne olmalıdır?
6- Hassasiyet değerlendirmesi konusunda ulusal arşivlerin uygulamaları nelerdir? Türkiye'deki durum nedir? sorularına yanıt bulmak.

Güvence Bölümü:

Bu araştırmada yer almak tümüyle sizin isteğinize bağlıdır. Araştırmada yer almayı reddedebilirsiniz ya da başladıktan sonra yarıda bırakabilirsiniz. Bu araştırmanın sonuçları bilimsel amaçlarla kullanılacaktır. Araştırmadan çekilmeniz ya da araştırmacı tarafından araştırmadan çıkarılmanız halinde, sizle ilgili veriler kullanılmayacaktır. Ancak veriler bir kez anonimleştikten sonra araştırmadan çekilmeniz mümkün olmayacaktır. Sizden elde edilen tüm bilgiler gizli tutulacak, araştırma yayınlandığında da varsa kimlik bilgilerinizin gizliliği korunacaktır.

Onay Bölümü:

Yukarıda yer alan ve araştırmaya başlanmadan önce gönüllülere verilmesi gereken bilgileri içeren metni okudum (ya da sözlü olarak dinledim). Eksik kaldığını düşündüğüm konularda sorularımı araştırmacılara sordum ve doyurucu yanıtlar aldım. Yazılı ve sözlü olarak tarafıma sunulan tüm açıklamaları ayrıntılarıyla anladığım kanısındayım. Çalışmaya katılmayı isteyip istemediğim konusunda karar vermem için yeterince zaman tanındı.

Bu koşullar altında, araştırma kapsamında elde edilen şahsıma ait bilgilerin bilimsel amaçlarla kullanılmasını, gizlilik kurallarına uyulmak kaydıyla sunulmasını ve yayınlanmasını, hiçbir baskı ve zorlama altında kalmaksızın, kendi özgür irademle kabul ettiğimi beyan ederim.

İmza Bölümü

İmza/Tarih:	İmza/Tarih:
Gönüllünün adı-soyadı:	Araştırmacının adı-soyadı:

Ek 3: Yarı Yapılandırılmış Görüşme Formu

Yarı Yapılandırılmış Görüşme Formu

Bartın Üniversitesi Edebiyat Fakültesi Bilgi ve Belge Yönetimi Bölümü'nde araştırma görevlisi olarak görev yapmaktayım. Aynı zamanda Ankara Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı doktora öğrencisiyim. "Hassas Bilgi İçerikli Kamu Belgelerinin Değerlendirilmesi" başlıklı doktora tez çalışması kapsamında hassas bilgi içerikli kamu belgelerinin yönetim ve arşiv süreci, bu süreçte yaşanan zorluklar, hukukî teknolojik yaklaşımlar ortaya konulacaktır. Araştırma sonucunda elde edilen verilerin, Türkiye'de hassasiyet değerlendirmesi sürecine olan farkındalığı artırarak ilgili alandaki gelişmeleri yansıtarak kamudaki bilgi ve belge güvenliğine/gizliliğine katkı sağlayacağı düşünülmektedir.

Bu araştırma kapsamında yapılan tüm görüşmelerden elde edilen veriler, sadece bu araştırmada kullanılacak ve kişisel bilgiler tamamen gizli tutulacaktır.

Görüşmenin yaklaşık 45 dakika süreceği düşünülmektedir. İzniniz olması durumunda zaman ve veri kaybının azaltılması amacıyla görüşme kayıt altına alınacaktır. İzin vermemeniz durumunda lütfen araştırmacıya bilgi veriniz. Görüşmede, sorulara vereceğiniz cevaplar metne aktarıldıktan sonra sizinle paylaşılacaktır. Görüşmeye başlamadan önce sormak istediğiniz bir soru varsa lütfen iletiniz.

Araştırmaya katılmayı kabul ettiğiniz, sunduğunuz destek ve kıymetli vaktinizi ayırdığınız için teşekkür ederim.

Arş. Gör. Hasan ÖZTÜRK

BÖLÜM 1: DEMOGRAFİK SORULAR

1. Adınız soyadınız nedir?

2. Eğitim durumunuz ve alanınız/mesleğiniz? (tamamladığınız eğitim ile birlikte devam ettiğiniz bir eğitim varsa lütfen belirtiniz)

3. Çalıştığınız kurum ve birim? (bu kurumda kaç yıldır çalışıyorsunuz)

4. Meslek hayatınızda kaçıncı yılınızı tamamladınız?

BÖLÜM 2: HASSAS BİLGİ İÇEREN BELGELERİN DEĞERLENDİRİLMESİNE İLİŞKİN SORULAR

1- Gizlilik/koruma veya kişisel veri mevzuatında yer alan hassas bilgi türleri hakkında ne düşünüyorsunuz?

   a) Listelenen türlerin dışında hassasiyet oluşabilir mi?

2- Hassas bilgilerin tanımı, tespiti ve kapsamı konusunda nasıl bir yaklaşım benimsenmelidir?

3- Hassas bilgi içeren kamu belgeleri ve bu belgelerin hassasiyet değerlendirmesi hakkında ne düşünüyorsunuz?

4- Kâğıt ve elektronik belgelerde yer alan hassas bilgilerin değerlendirme süreci nasıl yürütülmektedir?

   a) Farklılıklar var ise hangi yönlerden oluşmaktadır?

5- Hassasiyet değerlendirmesi sürecinde yaşanan/yaşanabilecek zorluklar hakkında ne düşünüyorsunuz?

   a) Kâğıt ve elektronik belgeler için bu zorluklar benzer midir?

6- Hassasiyet değerlendirmesi kişisel bakış açısı ve deneyimden bağımsız objektif olarak nasıl yürütülebilir?

7- Belgelerin zamana göre (zamanla artan veya azalan) hassasiyet kazanması/kaybetmesi konusunda ne düşünüyorsunuz?

a) Zaman konusunda ne gibi bir çözüm üretilebilir?

8- Hassasiyet değerlendirmesi sürecinde, belgenin "bağlamından kaynaklanan" hassasiyet oluşumu konusunda ne düşünüyorsunuz?

9- Belgelerin diğer belgeler ile "ilişki"sinden kaynaklanan hassasiyetler (mozaik hassasiyet) oluşturması konusunda ne düşünüyorsunuz?

a) Bu konuda ne gibi bir önlem alınabilir?

10- Hassasiyet değerlendirmesi sürecinde ulusal arşivler kurumlarında oluşturulan/oluşturulacak danışma/gizlilik kurulları nasıl oluşturulmalı?

a) Bu yapılar hassasiyet değerlendirmesi sürecinde nasıl bir rolü olabilir?

b) Bu yapılar bağımsız olmalı mı?

11- Elektronik belgeler hassasiyet açısından değerlendirilirken yardımcı araçların/yazılımların katkısı hakkında ne düşünüyorsunuz?

12- Dijital hassasiyet değerlendirme araçlarının değerlendirme işlemini otonom (bağımsız/kendiliğinde) olarak gerçekleştirilebilirliği hakkında düşünceleriniz nelerdir?

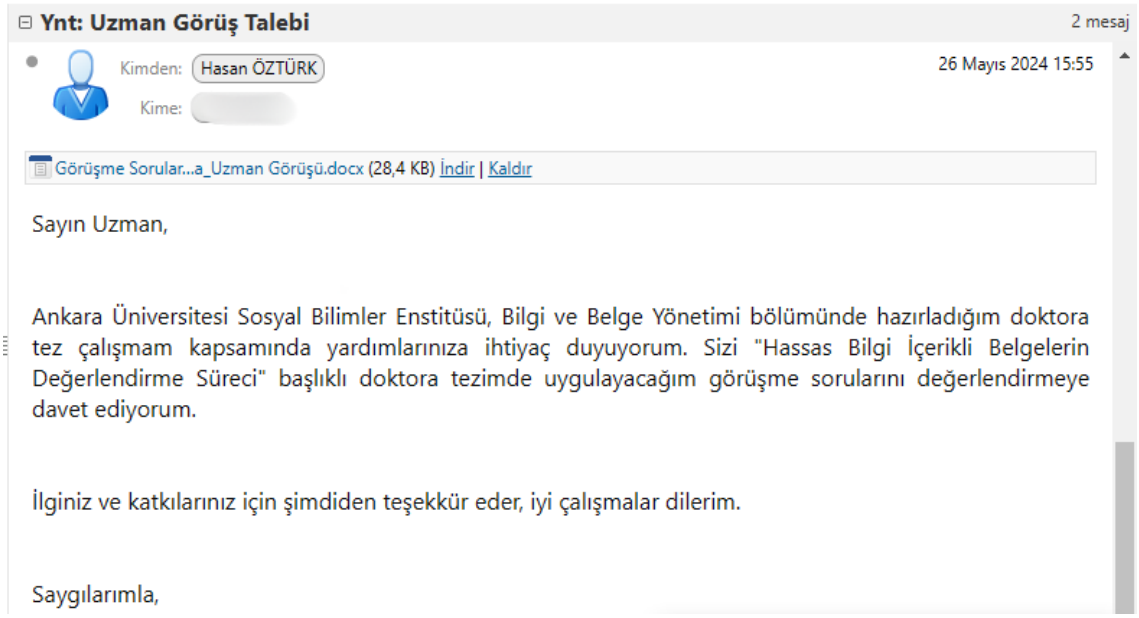
13- Dijital araçların hassasiyet değerlendirmesi sürecinde etik, hukukî sorunlara sebep olabilmeleri hakkında ne düşünüyorsunuz?

14- Hassas bilgi içeren belgelere yönelik bilgi edinme hakkı taleplerine (hacim ve zaman faktörleri doğrultusunda), yardımcı/otomatik araçların katkıları konusunda ne düşünüyorsunuz?

15- Kamu kurumlarında hassasiyet değerlendirmesi sürecinde kılavuz, rehber gibi yardımcı kaynakların kullanılması hakkında ne düşünüyorsunuz?

16- Hassasiyet değerlendirmesi konusunda eklemek istediğiniz bir şey var mı?

Ek 4: Uzman Görüş Daveti Mail Örneği



Ynt: Uzman Görüş Talebi

2 mesaj

Kimden: Hasan ÖZTÜRK

Kime:

26 Mayıs 2024 15:55

Görüşme Sorular...a_Uzman Görüşü.docx (28,4 KB) İndir | Kaldır

Sayın Uzman,

Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Bilgi ve Belge Yönetimi bölümünde hazırladığım doktora tez çalışmam kapsamında yardımlarınıza ihtiyaç duyuyorum. Sizi "Hassas Bilgi İçerikli Belgelerin Değerlendirme Süreci" başlıklı doktora tezimde uygulayacağım görüşme sorularını değerlendirmeye davet ediyorum.

İlginiz ve katkılarınız için şimdiden teşekkür eder, iyi çalışmalar dilerim.

Saygılarımla,

Ek 5: Kod Kitabı

Tema	Kategori	Kod
Hassas Bilgi	**Hassas Bilgi Mevzuatı**	Mevzuat Gerekliliği
		Konulara Göre Sınıflama
		Nesnel Olmayan Sınıflandırma
		Liste dışı hassasiyet oluşumu
		Statiktir
	Hassas Bilgi Kapsamı	Görecelilik
		Kurum Bazlı Sınıflama
		Hem Kamusal Hem Kişisel
		Güncellenebilir Olmalı
		Süreç Tabanlı Belirleme
		Geniştir
	Hassas Bilgi Tespiti	Bağlama duyarlı
		Tanım Esaslı Tespit
		Usul ve Esaslara Göre
		Yardımcı Doküman
		Formattan Bağımsız

Tema	Kategori	Kod
Hassasiyet Değerlendirmesi	**Değerlendirme Yaklaşımı**	Risk Temelli
		Mevzuat Temelli
		Üreten Kurumla İş Birliği
		Kurum Bazlı Yönetim Politikası
		İki Aşamalı Değerlendirme
	Fiziksel ve Dijital Değerlendirme	Benzer Süreç Yönetimi
		Formata Göre Yönetim Farklılığı
		Kâğıt Ortam Daha Kontrolsüz
		Dijital Ortam Daha Kontrolsüz
		Dijital Belge Miktarının Fazlalığı
		Dijital Bilginin Riski Yüksektir
		Dijital Belge İlişkisini Kurmak Zordur
		Yöntemden Bağımsız Risk

Tema	Kategori	Kod
		Bağlam
		Zaman
		Kişisel Bakış

Değerlendirme Zorlukları ve Çözümler	**Süreç Zorlukları**	Mozaik Yapı
		Gizlilik Derecesinin Tanımlanmaması
		Gizlilik Derecesinin Değişmesi
		Hibrit Süreç Yönetimi
		Mevzuat Değişiklikleri
		Dijital Belgelerin Bozulması
		Dosya ve Saklama Planı Yetersizliği
		Farkındalık Eksikliği
		Elektronik Transfer ve Süreç Yönetimi
		Tekrar Eden Kontrol Noktaları
	Objektifliği Sağlamaya Yönelik Çözümler	Görev tanımları ve talimatname
		Mevzuat
		Otomasyon
		Eğitim ve Bilgilendirme
		Görüş alışverişi
	Zamana Yönelik Çözümler	Erişime Kapatma
		Periyodik Değerlendirme
		Süreç Yönetimi
		Belge Üretici Kurum Kararı
	Mozaik Yapıya İlişkin Çözümler	İlişki Kurma
		Kurumlararası Koordinasyon
		İş birlikçi değerlendirme
	Erişime Sunmaya Yönelik Çözümler	Anonimleştirme
		Redaksiyon
		Kriptolu ve yetkilendirilmiş
		Kamu Yararı

Tema	Kategori	Kod
	Yardımcı Araçların Rolü	Anahtar Kelime ile Yakalama
		Hız
		Tutarlılık
		Hacim
		Otomatik sınıflandırma
		Zaman-maliyet faydası
		Daha az güvenilirlik
		Eş ve Yan Anlamlı Kelimelerde Zorlanır
		Terminoloji Değişmesi

Teknoloji Yardımlı Değerlendirme	**Yapay Zekâ**	Bağlam tespiti
		Objektiflik
		Zamana karşı duyarlı
		Otonom işlemler
		Öğrenebilir Olmalıdır
	Otonom Değerlendirme	İnsana Bağlı
		Merkezi Kural Tabanlı
		Yaşam Deneyimi, Sezgi ve Empati
		Doğrulanmalı
	Bilgi Edinme Hakkı Talebi	Gereklilik
		İnsan eliyle etiketleme işlemi yapıldıktan sonra
		Süreci Hızlandırır
	Hukukî, Teknik ve Etik Problemler	Kural Setlerine Bağlı
		Kurum sorumlu
		Sözleşmeye Bağlı
		Hukukî sorumluluk belirsizdir
		Yerli Yazılım

Tema	Kategori	Kod
Danışma Kurulları ve Kaynakları	**Kurulların Yapısı**	Risk Kontrol Sistemi
		Arşiv dışı üst kurul
		Danışma Kurulu
		Bağımsız
		Hem bağımlı hem bağımsız
		Denetleyici
		Politika Üretmeli
	Kişilerin Niteliği	Amprik ve Matematiksel Yaklaşım
		Farklı Disiplin ve Kurum Yöneticilerinden Oluşmalı
		Arşiv Uzmanlığı
		Yeni Nesil Teknoloji Becerisi
		Sivil Olmalı
	Rehber/Kılavuz Oluşturmak	Bilgi ve Tecrübelere Dayalı
		Genel ve Kurum Bazlı
		Kurumlararası İş birliği
		Problem çözer hız artar
		Sistematik ve verimli işleyiş

ÖZET

ÖZTÜRK, Hasan

Hassas Bilgi İçerikli Kamu Belgelerinin Değerlendirilmesi

Doktora Tezi

Danışman: Prof. Dr. Fatih RUKANCI

Kamu belgeleri, ulusal hafızanın korunması ve gelecek nesillere aktarılması açısından hayati bir öneme sahiptir. Bu belgeler; ulusal güvenlik, uluslararası ilişkiler ve bireysel mahremiyet gibi hassas bilgiler içerebileceğinden, arşiv değeri taşıyanların doğru yönetilmesi ve işlemlerin titizlikle yürütülmesi gerekmektedir. Hassasiyet değerlendirmesi olarak adlandırılan bu süreç, hassas/özel nitelikli bilgiler içeren arşiv veya arşivlik belgeleri kapsamaktadır. Türkiye'de uygulamada yer almayan ancak gizlilik kapsamına giren hassasiyet değerlendirmesi, birçok ulusal arşiv kurumu tarafından uygulanmakta olup, temel arşiv işlemlerinden "değerlendirme" (*appraisal*) sürecinin odak noktalarından biridir. Hassas bilgi içeren belgelerin erişim kontrolleri, kısıtlamalar, kapatma kararları ve kamuya erişime açılması, yönetimsel sürecin kritik adımlarıdır. Bu araştırma, hassasiyet değerlendirmesinin kuramsal çerçevesini, uygulama süreçlerini ve karşılaşılan zorlukları incelemeyi amaçlamaktadır.

Araştırmada, ulusal arşivlerin hassasiyet değerlendirmesi faaliyetleri; ilgili mevzuat, kılavuzlar, web siteleri ve kataloglar üzerinden analiz edilmiştir. Ayrıca, yarı yapılandırılmış görüşmeler aracılığıyla uzmanların görüşleri alınarak literatüre farklı bakış açıları kazandırılmıştır. Elde edilen bulgular, hassasiyet değerlendirmesinin önde gelen arşivler tarafından yürütüldüğünü ve sürecin, risk yönetimine dayalı çeşitli zorluklar içerdiğini göstermektedir. Bununla birlikte, hukukî düzenlemelerin yanı sıra yardımcı dokümanlar ve danışma kurullarının sürecin etkinliğinde önemli rol oynadığı belirlenmiştir. Öte yandan, teknoloji destekli değerlendirme yöntemlerinin ve yeni nesil araçların kullanımının giderek daha fazla önem kazandığı anlaşılmaktadır. Bu kapsamda,

araştırmada kamu kurumlarında hassasiyet değerlendirme sürecinde kullanılmak üzere bir kontrol ve tanımlama listesi oluşturulmuştur. Türkiye'de hassasiyet değerlendirmesi sürecine yönelik kapsamlı bir çerçeve sunan bu çalışma, bilgi ve farkındalık eksikliklerinin yanı sıra politika, rehber ve teknolojik altyapı yetersizliklerini de ortaya koymaktadır. Araştırma sonucunda, Türkiye'de hassasiyet değerlendirme sürecinin geliştirilmesine katkı sağlayacak öneriler sunulmuştur.

Anahtar Kelimeler: Hassas Bilgi, Gizlilik, Değerlendirme, Hassasiyet Değerlendirmesi, Değerlendirme Zorlukları, Ulusal Arşivler, Bilgi Edinme Hakkı, Redaksiyon, Anonimleştirme.

SUMMARY

ÖZTÜRK, Hasan

Appraisal of Public Records Containing Sensitive Information

PhD Thesis

Advisor: Prof. Dr. Fatih RUKANCI

Public records play a crucial role in preserving national memory and passing it on to future generations. Since these records may contain sensitive information such as national security, international relations, and individual privacy, it is essential to manage those with archival value properly and carry out processes meticulously. The process known as sensitivity review covers archival or pre-archival records containing sensitive/sensitive personal data. The sensitivity review which falls within the scope of confidentiality but is not implemented in practice in Türkiye, is applied by many national archival institutions and constitutes one of the focal points of the "appraisal" process, a fundamental archival function. Access controls, restrictions, closure decisions, and public availability of records containing sensitive information are critical steps in this administrative process. This study aims to examine the theoretical framework, implementation processes, and challenges of sensitivity review. The research analyzes the sensitivity review activities of national archives through relevant legislation, guidelines, websites, and catalogs. Additionally, semi-structured interviews were conducted to incorporate expert opinions and provide different perspectives to the literature. Findings indicate that sensitivity review is carried out by leading archival institutions and involves various challenges associated with risk management. Furthermore, legal regulations, supporting records, and advisory boards play a significant role in ensuring the effectiveness of the process. On the other hand, the use of technology-assisted review methods and next-generation tools is becoming increasingly important.

Within this scope, the study has developed a control and description checklist to be used in sensitivity review processes within public institutions. Providing a comprehensive framework for sensitivity review in Türkiye, the research highlights deficiencies in knowledge and awareness, as well as shortcomings in policies, guidelines, and technological infrastructure. As a result of the research, recommendations have been proposed to enhance the sensitivity review process in Türkiye.

Keywords: Sensitive information, Confidentiality, Appraisal, Sensitivity review, Appraisal Challenges, National Archives, Right of Access to Information, Redaction, Anonymization