Kamu Belgelerinin Hassasiyet Değerlendirmesi: Kuram, Süreç ve Zorluklar*

Sensitivity Review of Public Records: Theory, Process and Challenges

HASAN ÖZTÜRK**

ÖZ

Kamu belgeleri, ulusal hafızanın korunması ve gelecek nesillere aktarılması için hayati bir önem taşımaktadır. Bu belgeler ulusal güvenlik, uluslararası ilişkiler veya bireysel mahremiyet gibi hassas konular/bilgiler içerebileceğinden arşiv değeri taşıyanların doğru yönetilerek işlemlerin titizlikle yürütülmesi gerekmektedir. Hassasiyet değerlendirmesi olarak adlandırılan bu işlem, hassas/özel nitelikli bilgiler içeren arşiv/arşivlik belgeleri(ni) kapsamaktadır. Türkiye'de uygulama içerisinde yer almayan ancak gizlilik kapsamına giren hassasiyet değerlendirmesi, pek çok ulusal arşiv kurumu tarafından uygulanmakta olup temel arşiv işlemlerinden "değerlendirme (*appraisal*)" sürecinin odak bir safhasıdır. Hassas bilgi içeren belgelerin erişim kontrolleri, kısıtlamalar, kapatma kararları ve kamu erişimine sunulması, çeşitli yönlerden zorlukların oluştuğu bu yönetimsel sürecin adımlarıdır. Bu çalışma, odak bir işlem/adım olan hassasiyet değerlendirmesinin kuramsal çerçevesi, uygulama süreci ve zorlukları üzerine bir inceleme sunmayı amaçlamaktadır.

Anahtar Kelimeler: Hassas bilgi, gizlilik, değerlendirme süreci, hassasiyet değerlendirmesi, değerlendirme zorlukları.

ABSTRACT

Public records are of vital importance for the preservation and transmission of the national memory to future generations. Since these records may contain sensitive information relating to issues such as national security, international relations or privacy, those with archival value should be managed correctly and the procedures should be carried out meticulously. This process, called sensitivity

* Makale geliş tarihi: 7 Haziran 2024, kabul tarihi: 11 Temmuz 2024, araştırma makalesi.
Bu çalışma, adı geçen yazarın Ankara Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi ABD doktora programı kapsamında hazırlanmakta olan doktora tezine dayalı olarak oluşturulmuştur.

** Arş. Gör., Bartın Üniversitesi Edebiyat Fakültesi Bilgi ve Belge Yönetimi Bartın/Türkiye, hozturk@bartin.edu.tr. Doktora Öğrencisi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi ABD Ankara/Türkiye. ORCID

review, covers archive/archival records containing sensitive/personal information. Sensitivity review, which is not in practice in Türkiye but falls within the scope of confidentiality, is applied by many national archive institutions and is a focal stage of the 'appraisal' process, which is one of the basic archive processes. Access controls, restrictions, closure decisions, and public access to records containing sensitive information are steps in this administrative process, which can be challenging in various ways. This study aims to provide a review of the theoretical framework, implementation process and challenges of sensitivity review as a focal process/step.

Keywords: Sensitive information, confidentiality, appraisal process, sensitivity review, appraisal challenges.

Giriş

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.[1] Bilginin gizlilik esaslı olarak değişime ve bozulmaya uğramadan bütünlüğü korunarak yetkili kullanıcı/personel 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 erişimi kısıtlamak gizlilik ilkesine bağlı olarak kamu kurumlarındaki belge yönetimi ve arşiv süreçlerinde uygulanmaktadır. Gizlilik risklerinin yeterince ele alınmaması ve veri ihlallerinin yaşanması, arşivlere ve kamuya olan güveninin zarar görebileceği anlamına gelmektedir.[2] Bu süreçte ayrıca belge içeriğinin ortama bağlı olarak değiştirilme, bozulma, eskime ve tahribata uğramadan bütünlüğünün korunması gerekmektedir.

Kamu belgelerinin çeşitli niteliklerde bilgi taşıması, her bilgi türü için güvenlik düzeyinin farklı önlemler gerektirmesine ve uygulanacak mevzuat, standart ve politikaların seçimine etki etmektedir. Bazı bilgi türleri diğerlerinden daha hassas bir nitelik taşımaktadır.[3] Özellikle bireyler, kurumlar ve uluslararası ilişkileri

1 Harold F. Tipton, *Purposes of Information Security Management* (CRC Press, 1998), s. 1; Mehmet Tekerek, "Bilgi Güvenliği Yönetimi", *KSÜ Doğa Bilimleri Dergisi* C. XI, S. 1 (2008), s. 133; Fatih Rukancı, Hakan Anameriç ve Alparslan Başar, *Arşiv ve Arşivcilik: Kuram, Strateji ve Uygulamalar* (İstanbul: T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı Yayınları, 2021), s. 107.

2 Victoria Lemieux ve John Werner, "Protecting Privacy in Digital Records: The Potential of Privacy-Enhancing Technologies", *ACM Journal on Computing and Cultural Heritage*, C. XVI, S. 4 (2024), s. 3.

3 Amitai Etzioni, "A cyber age privacy doctrine: More coherent, less subjective, and operational", *Brooklyn. Law Review*, C. LXXX, S. 4 (2015), s. 1277.

içeren belgelerin açıklanması durumunda ciddi sonuçlara yol açabilecek olan hassas bilgileri tanımak ve doğru bir şekilde sınıflandırmak gerekir.

Kamu kurumlarında hassas bilgi içeren belgeler bulunmaktadır. Sosyal devlet olmanın bir gerekliliği olarak özellikle vatandaşların doğumundan ölümlerine kadar biriken veriler/belgeler toplanarak arşivlenmektedir. Bu süreçte veri ihlallerinin en az düzeyde tutulması kamu ve kişi haklarının korunmasına yardımcı olacaktır. 2017 yılında IBM (International Business Machine) desteği ile yapılan bir araştırmaya göre, hassas bilgi ihlalinin ortalama maliyeti 3,62 milyon dolardır.[4] Bilgi ihlalinin maddi 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 hassas bilgi içeren belgeler, toplumun güvenliğini sağlamak, vatandaşların haklarını korumak ve kurumları işler kılmak için son derece önemlidir. Bu belgeler, devlet sırları, vatandaşların kişisel bilgileri, ulusal güvenlik konuları ve diğer gizli bilgiler gibi çeşitli hassas bilgiler içerebilir. 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. Bir bilgi türünü hassas yapan nedir? sorusunun cevaplanması kamudaki bilgi güvenliği ve gizliliğinin temin edilmesi için önem arz etmektedir.

Bu çalışma, kamu belgeleri odağında arşivlenecek belgelere uygulanan hassasiyet değerlendirmesi sürecinin adımlarına ve bu süreçte oluşan/oluşabilecek zorluklara odaklanmaktadır. Hassas bilgi olgusu, mevzuata bağlı olarak ait olunan toplumdaki hassasiyet normlarını belirlemektedir. Ancak bu çalışma bir arşiv işlemi/süreci olarak konuyu ele almaktadır.

Hassas Bilgi Kavramı

Hassas (*sensitive*) terimi Türkçe'ye Arapça'dan geçmiş olup duyarlılık 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.[5] 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

4 Ponemon Institute, 2017 Cost of Data Breach Study. Research Report, (2017), s. 1.

5 E. Dale Thompson ve Michelle L. Kaarst-Brown, "Sensitive information: A Review and Research Agenda", *Journal of the American Society for Information Science and Technology*, C. LVI, S. 3 (2005), s. 255.

olan, çoğunlukla kişisel bilgilerden oluşan ve erişilmesi durumunda risk oluşturan bilgilerdir. Hassas bilgiler, özel bir nitelik taşıyan, sınırlı bir erişim veya süreli olarak erişime kapatılması gereken bilgilerden oluşabilmektedir.

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. Hassas olarak tanımlanan bilgiler bahsedilen olumsuzluklar ile birlikte gizlilik kaygısı taşıyan çatı 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.[6]

Hassas bilgiler, doğası gereği bir başkası tarafından bilinme kaygısıyla utanç verici (küçük düşürücü veya aşağılayıcı) olarak görme eğiliminde olunan bilgilerdir. Hassas bilgiler söz konusu olduğunda kişisel veriler ile büyük ölçüde bağlantı kurulup açıklanması hâlinde kişisel verilere göre daha büyük zararlara yol açabilme ihtimali bulunan koruma önceliği olan hukuki varlıklar düşünülmektedir.[7] Bu nedenle, hassas bilgiler yakında tutulma, gizli tutulma veya yalnızca güvenilir sırdaşlara aktarılma eğilimindedir.[8] İzinsiz olarak ifşa edilmesi, erişilmesi veya kullanılması durumunda bir kişiye, gruba veya kuruma zarar, hasar, utanç veren veya ayrımcılığa neden olabilecek bilgiler hassastır.

Hassas bilgi kavramı pek çok farklı şekilde tanımlanmıştır. Hassas bilgiler, yanlış ellerde olması durumunda gizliliği ve güvenliği zarara uğratabilecek bilgiler olarak tanımlanmaktadır.[9] 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.[10] 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.[11]

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.[12] Bu bağlamda

6 Paul J. Sillitoe, "Privacy in a public place: Managing public Access to personal information controlled by archives services", *Journal of the Society of Archivists*, C. XIX, S. 1 (1988), s. 9.

7 Metin Bulut, "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", *Ankara Barosu Dergisi*, C. LXXVIII, S. 3 (2020), s. 124.

8 Paul Ohm, "Sensitive Information", *Southern California Law Review*, C. LXXXVIII, S. 5 (2014), s. 1171.

9 Ohm, "Sensitive Information", s. 1133.

10 Transportation Security Administration, "TSA Management Directive No. 3700.4 Handling Sensitive Personally Identifiable Information" (2008), s. 1.

11 Chris Johnson, Lee Badger, David Waltermire, Julie Snyder ve Clem Skorupka, "Guide to Cyber Threat Information Sharing", *NIST Special Publication*, C. DCCC, S. 150(2016), s. 30.

12 Ohm, "Sensitive Information", s. 1162.

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.[13]

Hassas olarak kabul edilen kategorilerin listesi bir ülkeden diğerine,[14] toplumsal yapı, kültür, inanç[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.[16] 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. Mevzuat düzenlemelerinde "hassas veri" ve "hassas bilgi" terimleri sıklıkla birbirlerinin yerine kullanılmaktadır. Ayrıca benzer bir şekilde "kişisel veri" ya da "kişisel bilgi" kavramları da hukuki düzenlemeler ve bilgi güvenliğine ilişkin literatürde aynı anlamı işaret ederek birbiri yerine kullanılmaktadır.[17] 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 mevzuat düzenlemelerinde hassas veri (*sensitive data*), hassas bilgi (*sensitive information*), özel veri (*private data*), özel kategorideki kişisel veri veya (*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.

Hassas Bilgi İçerikli Belgeler

A Glossary of Archival and Records Terminology sözlüğüne göre[18] potansiyel olarak utanç verici olan, bireylerin gizli tutulmasını bekleyebileceği, kamu denetiminden

13 Sillitoe, "Privacy in a public place: Managing public Access to personal information controlled by archives services", s. 9.

14 Pekka Henttonen, "Privacy as an archival problem and a solution", *Archival Science*, C. XVII, S. 3 (2017), s. 286.

15 Nazife Şişman, *Mahremiyet Hayatın Sırları ve Sınırları*, (İnsan Yayınları, 2019), s. 15.

16 Spiros Simitis, "Revisiting Sensitive Data", (1999), s. 5.

17 Türkay Henkoğlu, "*Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi*", (Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, 2010), s. 18.

18 Richard Pearce-Moses, *A Glossary of Archival and Records Terminology* (Chicago: The Society of American Archivists, 2005), s. 357

korunması gereken yasal, mali veya kişisel nedenlerden dolayı gizlilik içeren bilgiler hassas olarak ifade edilmektedir. Hassas kavramı, gizlilik (*confidential/classified*) kapsamına giren çoğunlukla aynı durumu karşılayan bir terim olarak kullanılmaktadır. Gizlilik, "hukuki, idari, ticari 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.[19] Birçok kamu belgesi çeşitli niteliklerde 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, hukuki süreçlerin izlenmesi ve kamu kurumlarının şeffaflığı açısından kritik bir öneme sahiptir. Mahremiyet, kişisel bilgi içeren belgelere erişim menfaatini korumayı amaçlarken, şeffaflık devlet 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.[20] Kamu belgelerinin genellikle hassas içerikli bilgiler içermesi yaygın olarak kabul edilir.[21] Bir kişi araba kullanmak için ehliyet aldığında, trafik cezası aldığında, oy kullanmak için kayıt yaptırdığında, evlendiğinde ya da boşandığında bir belge düzenlenmektedir. Bir kolluk kuvveti, istihdam amacıyla veya gizli bir pozisyonda kabul edilen bir aday hakkında güvenlik soruşturması yürütebilir. Bu süreçte kamu kurumları tarafından kişilere ait suç geçmişi, tutuklama ve mahkeme kayıtları, eğitim geçmişi gibi belgelerin incelenmesi başta olmak üzere hassasiyet içeren belgeler kurumun faaliyet gösterdiği alana göre muhafaza edilmektedir. Sosyal yardım hizmeti sağlayan başka bir kurum, yardım alanlar ve bağışçılarla ilgili bilgiler içeren belgeler tutmaktadır. Aile toplumun en özel birimi olmasına rağmen, aile üyeleri arasındaki birçok işlem kamu belgelerine konu olmaktadır.

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. Örneğin kurumsal yapı gereği Dışişleri Bakanlığı gibi bir kamu kurumu, ulusal güvenlik, dış ilişkiler,

19 Arşiv Terimleri, haz. Fatih Rukancı, Hakan Anameriç ve Alparslan Başar (İstanbul: Devlet Arşivleri Başkanlığı, 2023), s. 65.

20 Tywanna Marie Whorley, *The Tuskegee Syphilis Study: Access and Control over Controversial Records* (University of Pittsburgh. The School of Information Sciences, 2006), s. 12

21 Ohm, "Sensitive Information", s. 1160.

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.[22] 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. Fotoğraf, resim, harita ve planların da dikkate alınması gerekir. Bir fotoğraf, altyazılarla veya üstveriler 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. Tıbbi 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.[23] Bunun dışında ses örneklerinin de ırksal veya etnik kökeni ortaya çıkarması muhtemeldir. Irk veya etnik kökeni ortaya çıkaran biyometrik verilerin toplanması ve işlenmesinin, etnik ve dinî gerilimlerin hüküm sürdüğü bölgelerde özellikle hassas olmaktadır.[24]

Arşiv belgeleri kaçınılmaz olarak, 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.[25] 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 devlet arşivinde muhafaza

22 Devlet Arşiv Hizmetleri Hakkında Yönetmelik (2019), 4/1.a.

23 The National Archives, "Guide to archiving personal data" (2018), s. 34.

24 Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications* (New York: Springer, 2016), s. 322.

25 Mary Jo Pugh, Providing Reference Services for Archives and Manuscripts (Chicago: The Society of American Archivists, 1992), s. 58.

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.[26] Ancak, kurumlar 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*) hükûmetlere 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.[27]

Güncel ve hassas belgelere erişimde bazı kısıtlamaların olmaması bireylere zarar verebilir.[28] 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 hâlde olduğundan üretim ve kullanım amaçları, yasal dayanakları değerlendirilebilir, birim personeli ve uzman görüşleri alınabilir".[29] 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.

Arşive Giden Adım: Değerlendirme ve Hassasiyet Değerlendirmesi

Belge yönetimi ve arşivcilik terminolojisine göre değerlendirme (*appraisal*), diğer tüm işlevlerin bağlı olduğu, birincil arşiv işlevidir ve bu nedenle dikkatli düşünmeyi gerektirir.[30] Erişim eşittir değerlendirme[31] 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,

26 Rukancı, Anameriç ve Başar, *Arşiv ve Arşivcilik: Kuram, Strateji ve Uygulamalar*, s. 34.
27 IFLA-ICA Statement on Privacy Legislation and Archiving (2020).
28 Jo Pugh, *Providing Reference Services for Archives and Manuscripts* s. 56
29 Rukancı, Anameriç ve Başar, *Arşiv ve Arşivcilik: Kuram, Strateji ve Uygulamalar*, s. 46.
30 Johns, "Appraisal and Disposal", s. 32.
31 Barbara Reed, "Reinventing Access", *Archives and Manuscripts*, C. XLII, S. 2 (2014), s. 127.

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.[32] Değerlendirme yaklaşımları, tüm belgeler için geçerli olmakla birlikte, kabul edilmelidir ki kişisel bilgi içeren veya çeşitli sebeplerden ötürü hassasiyet oluşturan dosyalar bir araya getirildiğinde, [ayrı bir sorundur] ve özel muamele gerektirir.[33] 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. Değerlendirme ve hassasiyet değerlendirmesinin birlikte yapılması önerilmektedir.[34] 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 amacı şu şekildedir:

(a) Herhangi bir bilginin arşiv hizmetine sunulmadan kurumda/birimde tutulup tutulmayacağını değerlendirmek,

(b) Belgeye erişim sınırlaması uygulanacak muafiyet (*exemption*) için transfer sürecinde kapatılıp kapatılmayacağını değerlendirmek,

(c) Sınırlanan bilginin kamu yararına açıklanması gerekip gerekmediğini değerlendirmek ve

(d) Erişim sınırlaması olmayan bilgileri teyit etmektir.[35]

Hassasiyet değerlendirmesi sürecindeki ilk adım, ulusal arşiv kurumlarına devredilmeden/transfer edilmeden önce potansiyel olarak hassas bilgi içeren belge ve belge gruplarının tespit edilmesidir. 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 incelemenin gerekli olmadığına karar verebilir.[36] Kimi 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.[37] Hassasiyet

32 Rukancı, Anameriç ve Başar, *Arşiv ve Arşivcilik: Kuram, Strateji ve Uygulamalar*, s. 45.

33 Terry Cook, *The Archival Appraisal of Records Containing Personal Information: A RAMP Study with Guidelines* (Paris: Unesco, 1991), s. 6.

34 Victoria Sloyan, "Born-Digital Archives at the Wellcome Library: Appraisal And Sensitivity Review Of Two Hard Drives", *Archives and Records*, C. XXXVII, S. 1 (2016), s. 31.

35 The National Archives, "Access to public records", (2015), s. 18.

36 Alex Allan, *Records Review*, (London: Cabinet Office, 2014), s. 14.

37 Graham McDonald, *A Framework For Technology-Assisted Sensitivity Review: Using Sensitivity Classification to Prioritise Documents for Review*, (University of Glasgow, School of Computing Science College of Science and Engineering, 2019), s. 2.

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.[38] 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 çok az sayıda belge vardır ve bu nedenle hassasiyet değerlendirmesine sınırlı olarak ihtiyaç duyulmaktadır. Dolayısıyla bu kurumlardaki hassasiyet değerlendirmesi, belgelerin güncel dönemlerinden ziyade arşivsel değerlendirmenin yürütüldüğü, 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.[39]

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.[40] Değerlendiricinin belge içeriğinde denk geldiği sorun başka bir birimle ilgili olması durumunda, diğer birime danışılır ve incelenmesi için dosyalar gönderilir.[41] Bu kapsamda ulusal arşiv kurumlarında ihtiyaç duyulması hâlinde kurumlar ile hassasiyet konusunda fikir alışverişi yapan, otorite bir danışma kurulunun oluşturulması gerekli olabilir. Bazı ulusal arşiv kurumlarında[42] 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.[43]

38 Sloyan, "Born-Digital Archives at the Wellcome Library: Appraisal And Sensitivity Review Of Two Hard Drives" s. 30; McDonald, *A Framework For Technology-Assisted Sensitivity Review: Using Sensitivity Classification to Prioritise Documents for Review*, s. 52.

39 Lise Jaillant ve Arran Rees, "Applying AI to digital archives: trust, collaboration and shared professional Ethics", *Digital Scholarship in the Humanities*, C. XXXVIII, S. 2 (2023), s. 576.

40 The National Archives, "Access at transfer – Sensitivity Review Overview", (2021a), s. 4.

41 Allan, *Records Review*, s. 15.

42 İngiltere, ABD, Avustralya, İrlanda vb. ülkelerin ulusal arşivlerinde danışma konseyi (*advisory council*), danışma kurulu (*advisory board*) veya danışma komitesi (*advisory committee*) gibi çeşitli uzmanlık alanına sahip kişilerin yer aldığı yapılar oluşturulmaktadır. Bu yapılar gizlilik ve hassasiyet konularında tavsiyelerde bulunmaktadır.

43 The National Archives, "Sensitivity Review", (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[44] 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 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 yayımlanmasının gerekliliği ve veri sahibine sıkıntı veya zarar verme ihtimali gözetilmelidir. Eğer ilgili kişi kendisiyle ilgili bilgiyi kamu malı[45] hâline 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 değerlendirmesiyararlıdır.[46]

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 üstveri bilgisi sağlama amacıyla gerekli olabilir. Ayrıca hassasiyetin derecelere ayrılması (Örneğin: düşük hassasiyet, orta hassasiyet, yüksek hassasiyet), belge üzerinde redaksiyon, maskeleme ve kapatma kararlarının uygulanmasını kolaylaştıracaktır. Gizlilik veya hassasiyet dereceleri-kategorileri hangi düzeyde olursa olsun arşivlerde üzerinde titizlik ve hassasiyet gösterilmesi gereken bir konudur. Nitekim kamu hafızasını oluşturan arşivler, bilgi hizmetlerini sunarken devletin, milletin ve bireylerin mahremiyetine ve çıkarlarına saygı göstermek durumundadır.[47]

44 McDonald, *A Framework For Technology-Assisted Sensitivity Review: Using Sensitivity Classification to Prioritise Documents for Review*, s. 2.

45 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.

46 The National Archives, "Guide to archiving personal data", s. 30-31.

47 Rukancı, Anameriç ve Başar, *Arşiv ve Arşivcilik: Kuram, Strateji ve Uygulamalar*, 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 bir kısıtlama getirmek.[48] Hassas bilgi içeren bir belgenin veya belge grubunu açık tutmak en iyi ihtimalle ihmalkârlık, en kötü ihtimalle de yasa dışı bir durum olduğu ifade edilmektedir. Sadece hassas bilgi içerdiği için belgeleri kaldırmak 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.[49] Bu durum açık devlet anlayışının kabul edildiği demokratik toplumlarda şeffaflık ve hesap verilebilirlik anlayışlarına aykırı olarak ahlaki, etik ya da siyasi 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.[50] 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,[51] imha seçenekler arasında düşünülmemelidir. Amerikan Arşivciler Derneğinin 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.[52] 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.

Arşivciler erişimi yasaklayan/sınırlandıran mevzuat hükümlerinin kontrolünü sağlamak için belgeleri tek tek inceledikten sonra anonimleştirerek, redakte ederek

48 Gabriela Redwine, Megan Barnard, Kate Donovan, Erika Farr, Michael Forstrom, Will Hansen, Jeremy Leighton John, Nancy Kuhl, Seth Shaw ve Susan Thomas, *Born Digital: Guidance for Donors, Dealers, and Archival Repositories* (Washington: Council on Library and Information Resources, 2013), s. 8.

49 Sloyan, "Born-Digital Archives at the Wellcome Library: Appraisal And Sensitivity Review Of Two Hard Drives", s. 30.

50 Henttonen, "Privacy as an archival problem and a solution", s. 298.

51 Naugler Harold, *The Archival Appraisal of Machine-Readable Records: A RAMP Study with Guidelines* (Paris: Unesco, 1984), s. 87.

52 Society of American Archivists, "SAA Code of Ethics. Society of American Archivists", (2020).

veya "sterilize" versiyonlar [hassasiyetten arındırılmış kopya] oluşturarak belgelere tam veya kısmi erişim sağlanıp sağlanamayacağını belirlemelidir.[53] Hassas içerikli belgeler söz konusu olduğunda kısıtlama, süreli veya süresiz kapatma seçenekleri bulunmaktadır. Kısıtlama, belge üzerinde anonimleştirme-maskeleme, redaksiyon, kapatma işlemleri/kararları ve kamu erişimine sunma olarak gerçekleşmektedir.

a. 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 anonimleştirme uygulanması, belge temizleme olarak da ifade edilmektedir. Belge temizleme, belgenin gizliliği korunan bir sürümünü üretmeyi içermektedir. Bu sebeple belge temizleme işlemi için tek tek terimler veya terim dizileri sınıflandırılmalıdır.[54] Hassas verilerin mümkün olduğunca anonimleştirilerek orijinallerin kopyalarının anonimleştirilmiş şekilde sunulması gerekmektedir.[55] Değerlendiricinin böyle bir durumla karşı karşıya kalması durumunda, belge üretici kurumla yüksek hassasiyete sahip veri dosyalarının anonimleştirilmesine yönelik bir prosedür üzerinde çalışması gerekli olabilir.[56] Anonimleştirmenin uygulandığı durumlarda, veri deposunda biri ham diğeri ise kamu kullanımına açık formattaki verileri içeren iki dosyası 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.[57]

Çeşitli anonimleştirme (maskeleme, genelleştirme, rastgeleleştirme vb.) teknikleri bulunmaktadır. Ancak kamu belgeleri üzerinde uygulanacak anonimleştirme işlemi, belgenin provenansı, aidiyeti ve bağlamı üzerinde negatif etkiler

53 Lemieux ve Werner, "Protecting Privacy in Digital Records: The Potential of Privacy-Enhancing Technologies", s. 3.

54 McDonald, *A Framework For Technology-Assisted Sensitivity Review: Using Sensitivity Classification to Prioritise Documents for Review*, s. 67.

55 Mikuláš Čtvrtník, "Closure periods for access to public records and archives. Comparative-historical analysis", Archival Science, C. XXI, S. 4 (2021), s. 324.

56 Naugler, *The Archival Appraisal of Machine-Readable Records: A RAMP Study with Guidelines*, s. 83.

57 Naugler, *The Archival Appraisal of Machine-Readable Records: A RAMP Study with Guidelines*, s. 84; Henttonen, "Privacy as an archival problem and a solution", s. 293.

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 coğrafi 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.

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****...

Tablo 1. *Veri Maskeleme İşlemi*

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[58] yapılması uygun bir seçenektir. Verilerin genel yapısını ve biçimini koruyacak şekilde belirli ayrıntıları gizlemek ve aynı zamanda bilgilerin tanımlanmasını veya kötüye kullanılmasını daha zor hâle 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 uygulanır. Örneğin isimler, adresler, doğum tarihleri, sosyal güvenlik numaraları, finansal hesap bilgileri maskelenebilecek yapılandırılmış türdeki verilerdir. Maskeleme tekniği belge içerisindeki yapılandırılmış

58 Maskelemenin çeşitli türleri olmak ile birlikte başlı başına sayı, harf ve sembol kullanılarak uygulanan bir teknik olduğu bilinmektedir. Bk. Ajayi, Olusola Olajide ve Adebiyi, "Temidayo Olerewaju, Application of data masking in achieving information Privacy", *IOSR Journal of Engineering*, C. IV, S. 2 (2014), 13-21.

veri türleri için uygun bir seçenektir. Bununla birlikte yapılandırılmamış veri ögelerindeki bağlamsal hassasiyetlerin anonimleştirilmesi için doğru bir tercih olmayacaktır. Örneğin siyasi 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 hâle gelecektir.

b. Redaksiyon

"Redaksiyon (*redaction*), 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".[59] Redaksiyon işlemi, anonimleştirmeyi kapsayan bir kavram olmasının yanı sıra farklı olarak belgenin yayımlanmadan önce tek tek kelimelerin, cümlelerin veya paragrafların karartılması ya da sayfaların veya bölümlerin görünmez hâle getirilmesi olarak uygulanmaktadır.[60] Anonimleştirilmesi zor belgelerde redaksiyon kararının alınması, erişim kaybının yüksek olacağına işaret etmektedir. Kurumlar, hassas bilgilerin redakte edilmesi hâlinde belgelerin bazı bölümlerinin yayımlanıp yayımlanamayacağını değerlendirmesini yapacaktır. Bu sebeple redaksiyon için harcanan zaman, bir belgenin tarihi değeri ve mevcut kaynaklarla orantılı olmalıdır.[61]

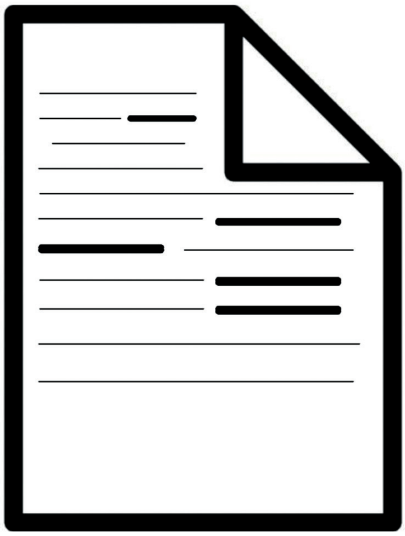
Redaksiyon işlemi, kâğıt veya elektronik belgenin her zaman bir kopyası üzerinde gerçekleştirilmelidir. Orijinal belgeye daha sonra erişim sağlanabilmesi için redaksiyon işleminde kullanılmamalıdır. Redaksiyon, hiçbir zaman metnin veya bilginin bir belgeden tamamen çıkarılmasıyla sonuçlanmamalıdır. Belgede 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 hâle geliyorsa bir belgenin anlamsız hâle gelmesine neden olacak kadar çok bilginin redakte edilmesi gerekiyorsa – belgenin üçten birinden fazlası çıkarılması gerekiyorsa –, belgenin tamamı erişime kapalı olarak muhafaza edilmelidir.[62]

59 Pearce-Moses, *A Glossary of Archival and Records Terminology*, s. 336; Association of Records Managers and Administrators, *Glossary of Records and Information Management Terms* (Lenexa KS: ARMA International, 2007).

60 The National Archives, "Redaction Toolkit: Editing exempt information from paper and electronic documents prior to release", (2022), s. 2.

61 The National Archives, "Procedures for closure on transfer", (2019b), s. 3; The National Archives, "Access at transfer – Sensitivity Review Overview", s. 4.

62 International Council on Archives, "Principles of Access to Archives", Committee On Best Practices And Standards Working Group On Access (2012), s. 11; The National Archives, "Access to public records", s. 29; The National Archives, "Redaction Toolkit: Editing exempt information from paper and electronic documents prior to release" 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'de görüldüğü üzere) redakte edilir. Redaksiyon tamamlandıktan sonra kopyanın kendisi fotokopi hâline 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.[63] Elektronik belgelerde bu işlem yazılım araçları ile sağlanmaktadır. Bununla birlikte elektronik belgenin basılı hâle 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 işlemlerinin bir kombinasyonu yoluyla redakte edilebilir.[64] 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.

63 Zachary G. Stein, "Privacy in Public Archives: Managing Personally Identifiable Information in Special Collections", *RBM: A Journal of Rare Books, Manuscripts, and Cultural Heritage*, C. XXII, S. 2 (2021), s. 8; The National Archives, 2022, s. 9.

64 The National Archives, "Redaction Toolkit: Editing exempt information from paper and electronic documents prior to release", s. 11.

Genel olarak redaksiyon sürecinde belge: anlam kaybı, kamuoyunun muhtemel ilgi düzeyi, harcanan çaba ve hata riski bakımından gözden geçirilmelidir.[65] 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.

c. 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 hâle 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 acces 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.[66] Bu bağlamda hassasiyet değerlendirmesi kavramı, İngiliz Ulusal Arşivleri tarafından hazırlanan "*Access to public records*" başlıklı rehberde belgelerin saklanıp saklanmayacağını ya da erişimin kısıtlanıp kısıtlanmayacağını belirleme süreci olarak tanımlanmıştır.[67] Erişim durumu kısmi sınırlılık olarak belge üzerinde anonimleştirme/maskeleme ve redaksiyon işlemleri ile sağlanır. Ancak belge ve belge gruplarının kısmi 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 üstveri öğesi görünür şekilde tanımlanmalıdır.[68] Örneğin X arşivi/belgesi KVKK'nın [ya da FOIA muafiyetinin] ilgili maddesi gereğince 100 yıl süre ile erişim kapalıdır. Belge içeriği hakkında tam bir açıklama yapılmasa da genel ifadeler ile

65 The National Archives, "Access to public records", s. 28, 29.

66 Lale Özdemir, "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*, C. XXX, S. 2 (2009), s. 138

67 The National Archives, "Access to public records", s. 6

68 The National Archives, "Access to public records", s. 7; Rukancı, Anameriç ve Başar, Arşiv ve Arşivcilik: Kuram, Strateji ve Uygulamalar, s. 169.

tanımlanmalıdır.[69] Bu konuda kurum veya konu esaslı olarak sınıflamalar[70] yapılmaktadır. Eğer belgenin özeti[71] sunulabiliyorsa üstveri alanına eklenmelidir. Araştırmacılar, personel ve ilgililerin belgenin varlığı hakkında bilgi sahibi olabilmesi için üstveri alanının mutlaka var olması gerekir. Hangi bilgi türün veya fon-seri-dosya grubunun ne kadar süre ile kapatılacağına dair zaman cetvelinin[72] 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 belgeleri (*court records*) mutlak suretle 20 yıl kapalı olacağı belirtilmiştir.[73]

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[74] işlemektedir.

d. 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:

69 The National Archives, "Procedures for closure on transfer", s. 6

70 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. Bk. Public Record Office, "A guide to accessing 'closed' records" (2022), s. 2.

71 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.

72 İngiliz 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.

73 The National Archives, "Access to public records", s. 10, 11.

74 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. Bk. The National Archives, "Disposal Scheduling", (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. Bk. National Records of Scotland, "Guidance to the Form and Content of the Model Records Management Plan", (2021), s. 31). 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 bk. https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/practical-methods-for-destroying-documents-that-are-no-longer-needed/

(a) Belgelerin gerçekten var olup olmadığını (doğası gereği yok edilme riski yüksektir) belirlenmek,

(b) Belgede hangi güvenlik/gizlilik derecelerinin veya sınıflandırmaların bulunduğunu ve bunların kısa veya uzun vadeli etkilerinin olup olmadığı değerlendirmek,

(c) Belgede hangi kişisel bilgilerin bulunduğunu ve geçen zaman göz önüne alındığında hâla kapatılıp kapatılmaması gerektiğini 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 yasal 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.[75]

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[76] da bulunmaktadır.

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 yayımlamama, belirlenen kapatma süresinden daha uzun saklama veya doğrudan erişimi aksatma riski kurumların güvenilirlik konusundaki itibarına zarar vermektedir.[77] 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 kararının verilmesi, erişim sınırlamalarının uygulanması

75 Josette Mathers, "Providing access to sensitive records: the Personal History Index (PHIND)", *Archives and Manuscripts*, C. XXVIII, S. 2 (2000), s. 60; The National Archives, "Access to public records", s. 19; The National Archives, "Procedures for closure on transfer", s. 4

76 Belge hassas bilgi içerse bile "önemli kamu yararının" olmasından dolayı erişime sunulması Man Adası Kamu Belgeleri Ofisi için geçerli bir gerekçe olarak listelenmiştir. Bk. Public Record Office, "A guide to accessing 'closed' records", s. 4).

77 Michael Moss ve Tim Gollins, "Our Digital Legacy: An Archival Perspective", *Journal of Contemporary Archival Studies*, C. IV, S. 2 (2017), s. 18-19.

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. Bunun birlikte iş tartışmalarıyla ilgili belgelerde bir çalışanın maaşıyla ilgili ayrıntıların hassas olma olasılığı, politik tartışmalarla ilgili belgelerde politikacıların, maaş ve harcama bilgilerinin bahsedilmesinden 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.[78]

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.[79] 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 hâle getirmektedir. Benzer bir şekilde bir kurum içerisinde yaygın olarak kullanılan bir isim ile nadir bulunan isme ait hassasiyet durumları arasında farklılık vardır. 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. Bazen iki hassas bilgiden biri diğerine göre daha hassas olabilir.

78 McDonald, *A Framework For Technology-Assisted Sensitivity Review: Using Sensitivity Classification to Prioritise Documents for Review*, s. 40; Hitart Narvala, Graham McDonald ve Iadh Ounis, "Sensitivity Review of Large Collections by Identifying and Prioritising Coherent Documents Groups", (ACM International Conference on Information & Knowledge Management, 2022), s. 4931.

79 The National Archives, "Guide to archiving personal data", s. 32.

Hassasiyetin objektif olarak ölçülemeyen sosyal ve kültürel faktörlere bağlı, gizlilik uzmanları tarafından belirlenmesi gereken bir konu olduğu düşünülmektedir.[80] Hassas bilgi kavramı, yaygın bir şekilde mevcut gibi görünse de, bazı yönleri belirsizdir. Hassas bilgilerin ayrı bir bilgi türü veya kategorisinde olup olmadığı, insanların genel bilgilerle ilgili olarak uygulayacağı hassasiyet kodlamasına ihtiyaç olup olmadığı ve hassas durumlar hakkındaki bağlamsal bilgilere referans yapılıp yapılmayacağı gibi konular belirsizdir.[81] 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 hâle getirilmelidir.

Değerlendirme, arşiv iş süreçleri içerisinde en hassas ve zorlayıcı konuyu oluşturmaktadır. Hassasiyet değerlendirmesiyle birlikte bu süreç, kurumlara ve değerlendiricilere çeşitli açılardan zorluklar çıkartmaktadır

a. 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[82]. 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[83] olduğundan mevzuat nesnel, bağlama 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.[84] 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.[85] Bu durum hassasiyet değerlendirmesini zorlaştırmaktadır. Hassasiyet yargısı genellikle bilginin üretildiği bağlama ve gözden geçirildiği zamana bağlıdır.[86]

80 Liqiang Geng, Yonghua You, Yunli Wang ve Hongyu Liu, "Privacy Measures For Free Text Documents: Bridging The Gap Between Theory and Practice", (Berlin Heidelberg: Springer, Trust, Privacy and Security in Digital Business: 8th International Conference Proceedings, 2011), s. 164.

81 Thompson ve Kaarst-Brown, "Sensitive information: A Review and Research Agenda", s. 248.

82 Rukancı, Anameriç ve Başar, 2021 s. 48.

83 Karen McCullagh, "Data sensitivity: proposals for resolving the conundrum", *Journal of International Commercial Law and Technology*, C. II, S. 4(2007), s. 197.

84 Kindt, *Privacy and Data Protection Issues of Biometric Applications*, s. 125; Kirsten Martin ve Helen Nissenbaum, "Privacy interests in public records: An empirical investigation", *Harv. JL & Tech*, S. 31(2017), s. 113.

85 OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD Publishing, 2002), s. 40; Mark Elliot, Elaine Mackey ve Kieron O'Hara, The Anonymisation Decision-making Framework 2020, s. 136.

86 Graham McDonald, Craig MacDonald ve Iadh Ounis, *Active learning strategies for technology assisted sensitivity review* (Cham: Springer International Publishing, European Conference on Information Retrieval, 2018), s. 440.

Pek çok durumda hassasiyetin bağlama bağlı olduğu görülmektedir ve bu her zaman dilbilimsel bir analizde ele alınamaz.[87] 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.[88] Bağlama göre hassasiyet senaryoları değişmektedir. Bağlamın hassas olmayan verileri hassas verilere dönüştürebileceğini göz önünde bulundurmak önemlidir. Veriler kullanıldığı bağlamda (örneğin kültürel, coğrafi, dinî, siyasi koşullar vb.), açıkça kişisel veya hassas olmasa bile veri analizi, birey veya grupları/toplulukları etkileyebilir.[89] 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.[90] Hassas bilgiler örtük veya dolaylı olabilir. Bağlama bağlı olarak kişisel, kurumsal, siyasi ve ulusal güvenlik konuları ve diğer çağrışımlarla ilgili olabilir.[91] Bilginin hassas olup olmadığını belirleyen değerlendirici, bilgiyi kamuya açık hâle 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.[92] Bu durum "mozaik hassasiyet" kavramı ile açıklanmaktadır. 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.[93] Mozaik hassasiyet "*ilişki*" kurma kavramı ile bağdaşmaktadır.

87 Sabah Al-Fedaghi, *How sensitive is your personal information?* (New York: Association for Computing Machinery, Proceedings of the 2007 ACM symposium on Applied computing 2007), s. 165.

88 McDonald, *A Framework For Technology-Assisted Sensitivity Review: Using Sensitivity Classification to Prioritise Documents for Review*, s. 65.

89 Birleşmiş Milletler Geliştirme Grubu, *Data Privacy, Ethics and Protection. Guidance Note on Big Data for Achievement of the 2030 Agenda* (2017), s. 5.

90 Thompson ve Kaarst-Brown, "Sensitive information: A Review and Research Agenda", s. 248.

91 Moss ve Gollins, "Our Digital Legacy: An Archival Perspective", s. 13.

92 Constatine Photopoulos, *Managing catastrophic loss of sensitive data: A guide for IT and security professionals* (Burlington: Elsevier, 2011), s. 32; Rahime Belen-Sağlam, Jason R. C. Nurse ve Duncan Hodges, "Personal information: Perceptions, types and evolution" *Journal of Information Security and Applications*, S. 66 (2022), s. 14.

93 McDonald, *A Framework For Technology-Assisted Sensitivity Review: Using Sensitivity Classification to Prioritise Documents for Review*, s. 185.

Bir belge/nesne düzeyinde açıklama kendi başına zararsız olabilir, ancak daha yüksek düzeydeki bağlamsal bilgilerle birlikte, bireyin veri koruma haklarını ihlal edebilir. Örneğin, bir isim ve doğum tarihi tek başına zararsız görünebilir, ancak akıl sağlığı hastanesi hastalarının vaka dosyaları bağlamında hassas hâle gelir.[94] Bir isim tek başına bir kişiyi tanımlamak için yeterli değilken kişinin tanımlanmasını sağlayacak olan, ismin sahip olduğu pozisyon veya bir olay veya yer gibi diğer bilgilerle ilişkilendirilerek netlik kazanması sağlanır.[95] 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, Parlamento'da söylenen ve kaydedilen aynı sözlerin hassas olarak kabul edilmesi mümkün değildir.[96] Bir basın haberi gibi hâlihazırda yayınlanmış bir içerikte yer alan bilgilerin, özel olarak iletilen bilgileri tartışsa bile kamuya açıklandığından gizli olmadığı düşünülür. Ancak belge, hükûmetten veya başka bir kuruluştan bir yetkilinin basın açıklamasının içeriği hakkında ek bilgi sağlayan görüşlerini içeriyorsa, bu durumda görüşlerin hassas ve gizli olduğu kabul edilebilir.[97] 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 hâlegelebilir.[98]

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.

94 The National Archives, "Guide to archiving personal data", s. 30.

95 The National Archives, "Guide to archiving personal data". 30-31.

96 Alistair G. Tough, *The Scope and Appetite for Technology-Assisted Sensitivity Reviewing of Born-Digital Records in a Resource Poor Environment: A Case Study From Malawi* (Hershey: IGI Global, Handbook of Research on Heritage Management and Preservation, 2018), s. 177.

97 McDonald, *A Framework For Technology-Assisted Sensitivity Review: Using Sensitivity Classification to Prioritise Documents for Review*, s. 34.

98 Moss ve Gollins, "Our Digital Legacy: An Archival Perspective", s. 14.

b. Zaman

Belgeler, arşiv değerlerini koruduğu sürece saklanırlar.[99] 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 hâla geçerli olabilir.[100] 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.[101] Ancak hassasiyetin zaman geçtikçe azaldığı yaygın olarak kabul edilmektedir.[102] 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. Amerikan Ulusal Arşivler ve Kayıtlar İdaresinin 2004 yılında ölen bir avukata ait cesedin fotoğraflarını istemesi üzerine yüksek mahkeme, ölüm sahnesi fotoğraflarının yayımlanmasının 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 sahnesi fotoğraflarının kişisel gizliliğini, hayatta kalan aile üyelerini kapsayacak kadar genişlemesine karar vermiştir.[103] 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 oluşabilmektedir. Böyle durumlarda arşivciler, arşiv normları esasınca bireyin ölümüyle birlikte mahremiyet haklarının sona erdiğini[104] öne sürerken, diğer yanda bağışçıların yakınları tarafından talep edilen makul kısıtlamalara sıklıkla saygıgöstermektedir.[105]

İngiliz Ulusal Arşivi tarafından yayınlanan rehberler ve pek çok bilimsel çalışma, hassas bilgi içerikli belgelerde yaşanması muhtemel zamana dayalı problemler

99 Rukancı, Anameriç ve Başar, 2021, s. 49.

100 The National Archives, "Guide to archiving personal data", s. 33.

101 Bulut, "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", s. 124.

102 Sillitoe, "Privacy in a public place: Managing public Access to personal information controlled by archives services", s. 12; The National Archives, "Access to public records", s. 7; Moss ve Gollins, "Our Digital Legacy: An Archival Perspective", s.17; McDonald, *A Framework For Technology-Assisted Sensitivity Review: Using Sensitivity Classification to Prioritise Documents for Review*, s. 51.

103 Sillitoe, "Privacy in a public place: Managing public Access to personal information controlled by archives services", s. 12; J. Lyn Entrikin, "Family Secrets and Relational Privacy: Protecting Not-SoPersonal, Sensitive Information from Public Disclosure", *University of Miami Law Review*, S. 74 (2020), s. 827.

104 The National Archives, "Access to public records", s. 9.

105 Alex H. Poole, "An ethical quandary that dare not speak its name: Archival privacy and access to queer erotica", *Library & Information Science Research*, C. XLII, S. 2 (2020), s. 6-7.

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, yaşayan bir bireyin mahremiyetini ihlal edecek hassas bilgi içeren belgelerin 75 yıla kadar saklanmasına izin vermektedir.[106] Avrupa ülkelerinde kişinin yaşı bilinmiyorsa, reşit olmayanlar için tüm süre boyunca, 16 yaşın üzerinde olduğu düşünülenler için ise 80 veya 94 yıl boyunca kapatılmaktadır.[107] 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.[108] Bu süre, yalnızca ölüm oranı için keyfi bir rakam olarak değil, daha ziyade, doğal yaşam sırasında kapatma ve ölüm sonrası sınırlı korumayı öngörmektedir.[109] Sınırlı koruma, kişinin ailesi ve yakınlarının zarar görmemesi anlayışı için dikkate alınmalıdır.

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.[110] Kapatma süreleri, hassasiyet zaman içinde azaldığından, belgenin bitiş tarihinden itibaren tanımlanmış bir süre için olmalıdır. Belgelerin açılabileceği belirli bir zamanın belirlenmesinin mümkün olmadığı durumlarda, kapatmaya devam edilmesinin gerekli olup olmadığına karar vermek ilgili birim tarafından yeniden gözden geçirileceği ileri bir tarih belirlenmelidir. Yaygın kapatma süreleri kişilerle ilgili olanlar için "ömür boyu" veya yeniden inceleme için on yıllık dönemlerdir.[111] Bazı görüşlerde, bu süre 30 yıl olarak ifade edilmektedir. Eğer 30 yıl sonra hâla önemli sıkıntıların yaşanacağı hissediliyorsa aynı 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.[112] Bu bağlamda

106 Bennet B. Borden ve Jason R. Baron, *Opening up dark digital archives through the use of analytics to identify sensitive content* (IEEE, IEEE international conference on big data, 2016), s. 3225.

107 Moss ve Gollins, "Our Digital Legacy: An Archival Perspective", s. 13.

108 Sillitoe, "Privacy in a public place: Managing public Access to personal information controlled by archives services", s. 11; Thompson ve Kaarst-Brown, "Sensitive information: A Review and Research Agenda", s. 252; Allan, *Records Review*, s. 14; The National Archives, "Closure Periods", s. 4.

109 Sillitoe, "Privacy in a public place: Managing public Access to personal information controlled by archives services", s. 11.

110 The National Archives, "Closure Periods", s. 2.

111 The National Archives, "Access to public records", s. 7; The National Archives, "Access at transfer – Sensitivity Review Overview", s. 3.

112 Thompson ve Kaarst-Brown, "Sensitive information: A Review and Research Agenda", s. 252.

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, siyasi ya da kamu tanınırlığı yüksek kişiler hâline gelmesi; uluslararası ilişkilerin zaman içinde değişmesi; zamanla sosyal, siyasi 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 hukuki varlık, gizlilik ve hassasiyet değerlendirmesinin uygulanabilmesi için gereklidir. Örneğin Osmanlı dönemi arşiv belgelerini içeren Osmanlı Arşivinde yer alan belge ve belge gruplarına yönelik bir gizlilikten ve hassasiyetten bahsetmek çoğunlukla mümkün değildir. Ancak son dönem siyasi 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 siyasi 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.[113]

Bunun dışında açıklanma zamanı birtakım ticari risklere sebebiyet verecek belgeler için de aynı durum söz konusudur. Şirketler için önemli piyasa sonuçları olan bir ticari 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 yayımlandıktan veya yasalaştıktan sonra hassas değildir.[114] Bu bağlamda, zamanın hassasiyet oluşumu için önemli ve dikkat edilmesi gereken nokta olduğu anlaşılmaktadır

c. Belge Hacmi, Kaynak ve Bütçe

Kamu kurumlarında üretilen ve kullanılan belge miktarında yaşanan artış değerlendirme işlemlerini zorlaştırmaktadır. Özellikle elektronik belge yönetim sistemlerine geçilmesi, çok sayıda belgenin üretilmesini kolaylaştırırken birikmekte olan belge yığınının değerlendirme, analiz, koruma ve yetkisiz erişim ihlallerini önleme süreçlerini karmaşık hâle 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

113 McDonald, McDonald ve Ounis, *Active learning strategies for technology assisted sensitivity review*, s. 3

114 Moss ve Gollins, "Our Digital Legacy: An Archival Perspective", s. 14.

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. Bu bağlamda her belgeyi baştan sona incelemek pratik olmayarak hassas bilgilerin tespitinde olası gözden kaçmalara yol açar.

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 gerektirir. Hata oranı, değerlendirmenin yardımcı araçlar kullanılarak yapıldığı sistemler/yazılımlar için de geçerlidir. Hassasiyet değerlendirmesi için kullanılan otomatik araçlar, yanlış pozitifler (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.

d. 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 bahsedildiği üzere mevzuat düzenlemelerinde çeşitli kavramlar ile yer bulmuştur. Mevcut mevzuata değerlendirme bölümünde ayrıca değinilecektir. 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 çerçevesinin daraltmaktadır.

Hassas bilgilerin mevzuat düzenlemelerinde hangi koşullarda işleneceği ifade edilmektedir. Kamu yararına yürütülen bir görev, resmî yetkinin kullanılması veya meşru bir menfaat gibi alternatif bir hukuki dayanağın daha uygun olması hâlinde, 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.[115] Ancak bir kişinin din 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. Veya veri sorumlularının bu tür kişisel

115 The National Archives, "Guide to archiving personal data", s. 16.

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.[116] 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 hâle getirmektedir.[117]

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 bağlamın hassasiyet oluşumu ve işleme süreçlerinde büyük bir etkiye sahiptir.

e. 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.[118] Mevzuat düzenlemelerinde sayılan hassas konuların seçimine ilişkin hukuki tercih, büyük oranda veri türlerinin hassas verilere dönüşmesinde etkili olan toplumsal değer yargılarının değişken olmasından ve kültürel kodlara göre kaynaklandığı söylenebilir.[119] Bir ülkede evrensel kişisel tanımlayıcılar hem zararsız hem de yararlı olarak kabul edilirken, başka bir ülkede son derece hassas olarak kabul edilebilir ve kullanımları kısıtlanabilir, hatta yasaklanabilir. Bazı ülkelerde, gruplar ve benzer varlıklarla ilgili verilere koruma sağlanırken, başka bir ülkede bu tür bir koruma tamamen mevcut olmayabilir.[120]

Sosyo-kültürel faktörler belirli verilerin hassasiyetini önemli ölçüde değiştirebilir. Bir kişinin yaşı Kuzey Amerika'da mahremiyet olarak kabul edilirken, bazı Asya ülkelerinde olmayabilir.[121] Otoriter veya teokratik toplumlarda din, cinsel

116 Belen-Sağlam, Nurse ve Hodges, "Personal information: Perceptions, types and evolution", 2022, s. 9

117 Lemieux ve Werner, "Protecting Privacy in Digital Records: The Potential of Privacy-Enhancing Technologies", s. 3

118 Peter Fule ve John Roddick, *Detecting privacy and ethical sensitivity in data mining results* (*Proceedings of the 27th Australasian conference on Computer science-Volume*, Dunedin: Australian Computer Society, 2004), s. 162.

119 Bulut, "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", s. 138.

120 OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, s. 38.

121 Geng ve diğerleri, "Privacy Measures For Free Text Documents: Bridging The Gap Between Theory and Practice", s. 164.

tercih, siyasi 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.[122]

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 Bürosunun belgelerini değerlendiren arşivcinin bile dosyalarda gelir vergisi beyannamesi bilgilerini görmesine izin verilmezken, İsveç'te ise aksine gelir vergisi bilgileri kamuya açıktır.[123] 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 siyasi 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.[124] 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 arşiv kurumları evlilik dışı çocuklara yönelik bilgileri içeren belgeleri geçmişte redakte ederek yayımlarken artık günümüzde böyle bir uygulamaya ihtiyaç duyulmamaktadır. 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 etmesi mümkündür. 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

122 John M. M. Rumbold ve Barbara K. Pierscionek, 2018, s. 57

123 Henttonen, 2017, s. 288

124 Rumbold ve Pierscionek, "What are data? A categorization of the data sensitivity spectrum", *Big data Research*, S. 12 (2018), s. 56.

etmelidir[125]. Hassasiyet değerlendirmesi sürecinde, bireylerin ve toplumların kendi iç dinamiklerine ek olarak kültürel çeşitliliğin dikkate alınması beklenmektedir.

f. Kişisel Bakış ve Deneyim

Değerlendirme, önyargıdan ve öznellikten bağımsız olmamakla birlikte günün kültürel değerleri esasınca değerlendiricilerin eğilimlerine yansımaktadır.[126] 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 bağlıdır.[127] Değerlendirme sürecinde, objektif ve tarafsız yaklaşılması beklenmektedir. Ancak değerlendiricinin kişisel bakış açısı ve deneyimleri kişinin yargısını istemeden de olsa şekillendirir. Özellikle hassasiyet değerlendirmesi söz konusu olduğunda doğrudan etki edebilmektedir. Değerlendiriciler kişisel inançlarına, kültürel geçmişlerine veya deneyimlerine dayanarak belirli bir siyasi veya sosyal bakış açısıyla birbirlerinden farklı hassasiyet yargılarına ulaşabilmektedir. 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.[128] 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[129] değerlendirme işleminin farklı kişiler tarafından kontrolüne, değerlendiricilerin belge üstveri bilgisine eklenmesine ve değerlendirilen belgenin periyodik aralıklar ile tekrarına gereksinim duyulmaktadır.

Değerlendirme ve Sonuç

Bu çalışmada, kamu belgelerinin güvenlik ve gizliliğinin hassasiyet bağlamında nasıl değerlendirildiği, sürecin karmaşıklığı ve zorlukları incelenmiştir. Hassasiyet değerlendirmesi, kamu kurumlarında üretilen ve kullanılan belgelerin dolaşımdaki güncel dönemleri, ulusal arşive transferi, erişim veya kapatma kararı alınması

125 Katherine McCardwell, *Intellectual Propoerty Concerns in Undocumented Corporate Collections – Case Studies in Archival Ethics* (Chicago: Society of American Archivist, 2014), s. 4.

126 Johns, "Appraisal and Disposal", s. 32.

127 Thompson ve Kaarst-Brown, "Sensitive information: A Review and Research Agenda", s. 248.

128 Henttonen, 2017, s. 288.

129 Rukancı, Anameriç ve Başar, 2021 s. 46.

bakımından kritik önem taşımaktadır. Ancak bu süreç, anılan faktörlerden dolayı oldukça zorlayıcı olabildiğinden bireylerin mahremiyeti, kurumların itibarı ve güveni bakımından hassas bir yönü bulunmaktadır. Kamu belgelerinin güvenli ve etkin bir şekilde yönetilmesi, kamu şeffaflığını ve hesap verebilirliğini güçlendirmektedir. Hassas bilgi içeren belgelerin arşivlenmesi, hassasiyet ve güvenlik dengesini gözetmeyi gerektiren karmaşık bir süreçtir. Her bir değerlendirme zorluğuna yönelik önlemlerin alınması mümkündür. Örneğin zaman problemi periyodik değerlendirme ve saklama süresi sınıflandırmaları ile; kişisel bakış açısı ve deneyime bağlı problemler birden fazla değerlendirici ve teknoloji destekli muadil karar hatırlatma sistemleri ile; belge hacminden kaynaklanan bütçe ve personel problemleri teknoloji destekli değerlendirme yazılımları ile; sosyo-kültürel ortam ve mevzuat problemleri, dönüşen toplumsal yapı, hassasiyet zayıflaması/kaybı veya edinimi ihtimali ve bağlam çerçevesinde yeniden yapılandırılarak çözülebilir. Ancak bahsedilen zorluklar arasında yer alan "bağlam", her belge özelinde sonsuz bir ihtimali barındıran hassasiyet değerlendirmesi sürecinin en önemli ve zorlayıcı konusu olmaktadır. Bağlam ve ilişki [diğer belgelerin/bilgi kırıntılarının hassasiyete etkisi] etkisinin hassasiyet değerlendirmesi sürecinde tartışılmaya ve çözümler üretilmeye devam eden konular olacağı açıktır.

Hassasiyet değerlendirmesi, Türkiye'de belgelerin gizliliği konusuna giren ancak özel bir değerlendirmenin yapılmadığı veya odak yönü olmayan bir süreçtir. Arşiv iş süreçleri diğer ulusal arşiv kurumlarında ve Türkiye'de olduğu üzere mevzuat kapsamında işlemektedir. 11 sayılı Cumhurbaşkanlığı Kararnamesi'ne göre devlet ve kişilerin ulusal ve uluslararası haklarını belgelemek ve korumak" Devlet Arşivleri Başkanlığı'nın görevi olarak kabul edilmektedir (5/1.b). 11 sayılı Kararname, kararnameye bağlı olarak yayımlanan Devlet Arşiv Hizmetleri Hakkında Yönetmelik ve Arşivlerden Yararlanma Usul ve Esasları Hakkında Yönetmelik belgelerin gizliliği ve güvenliği hususunda temel bağlayıcılığı olan bazı bildirimlerde bulunmaktadır. Bununla birlikte Kişisel Verilerin Korunması Kanunu, Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik, Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik ve Bilgi Edinme Kanunu kamu belgelerinin gizliliği, erişime sunulması, belge yönetimi ve arşivlenmesi hususunda dikkate alınan düzenlemelerdir. Hassas bilgi tanımları ve bu tür bilgi taşıyan belgelere yönelik yaklaşımlar bahsedilen düzenlemelerde kapsamlı ve uygulamaya dönük bir çerçeve çizmese de yer almaktadır. Dünyadaki ulusal arşiv kurumları hassasiyet değerlendirmesi uygulamalarını anılan türdeki [Türkiye özelinde] mevzuata dayandırarak özel bir işlem olarak değerlendirip gerçekleştirmektedir. Temel arşiv mevzuatında ve bağlı olarak iş ve işlemlerin açıklandığı rehberlerde bilgilendirmeler yayımlamışlardır.

Bu çalışma, hassasiyet değerlendirmesi sürecine bir içgörü sunmaktadır. Hassasiyet değerlendirmesi süreci, belgelerin güvenlik ve gizlilik kaygılarına içerik (*content*) bağlamında odaklanan, uluslararası arşiv uygulamalarında var olan bir meseledir. Bu bakımdan yapılan değerlendirmelerin konunun önemine dikkat çekeceği, uygulamacılara ve karar vericilere yol/yön gösterici olacağı düşünülmektedir.

EXTENDED ABSTRACT

Some types of information are more sensitive than others. In particular, it is necessary to recognise and correctly classify sensitive information that may lead to serious consequences in case of disclosure of records involving individuals, institutions and international relations. Public records hold critical importance for preserving national memory and transmitting it to future generations. As a result of the natural interactions of citizens, these records are not only historical and official records, but also contain critical information on sensitive issues such as national security, international relations and individual privacy. Therefore, the proper management and meticulous execution of processes involving sensitive public records of archival value are essential. This process, known as "sensitivity review", involves evaluaating archival records that contain sensitive or special data categories of information. Sensitivity review includes identifying which sensitive information is contained within the records, applying restriction procedures (such as masking, redaction, etc.), determining how long the records should remain closed, and under what conditions they can be made accessible again. Although sensitivity review is not yet implemented in Türkiye, it is widely practiced by many national archival institutions and is a crucial part of the confidentiality aspect of records. For records classified as confidential, this reviews forms a focal phase of the fundamental archival process known as "appraisal." The management of records containing sensitive information consists of several key steps. Firstly, these records need to be accurately identified and classified. In this step, the type of information contained in the records and the degree of its sensitivity are determined. Next, access controls and restrictions for these records are established. Access controls define who can access these records and under what conditions access can be granted. Restrictions determine how long the records should remain confidential and under what circumstances they can be made accessible. Finally, there is the process of making the records available to the public. This step involves deciding how the records will be presented to the public and which information will remain confidential. This management process presents various challenges. For instance, the context of the records, their relationship with other records, their timing, volume, socio-cultural environment, legislation, personal perspectives, and experiences are all challenging factors in the evaluation process. Additionally, classifying types of sensitive information and determining their sensitivity levels is quite a complex process. Errors in this process can lead to the inadvertent disclosure of critical information or unnecessary restrictions. This makes the determination of access controls and restrictions a crucial issue. These controls and restrictions must ensure both the security of the information and the protection of the right to access information. Sensitivity review is applied both before and after the transfer of records with archival value, making it extremely important for public archives. Public archives contain a wide range of records, many of which may include sensitive information. Therefore, the correct management and protection of these records are of great importance. The fact that sensitivity review is not yet a focal point in practice in Türkiye is seen as a significant shortcoming in this area. This study aims to examine the theoretical framework, implementation process, and challenges of sensitivity review. The goal of the study is to detail why sensitivity review is important and how this review should be conducted. In conclusion, sensitivity review is critically important for the proper management and protection of public records. This review process involves the accurate classification of records, the determination of access controls and restrictions, and the public presentation of the

records. Correctly conducting this process is crucial for preserving national memory and accurately transmitting it to future generations. The study can contribute to overcoming this deficiency by providing an insight into this issue, which is not included in practice in Türkiye. The evaluations made in this study highlight the importance of the subject and are expected to lead to a better understanding and further research in this area. In conclusion, the objective of this study is to highlight the pivotal role of sensitivity review in archival practice and to pioneer the effective integration of this process into the management of public records in Türkiye. This can ensure that sensitive information is appropriately protected while also balancing the need for transparency and public access to historical records. By doing so, the management of public records can be enhanced, ensuring that sensitive information is safeguarded without compromising the integrity and accessibility of the nation's historical archives. This will contribute significantly to the preservation of national heritage and the accurate documentation of historical events for future generations.

Kaynakça

Allan, Alex: *Records Review,* London: Cabinet Office, 2014.

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

Belen-Sağlam, Rahime. - Jason R. C. Nurse - Duncan Hodges: "Personal information: Perceptions, types and evolution", *Journal of Information Security and Applications*, S. 66 (2022), 103163.

Birleşmiş Milletler Geliştirme Grubu: (2017). Data Privacy, Ethics and Protection. Guidance Note on Big Data for Achievement of the 2030 Agenda. https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf [Erişim tarihi: 31.03.2024].

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

Bulut, Metin: "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler". *Ankara Barosu Dergisi*, C. LXXVIII, S. 3 (2020), 99-150.

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

Cook, Terry: *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, 1991.

Čtvrtník, Mikuláš: "Closure periods for access to public records and archives. Comparative-historical analysis", *Archival Science*, C. XXI, S. 4 (2021), 317-351.

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)

Elliot, Mark. - Elaine Mackey - Kieron O'Hara: *The Anonymisation Decision-making Framework* (2. baskı), Manchester: UKAN, 2020.

Entrikin, J. Lyn: "Family Secrets and Relational Privacy: Protecting Not-So-Personal, Sensitive Information", *University of Miami Law Review*, S. 74 (2020), 781-897.

Etzioni, Amitai: "A cyber age privacy doctrine: More coherent, less subjective, and operational", *Brooklyn Law Review,* C. LXXX, S. 4 (2014), 1263-1308.

Fule, Peter. - John F. Roddick: 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. (2004)

Geng, Liqiang. – Yonghua You – Yunli Wang ve Hongyu Liu: "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, 2011.

Henkoğlu, Türkay: *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, 2015.

Henttonen, Pekka: "Privacy as an Archival Problem and a Solution", *Archival Science*, C. XVII, S. 3 (2017), 285-303.

IFLA-ICA Statement on Privacy Legislation and Archiving: (2020). https://www.ifla.org/publications/ifla-ica-statement-on-privacy-legislation-and-archiving/ [Erişim tarihi: 30.01.2024].

International Council on Archives: Principles of Access to Archives. Committee On Best Practices And Standards Working Group On Access. https://www.ica.org/sites/default/files/ICA_Access-principles_EN.pdf [Erişim tarihi: 20.01.2024].

Jaillant, Lise. - Arran Rees: "Applying AI to digital archives: trust, collaboration and shared professional Ethics", *Digital Scholarship in the Humanities*, C. XXXVIII, S. 2 (2023), 571-585.

Jo Pugh, Mary: *Providing Reference Services for Archives and Manuscripts*. Chicago: The Society of American Archivists, 1992.

Johns, R: Appraisal and Disposal. https://silo.tips/embed/04-appraisal-and-disposal.html?sp=0 [Erişim tarihi: 20.05.2024].

Johnson, Chris. - Lee Badger - David Waltermire – Julie Snyder – Clem Skorupka: "Guide to Cyber Threat Information Sharing", *NISTS Special Publication*, C. DCCC, S. 150 (2016), 1-35.

Kindt, Els J.: *Privacy and Data Protection Issues of Biometric Applications*. New York: Springer, 2016.

Lemieux, Victoria. L. - John Werner: "Protecting Privacy in Digital Records: The Potential of Privacy-Enhancing Technologies", *ACM Journal on Computing and Cultural Heritage*, C. XVI, S. 4 (2024), 1-18.

Martin, Kirsten. - Helen Nissenbaum: "Privacy interests in public records: An empirical investigation". *Harv. JL & Tech*, S. 31 (2017), 111-125.

Mathers, Josette: "Providing access to sensitive records: the Personal History Index (PHIND)", *Archives and Manuscripts*, C. XXVIII, S. 2 (2000), 58-70.

McCardwell, Katherine: *Intellectual Propoerty Concerns in Undocumented Corporate Collections – Case Studies in Archival Ethics*, Chicago: Society of American Archivist, 2014.

McCullagh, Karen: "Data sensitivity: proposals for resolving the conundrum", *Journal of International Commercial Law and Technology*, C. II, S. 4 (2007), 190-201.

McDonald, Graham: *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. 2019.

McDonald, Graham. – Craig MacDonald – Iadh Ounis: "Active learning strategies for technology assisted sensitivity review", *European Conference on Information Retrieval* içinde (s. 439-453), Cham: Springer International Publishing, 2018.

Moss, M. S. – T. J. Gollins: "Our Digital Legacy: An Archival Perspective", *Journal of Contemporary Archival Studies*, C. IV, S. 2 (2017), 3.

Narvala, Hitart. - Graham McDonald – Iadh Ounis: "Sensitivity review of large collections by identifying and prioritising coherent documents groups", *Proceedings of the 31st ACM International Conference on Information & Knowledge Management* içinde (s. 4931-4935), 2022.

National Records of Scotland. Guidance to the Form and Content of the Model Records Management Plan. https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/Guidance_Document_v2.0_-_21_February_2024.pdf [Erişim tarihi: 21.04.2024].

Naugler, Harold: *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, 1984.

OECD: *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris: OECD Publishing, 2002

Ohm, Paul: "Sensitive information". *Southern California Law Review*, C. LXXXVIII, S. 5 (2014), 1125-1196.

Olusola Olajide Ajayi. - Adebiyi Olarewaju Temidayo: "Application Of Data Masking in Achieving Information Privacy", *IOSR Journal of Engineering*, C. IV, S. 2 (2014), 13-21.

Özdemir, Lale: "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*, C. XXX, S. 2 (2009), 137-145.

Pearce-Moses, Richard: *A Glossary of Archival and Records Terminology*. Chicago, IL: The Society of American Archivists, 2005.

Photopoulos, Constatine: *Managing catastrophic loss of sensitive data: A guide for IT and security professionals*. Burlington: Elsevier, 2011.

Ponemon Institute:. 2017 Cost of Data Breach Study. Research Report. https://documents.ncsl.org/wwwncsl/Task-Forces/Cybersecurity-Privacy/IBM_Ponemon2017CostofDataBreachStudy.pdf [Erişim tarihi: 31.01.2024].

Poole, Alex H: "An ethical quandary that dare not speak its name: Archival privacy and access to queer erotica", *Library & Information Science Research*, C. XLII, S. 2 (2020), 101020.

Public Record Office, A guide to accessing 'closed' records. https://www.gov.im/media/1377168/20220725-accesstoclosedrecords-v1-2.pdf (2022). [Erişim tarihi: 13.03.2024].

Redwine, Gabriela. - Megan Barnard.- Kate Donovan -Erika Farr.- Michael Forstrom – Hansen Michael.- John Will.- Leighton Jeremy - Nancy Kuhl – Seth Shaw – Susan Thomas: *Born digital: Guidance for donors, dealers, and archival Repositories*, Washington: Council on Library and Information Resources, 2013.

Reed, Barbara: "Reinventing Access", *Archives and Manuscripts*, C. XLII, S. 2 (2014), 123-132.

Rukancı, Fatih. – Hakan Anameriç – Alparslan Başar: *Arşiv ve Arşivcilik: Kuram, Strateji ve Uygulamalar*. Ankara: T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı Yayınları, 2021.

Rukancı, Fatih. – Hakan Anameriç - Alparslan Başar: "Gizlilik", Arşiv Terimleri, İstanbul, Devlet Arşivleri Başkanlığı Yayınları, 2023

Rumbold, John M. M. – Barbara K. Pierscionek: "What are data? A categorization of the data sensitivity spectrum", *Big data research*, S. 12 (2018), 49-59.

Sabah Al-Fedaghi: "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, 2007.

Sillitoe, Paul J: "Privacy in a Public Place: managing public access to personal information controlled by archives services". *Journal of the Society of Archivists*, C. XIX, S. 1 (1998), 5-15.

Simitis, Spiros: Revisiting sensitive data. https://rm.coe.int/16806845af%3E, (1999). [Erişim tarihi: 17.05.2024].

Sloyan, Victoria: "Born-Digital Archives at the Wellcome Library: Appraisal And Sensitivity Review Of Two Hard Drives", *Archives and Records*, C. XXXVII, S. 1 (2016), 20-36.

Stein, Zachary G: "Privacy in Public Archives: Managing Personally Identifiable Information in Special Collections", *RBM: A Journal of Rare Books, Manuscripts, and Cultural Heritage*, C. XXII, S. 2 (2021), 85.

Society of American Archivists, SAA Code of Ethics. Society of American Archivists, tarafından Şubat 2005'te onaylandı; Ocak 2012 ve Ağustos 2020'de gözden geçirildi. https://www2.archivists.org/statements/saa-core-values-statement-and-code-of-ethics (2020) [Erişim tarihi: 19.04.2024].

Şişman, Nazife: *Mahremiyet, Hayatın Sırları ve Sınırları*, İstanbul: İnsan Yayınları, 2019.

Tekerek, Mehmet: "Bilgi Güvenliği Yönetimi", *KSÜ Doğa Bilimleri Dergisi*, C. XI, S. 1 (2008), 132-137.

The National Archives, Disposal scheduling. https://cdn.nationalarchives.gov.uk/documents/information-management/sched_disposal.pdf (2012). [Erişim tarihi: 23.03.2024].

The National Archives, Access to public records. https://cdn.nationalarchives.gov.uk/documents/information-management/access-to-public-records.pdf (2015). [Erişim tarihi: 24.04.2024]

The National Archives, Guide to archiving personal data. https://cdn.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf (2018), [Erişim tarihi: 15.02.2024]

The National Archives, Procedures for closure on transfer. https://cdn.nationalarchives.gov.uk/documents/information-management/procedures-for-closure-on-transfer.pdf, (2019b). [Erişim tarihi: 12.03.2024].

The National Archives, Access at transfer – Sensitivity Review Overview. https://cdn.nationalarchives.gov.uk/documents/information-management/access-at-transfer-sensitivity-review-overview.pdf (2021a). [Erişim tarihi: 03.04.2024].

The National Archives, Closure Periods. https://cdn.nationalarchives.gov.uk/documents/information-management/closure-periods.pdf, (2021b) [Erişim tarihi: 10.05.2024]

The National Archives, Redaction Toolkit: Editing exempt information from paper and electronic documents prior to release. https://cdn.nationalarchives.gov.uk/documents/information-management/redaction_toolkit.pdf, (2022) [Erişim tarihi: 03.01.2024].

The National Archives, Sensitivity Review. https://www.nationalarchives.gov.uk/information-management/manage-information/public-inquiry-guidance/sensitivity-review/ (2023) [Erişim tarihi: 27.05.2024].

Thompson, E. Dale. - Michelle L. Kaarst-Brown: "Sensitive information: A Review and Research Agenda", *Journal of the American Society for Information Science and Technology*, C. LVI, S. 3 (2005), 245-257.

Tipton, Harold F: *Purposes of Information Security Management*. Handbook of Information Security Managemen, CRC Press, 1998

Tough, Alistair G: "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, 2018.

Transportation Security Administration, TSA Management Directive No. 3700.4 Handling Sensitive Personally Identifiable Information. https://www.tsa.gov/sites/default/files/foiareadingroom/handling_sensitive_personally_identifiable_information_3700.4.pdf, (2008) [Erişim tarihi: 20.02.2024].

Whorley, Tywanna Marie: *The Tuskegee Syphilis Study: Access and Control over Controversial Records* (Doktora Tezi). University of Pittsburgh. The School of Information Sciences, 2006.