Üniversite Kütüphanelerinde Kişisel Verilerin Korunması*

Protection of Personal Data in University Libraries

*Türkay HENKOĞLU** ve Nazan ÖZENÇ UÇAK****

Öz

Güvenilir bilgiye erişim ve büyük ölçüde elektronik ortamda saklanan mevcut bilginin korunmasına yönelik ihtiyaçların arttığı günümüzde, korunacak bilgi varlıkları içinde kişisel veriler önemli bir yer tutmaktadır. Bu bilgi varlıklarının korunması hukuksal, teknik ve idari boyutların dikkate alındığı bilgi güvenliği politikalarının gücü ile mümkün olabilmektedir. Bu çalışmada, kişisel verilerin korunmasına ilişkin temel ilkeler ve hukuksal düzenlemeler çerçevesinde üniversite kütüphanelerindeki mevcut durum değerlendirilerek, eksikliklerin giderilmesine yönelik önerilerde bulunulmuş ve bilgi güvenliği kültürünün oluşmasına katkı sağlanması hedeflenmiştir. Bu amaçla Ankara'da bulunan 15 üniversite kütüphanesini kapsayacak şekilde görüşme yoluyla anket uygulanmış ve alınan bilgi güvenliği önlemleri mevcut hukuksal düzenlemeler çerçevesinde değerlendirilmiştir.

Çalışma sonucunda; yasal düzenlemelerin yeterli ve önleyici nitelikte olmadığı, üniversitelerde kişisel verilerin korunmasına ve verilerin güvenli olarak imha edilmesine ilişkin politikaların bulunmadığı, risk yönetiminin yapılmadığı, üniversite birimleri arasında sorumlulukların paylaşılmadığı, kişisel verileri işleyen personele veri korumaya ilişkin bilinçlendirme eğitimi verilmediği ve kişisel verileri işleyen birimlerin hangi verilerin kişisel veri olduğu konusunda dahi tereddütlerinin bulunduğu görülmektedir.

Anahtar Kelimeler: *Bilgi güvenliği, Kişisel veri, Hassas veri, Bilgi güvenliği politikası*

Abstract

Today, with the significant increase in the need for the access to reliable information and for the protection of available information stored electronically; personal data has become one of the most important information assets that must be protected. The protection of these information assets is only possible with the power of information security policies including legal, technical, and administrative dimensions. In this study, current situation of university libraries has been evaluated based on the framework of basic principles and legal regulations related to

* Bu makale Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümünde Hazırlanan "Hassas bilgi varlıklarının ve kişisel verilerin hukuksal düzenlemeler ile korunması ve bu kapsamda üniversiteler için bilgi güvenliği politikasının geliştirilmesi" başlıklı doktora tezinin bir bölümü üzerine temellendirilmiştir. İlgili tez çalışması "2211-C Öncelikli Alanlara Yönelik Yurt İçi Doktora Burs Programı" kapsamında TÜBİTAK tarafından desteklenmiştir.

** Dr., Hacettepe Üniversitesi, Beytepe, Ankara. (henkoglu@ hacettepe.edu.tr)

*** Prof. Dr., Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü, Beytepe, Ankara. (ucak@hacettepe.edu.tr)

the protection of personal data; and it has been aimed to make suggestions for elimination of deficiencies in this area and to contribute to the creation of information security culture. For this purpose, a survey was conducted through interviews at 15 different university libraries located in Ankara, and the collected data relating to the information security measures was evaluated in accordance with the existing legal regulations.

The results show that the legal regulations are not adequate and preventive in nature, the universities do not have any security policies concerning the protection and the safe destruction of personal data. There is not any risk management, and the responsibility is not shared within the units of universities. Training for personal data protection awareness is not provided for the staff who is responsible for data processing, and the units responsible for the data processing have hesitation even in deciding whether data is personal or not.

Keywords: *Information security, Personal data, Sensitive data, Information security policy*

Giriş

Güvenilir bilgiye erişim ve var olan bilginin korunmasına yönelik ihtiyaçların ve tartışmaların arttığı günümüzde, korunacak bilgi varlıkları içinde en önemli payı kişisel veriler[1] oluşturmaktadır (King ve Raja, 2012). Kütüphanelere ilişkin olarak da üye bilgileri (isim, adres, telefon, eğitim vd. mesleki bilgiler) ile ödünç alma ve araştırma bilgileri bu kapsamda kişisel veriler olarak nitelendirilmektedir (Preisig, Rösch ve Stückelberger, 2014). Ancak büyük ölçüde elektronik ortamda saklanan bu verilerin korunmasında ne kadar ihtiyatlı olunduğu, hangi güvenlik politikalarının uygulandığı, kişisel verilerin işlenmesinin disiplin altına alınıp alınmadığı ve temel hak ve özgürlüklerin nasıl korunduğu konusunda belirsizlikler bulunmaktadır. Üniversite Bilgi İşlem Daire Başkanlığı (BİDB) tarafından alınan teknik önlemlerle, verinin gizliliğinin sınırlı olarak (kişilik hakları göz ardı edilerek) korunması sağlanabilmektedir. Bu yaklaşım, Whitman ve Mattord tarafından dikkat çekilen kişilik haklarının korunması ile bilginin gizliliğin korunması arasındaki bağın kurulamamasına (Whitman ve Mattord, 2011) ve alınan önlemlerin bir yönünün zayıf kalmasına neden olmaktadır. Kişisel verilerin korunması için alınan önlemlerin ve uygulanacak yöntemlerin çeşitliliğinin artması, bu konunun disiplinler arası boyutunun da gelişmesine ve çok yönlü yaklaşımın benimsenmesine neden olmaktadır. Teknik önlemlerin yanı sıra hukuksal çerçevede alınacak idari önlemlerin, tüm üniversite birimlerinde uygulanabilir genel güvenlik unsurlarını içerecek ve kişisel hakları koruyacak nitelikte olması gerekmektedir. AB Kişisel Verileri Koruma Direktifi reform paketine ilişkin gerekçede de vurgulandığı gibi, kişisel verilerin korunması konusundaki eksikliklerin temel nedenleri arasında farkındalığa ilişkin eksiklikler bulunmaktadır (Avrupa Konseyi, 2012). AB içinde bu eksikliklerin giderilebilmesi için, bilgi güvenliği kültürünün oluşturulmasına yönelik bilgi güvenliği politikalarının geliştirilmesine büyük önem verilmektedir (Henkoğlu ve Yılmaz, 2013).

1 26 Aralık 2014 tarihli Kişisel Verilerin Korunması Kanunu Tasarısı'nda (KVKKT) kişisel veriler, "kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanarak, hassas ve kişisel verilere ilişkin örneklere yer verilmiştir (T.C. Başbakanlık, 2014).

Kişisel verilerin işlenmesi sürecinin hukuksal ve teknik boyutları bulunmaktadır. Hukuksal dayanağı bulunmayan teknik önlemlerin alınması ya da sadece hukuksal düzenlemelerin yapılmasıyla bilgi varlıklarının korunabilmesi mümkün değildir (Fischer-Hübner, 2001). Bununla birlikte, kişisel verilerin korunmasına yönelik hukuksal düzenlemeler, bilgi güvenliğine ilişkin politikaların üretilmesi ve uygulanmasının en önemli dayanağını oluşturmaktadır. Ancak bilgi güvenliği konusunun çok yönlü oluşu ve disiplinler arası işbirliğini gerektirmesi, bu konunun ötelenmesine ve üniversiteler için risklerin artmasına neden olmaktadır. Toplumsal hayatın her alanında ihtiyaç duyulan bilgi güvenliğinin sağlanmasına ilişkin olarak, Türkiye'deki üniversitelerde hukuksal düzenlemelerle uyumlu ve standartlaşmış bilgi güvenliği politikaları bulunmamaktadır. Bu çalışmada veri gizliliğinin korunmasıyla ilişkili olarak, bilgi güvenliği kapsamında alınan önlemlere yönelik veriler de toplanmış ve değerlendirilmiştir. Ancak bilgi güvenliğine yönelik olarak elde edilen bulgular ve çalışma sonunda sunulan öneriler, kişisel haklar ve bireyin kendi verileri üzerindeki haklarının korunması çerçevesinde oluşturulmuştur.

Üniversite Kütüphanelerinde Gizlilik ve Kişisel Hakların Korunması

Kişisel verilerin korunması hakkı, bireyin özel hayatını ilgilendiren, kişilik haklarının ve onurun korunması anlamına da gelen bir temel haktır. Kişisel verilerin korunmasıyla, bireyin kendisine ait kişisel veriler üzerindeki karar verme özgürlüğünün ve bu verilerin hukuka aykırı müdahalelere karşı korunması amaçlanmaktadır (Winter, 1997). Kişinin rızası dışında ve hukuka aykırı olarak kişisel verilerin elde edilmesi ve işlenmesi, genel kişilik hakkına ve kişiliğin özgürce geliştirilmesi hakkına da müdahale edilmesi anlamına gelmektedir. Ancak kütüphaneler tarafından toplanan kişisel verilerin hangi amaçla elde edildiği ve hangi amaçla kullanılacağına ilişkin belirsizlikler bulunmakla birlikte, kütüphane üyelerine bu konuda nadiren bilgi verilmekte ve kişisel verilerin korunacağına ilişkin taahhütte bulunulmamaktadır (Preisig, Rösch ve Stückelberger, 2014).

Danışma hizmetleri ve ödünç verme hizmetlerine ilişkin olarak elde edilen kişisel veriler, üniversite kütüphanelerinde korunması gereken önemli bilgi varlıklarıdır. Bununla birlikte, üniversite kütüphaneleri üzerinden sunulan web tabanlı uygulamalarla ilişkili olarak da elde edilen bilgilerin (IP adresi vd.) kişisel veri kapsamında korunması önem taşımaktadır (Avrupa Komisyonu, 2012a). Somut kişilerle eşleştirilen bu bilgiler kullanılarak, ilgili kişinin hayat görüşü hakkında bilgi edinilmesi ve sonrasında (gerekli ortam ve şartlar oluştuğunda) müdahale edilmesi söz konusu olabilmektedir. AB ülkelerinde bu bilgilerin kişi ile ilişkilendirilmesi ve sadece soruşturma kapsamında yetkili makamlarla paylaşılmasına ilişkin hukuksal düzenlemelerin 30-35 yıl önce yapıldığı (Küzeci, 2010) ve günümüzde uygulamada birtakım önlemlerin alındığı görülmektedir (Wildermann, 2014). Türkiye'de ise bu konuya ilişkin hususlara sadece bilgi hizmetleri alanında çalışanların uyması gereken norm, kural ve davranışları belirlemeye yönelik

olarak Türk Kütüphaneciler Derneği (TKD) tarafından kabul edilen "Mesleki Etik İlkeleri"[2] (TKD, 2010) ve TKD tarafından kabul edilen "Düşünce Özgürlüğü Bildirgesi"[3] (TKD, 2008) içinde yer verildiği görülmektedir. Ancak bu ilkelerin uygulamada ne kadar dikkate alındığını gösteren kapsamlı çalışmalar bulunmamaktadır.

Anayasal bir hak olarak tanımlanan kişisel verilerin korunması hakkı, kişinin rızası ya da hukuksal düzenlemelerde yer alan zorunlu haller dışında sınırlanamayan, devredilemeyen ve vazgeçilemeyen temel haklardan biridir. Bu nedenle kamu yararı için dahi olsa, veri sahibinin rızası, yasal dayanağının bulunması, kullanım amacının belirginliği ve sadece amaca yönelik minimum seviyede kişisel bilginin toplanması ve işlenmesi önem taşımaktadır. Veri koruma ve özel hayatın gizliliğinin korunmasına ilişkin olarak dünya genelinde hukuksal düzenlemeler incelendiğinde, özünde bireyin kendisine ait kişisel verileri üzerinde kontrol imkânının sağlanmasının yer aldığı görülmektedir (Aksoy, 2008; Stone, Gueutal, Gardner ve McClure, 1983). Bu çerçevede kişisel verilerin korunmasına ilişkin olarak benimsenen ve üniversite kütüphanelerinin de uygulamalarında dikkate almaları beklenen başlıca temel ilkeler şunlardır (Avrupa Konseyi, 1995; OECD, 2013).

- ◊ Kişisel verilerin toplanması ve işlenmesinin sınırlı olması ilkesi
- ◊ Kişisel veride kalite (tam ve doğru olma) ilkesi
- ◊ Kişisel verilerin toplama ve işlenmesinde amacın belirginliği ilkesi
- ◊ Kişisel verilerin amacına uygun olarak kullanılması ilkesi
- ◊ Kişisel verilerin korunması için gereken tedbirlerin alınması ilkesi
- ◊ Açıklık ilkesi (veri sahibinin bilgilere erişimi ve kurul raporlarının halka açık olması)
- ◊ Kişinin bireysel katılımı (bilgilendirilme ve itiraz) ilkesi
- ◊ Sorumlu tutulabilirlik (veri sorumlularının yükümlülükleri ve uygulanacak yaptırımlar) ilkesi

Veri koruma kanunlarının içeriği detaylı olarak incelendiğinde, kişisel hak ve özgürlüğün veri gizliliğinin korunmasıyla sağlandığı görülmektedir. Veri gizliliği, kişilere sahip oldukları kişisel verilerin gizliliğinin korunmasını isteme hakkını veren bir bilgi güvenliği unsurudur (Chirillo ve Danielyan, 2005). Literatürde bilgi güvenliğinin sadece veri gizliliğini koruma yönüyle ele alındığı ve tanımlamaların bu yönde yapıldığı yayınlar oldukça fazladır. Bu durumun, bilgi güvenliği konusunun daha çok bilişim alanında çalışılması ve hukuksal boyutunun genelde ihmal edilmesinden kaynaklandığı değerlendirilmektedir. Miller'in (Miller, 1971) veri gizliliğini, veri sahibinin verilerinin dolaşımını kontrol yeteneği ve bireyin kendisiyle ilgili verileri kontrol hakkı olarak 44 yıl önce yapmış olduğu tanım, hukuk ve bilişim dünyasının gizlilik anlayışını ortak bir

2 TKD Mesleki Etik İlkeleri, 7. Madde: "Kullanıcıların yaptığı araştırmaların, ödünç aldığı ve/veya yararlandıkları bilgi kaynaklarının neler olduğunun gizliliğini garanti eder, onların kişisel bilgilerini yasal gereklilik dışında kimseyle paylaşmazlar."

3 TKD Düşünce Özgürlüğü Bildirgesi, 8. Madde: "Bilgi merkezlerinde kullanıcıların özel yaşam gizliliğine saygı duyulur. Bu nedenle, kullanıcıların kimliği ve yararlandığı bilgi kaynakları üçüncü kişilere açıklanamaz."

noktada birleştirmektedir. Kişisel verilerin korunmasıyla sadece verinin gizliliğinin değil, kişisel hak ve özgürlüğün korunması da hedeflenmektedir. Hukuksal koşulların dikkate alınmadığı bilgi güvenliği politikalarının kişisel hak ve özgürlüğü korumadan yoksun olacağı açıktır.

Hukuksal Düzenlemeler Kapsamında Kişisel Verilerin Korunması

Anayasa'nın 20. Maddesi kişisel verilerin korunmasını öngörmekte ve kanunda öngörülen hallerde veya kişinin açık rızası ile kişisel verilerin işlenebileceğini söylemektedir (T.C. Anayasası, 1982). Bu madde ile birlikte, üniversitelerde toplanan ve işlenen kişisel veriler üzerinde veri sahipleri mutlak hak sahibidirler. Bu açıdan değerlendirildiğinde, üniversitelerde ve diğer kamu kuruluşlarında idari düzenlemelere bağlı olarak işlenen kişisel verilere ilişkin sorumluluk, idare ve veriyi işleyen tüm personeli kapsamaktadır.

Türk Ceza Kanunu'nda (TCK) da kişisel verilerin korunmasına ilişkin temel ilkeler tanımlanmamış olmasına karşın; kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi ve dağıtılmasına ilişkin düzenlemeler yer almaktadır. Ayrıca TCK'da, kamu hizmetlerine ilişkin olarak kanun hükümleri kapsamında kaydedilen bilgilerin dışında; kişilerin siyasi, felsefi veya dini görüşleri ve ırki kökenlerini gösteren bilgilerin, gerekçesi ne olursa olsun kaydedilmeyeceği düzenlenmiştir. Bu nedenle, üniversitelerde kişisel verilerin işlenmesi ve korunmasına yönelik tüm uygulamalarda TCK'nın da dikkate alınması gerekmektedir. Ancak kişisel verilerin elde edilmesi, işlenmesi/kullanılması ve depolanması gibi bilginin durumunu nitelendiren ve kişisel verilerin korunması açısından çok önemli olan diğer unsurlara yer verilmemiş olması nedeniyle TCK'nın veri korumaya ilişkin eksiklikleri bulunmaktadır. Bunun dışında, haberleşmenin ifşa edilmesine ilişkin düzenlemelerin de (TCK Md. 132/3) üniversite kütüphaneleri tarafından dikkate alınması gerektiği düşünülmektedir. Kullanılacak haberleşme aracının (e-posta, anlık mesajlaşma, telefon vd.) belirtilmemiş olması, danışma hizmetleri kapsamında elde edilen verilerin de bu çerçevede değerlendirilmesine imkân sağlamaktadır. Bilgi profesyonellerinin hukuksal sorumluluklar konusundaki farkındalıklarının arttırılması, Türk Hukuk Mevzuatında yer alan birçok farklı düzenleme içindeki yükümlülüklerin yerine getirilebilmesi açısından önem taşımaktadır.

Türk Hukuk Mevzuatı içerisinde yer alan birçok hukuksal düzenlemede (Anayasa, TCK, 5651 Sayılı Kanun, Medeni Kanun, vd.) doğrudan ya da dolaylı olarak kişisel verilerin korunması konusuna yer verilmiştir. Ancak bu hükümler kişisel verilerin korunması amacıyla değil, ilgili olduğu sahalarda zamanın ihtiyaçlarına cevap vermesi amacıyla hazırlanmıştır. Mevcut hukuksal düzenlemeler, kişisel verilerin korunmasına ilişkin bireysel hakların korunabilmesi için gerekli önleyici tedbirleri içermemektedir. Bu nedenle, modern hukuk sistemlerinde olduğu gibi, Türkiye'de de kişisel verilerin korunmasına yönelik genel bir çerçeve oluşturacak kanunun yürürlüğe girmesi ve kamu kurum ve kuruluşları ile farklı sektörlerin bu kanuna uyum sağlayacak düzenlemeleri yapmaları zorunlu hale gelmiştir. Alınan hukuksal ya da teknik önlemlerin önleyiciliğinin belirlenebilmesi için ise, denetim sistemlerinin geliştirilmesi ve belirli standartlar çerçevesinde aralıklı olarak iç ve dış denetimlerin yapılması gerekmektedir.

Hukuksal olarak kamu kurum ve kuruluşlarının kamusal yarar amacıyla kişisel bilgi elde etmesinde bir engel bulunmamaktadır. Ancak Anayasanın 90. Maddesinde, imzalanan milletlerarası antlaşmaların yasa hükmünde olduğu ve çıkabilecek uyuşmazlıklarda milletlerarası antlaşmaların hükümlerinin esas alınacağı ifade edilmektedir (T.C. Anayasası, 1982). Buna göre, kişisel veriler AİHS'nin 8. Maddesi kapsamında korunmakta ve değerlendirilmektedir. Kişisel verilerin hangi amaçla alındığı konusunda bilgilendirme yapılması, bilginin işlenmesi, kullanımı, saklanması ve transferine ilişkin olarak bireye tanınan haklar, Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) 8. Maddesi kapsamında birey için korunma alanı oluşturmaktadır (Anayasa Mahkemesi, 2011).

Kişisel verilerin korunmasına ilişkin olarak AB ülkelerinde yapılan çalışmaların teknik, hukuksal ve bilgi güvenliği politikaları boyutlarıyla birbiriyle bütünleşmiş olarak yürütüldüğü görülmektedir. Hukuksal düzenlemeler, kişisel verilerin korunması amacıyla yapılan çalışmaların önemli bir parçası olmakla birlikte, uygulamaya dönük resmi dayanağı niteliğindedir. AB veri koruma direktifinin ana unsurunu kişisel verilerin korunması konusu oluşturmaktadır. Bu açıdan bakıldığında, bilgi güvenliği için alınan önlemlerin odak noktası kişisel verilerin korunmasıdır. Ancak Türkiye'de daha çok gizliliğin korunmasına yönelik önlemler alınmaktadır. Türkiye'nin veri koruma kanunu için gerekçeleri temelde AB ile benzer yönler taşımakla birlikte, AB'ye uyum sağlama süreci daha ön planda tutulmakta ve temel hak ve özgürlüklerin korunması amacı KVKK'ya duyulan gereksinimler içinde ikinci öncelikli sırayı almaktadır. Türkiye'ye yönelik raporlarda yer alan eleştirilerin içerisinde kişisel verilerin korunmasına ilişkin hukuksal düzenlemelerin yetersizliğine yapılan vurgu dikkat çekicidir (Avrupa Komisyonu, 2012b).

AB üyelik sürecinde olan Türkiye'nin kişisel verilerin korunmasına ilişkin yaptığı hukuksal düzenlemelerde AB hukuku ile uyumluluğu dikkate aldığı düşünüldüğünde; üniversitelerde AB hukuk normları dikkate alınarak geliştirilecek politikalar, kişisel hakların korunması için daha doğru bir yaklaşım olacaktır (Henkoğlu ve Yılmaz, 2013). Bu süreçte üniversite birimlerinde kişisel verilerin korunmasına yönelik temel ilkeler çerçevesinde bilgi güvenliği politikalarının oluşturulması ve kişisel verileri işleyen personelin bu konudaki farkındalığının arttırılmasının önemli bir başlangıç olacağı değerlendirilmektedir. Bazı AB ülkelerinde iç hukukta ve uygulamada sorumlulukları genişleten farklılıklar bulunabilmektedir. Örneğin İngiltere'de, üniversitelerde kişisel verilerin bulunduğu birimlerde çalışan tüm personelin (doğrudan veriyi işleme ya da dağıtım sorumluluğu olmasa dahi) kişisel ve hassas verilerin korunması ve risklerin azaltılması yükümlülükleri bulunmaktadır. Ayrıca, veri koruma direktifinde tanımlanan ihlâllerin gerçekleşmesi durumunda, önemli miktarda yaptırımlar da (para cezası olarak) uygulanabilmektedir (Johnston, 2011).

Araştırmanın Yöntemi

Kişisel verilerin ve kişisel hakların korunması konusunun kendi koşulları içinde tanımlanması ve açıklanması için, bu çalışmada betimleme yöntemi kullanılmıştır.

Betimleme, geçmişte ya da halen var olan bir durumu veya araştırmaya konu olan olayı kendi koşulları içinde olduğu gibi tanımlamaya çalışan bir araştırma yöntemidir (Karasar, 2012).

Çalışma kapsamında yer alan kişisel veriler, gerçek kişi ile ilişkili olarak değerlendirilmektedir. Veri sahibi olarak veri üzerinde hak sahibi olan şirket ve devlet gibi diğer unsurlar çalışma kapsamı dışında tutulmuştur. Bu çalışmada ağırlıklı olarak, veri sahibinin bilgisi ve izni dışındaki her türlü yetkisiz erişime karşı üniversite kütüphanelerinin hukuksal düzenlemeler çerçevesinde alması gereken önlemler irdelenmektedir.

Örneklem ve Araştırma Evreni

Araştırma evrenini Ankara'da bulunan 5 devlet ve 10 vakıf üniversite kütüphanesi oluşturmaktadır. Araştırmada örneklem alınmamış, tüm evren üzerinde çalışılmıştır. Kuruluş işlemlerini tamamlamış ancak yapılanma çalışmaları devam eden 1 devlet ve 2 vakıf üniversitesi araştırma kapsamına alınmamıştır. Araştırma kapsamında, üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin korunmasına ilişkin hususlar Türk Hukuk Mevzuatı ve AB Hukuk Mevzuatı çerçevesinde incelenmiştir.

Verilerin Toplanması

Araştırma kapsamında üniversite kütüphanelerinden verilerin toplanması amacıyla hazırlanan anket soruları için, ODTÜ ve Hacettepe Üniversitesi'nden etik kurul onayı alınmıştır. Ayrıca, araştırma kapsamında yer alan iki üniversitenin isteği üzerine, etik kurul kararına ilâve olarak Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü tarafından hazırlanan araştırmaya ilişkin üst yazı ile görüşme başvurusu yapılmıştır.

Bu araştırmanın verileri, görüşme ve anket tekniği birlikte kullanılarak elde edilmiş ve bu amaçla üniversite kütüphanelerine yapılandırılmış sorular yöneltilmiştir. Anket yöntemi, üniversite kütüphanelerinden elde edilen verilerin karşılaştırılabilmesine ve verilen cevapların tekrar kontrol edilebilmesine olanak sağlamaktadır (Kaptan, 1995). Uygulanan anketler; katılımcıların sorulara farklı anlamlar verebileceklerinin göz önüne alınması (Karasar, 2012), posta yoluyla yapılan ankete olasılıkla yanıt alma oranının daha yüksek olması ve yanlışlıkları düzeltme, eksikleri tamamlama ve daha sağlıklı bilgi alarak farkındalığı en iyi şekilde ölçebilme olanağı sunması nedeniyle, yüz yüze görüşme yoluyla uygulanmıştır. Kütüphanelerde bilgi güvenliğine ilişkin farkındalığın oluşturulması ve belirlenen politikaların uygulanması konusunda yönetici sorumluluğunu taşıyan kişiler olmaları nedeniyle, görüşme ve anket soruları daire başkanları ya da yardımcılarına yöneltilmiştir. Görüşme ve anketlerle üniversitelerde mevcut bilgi güvenliği politikaları, farkındalık, eğitim durumu ve bilgi güvenliğinin sağlanmasına yönelik uygulamalar hakkında detaylı bilgi alınmıştır.

Uygulanan anket soruları; kişisel verileri işleyen personeli bilinçlendirmek amacıyla yapılan çalışmalar, bilgi güvenliği politikaları hakkındaki farkındalık, kişisel verilerin elde edilmesinden imhasına kadar olan sürecin yönetimi, personel hatalarına ilişkin idari yaptırımlar, bilgi erişim yetkilendirmelerine ilişkin mevcut durum ve bilgi güvenliği konusundaki tüm uygulamalar hakkında bilgi sağlayacak içerikte hazırlanmıştır. Araştırma için hazırlanan anket soruları tek seçimli sorular, çok seçimli sorular, dizi soruları, yanıtı tanımlı sorular ve uygulamaya ilişkin görüşlerin alınabileceği açık uçlu sorulardan oluşmaktadır. Anket sorularına ilişkin eksikliklerin belirlenebilmesi amacıyla üç üniversitede pilot (ön) çalışma uygulanmış ve öneriler doğrultusunda anket soruları tekrar düzenlenmiştir. Görüşme ve anket sorularının hazırlanmasında; uluslararası bilgi güvenliği standartları, diğer kurumlarda yapılmış olan bilgi güvenliği denetimleri sonucunda yayınlanan raporlar, kişisel verilerin korunmasına yönelik etik ilkeler, AB Veri Koruma Direktifi ve kişisel hakların korunmasına ilişkin hukuksal düzenlemelerden faydalanılmıştır.

Çalışma kapsamında yanıt aranan araştırma soruları şunlardır;

1. Mevcut yasal düzenlemeler kütüphanelerde kişisel verilerin korunmasına ilişkin kişisel hak ve özgürlüğü koruyabilecek yeterliliği taşımakta mıdır?
2. Üniversitelerde yazılı bilgi güvenliği politikaları mevcut mudur? Kütüphanelerde kişisel verilerin işlenmesi ve korunmasına yönelik politikalar belirlenmiş midir?
3. Kütüphanelerde gereğinden fazla hassas ve kişisel bilgi işlenmekte midir? Verilerin ne kadar süreyle saklanacağı konusunda politikalar belirlenmiş midir?
4. Mevcut bilgi güvenliği politikaları içinde kişisel verilerin korunmasına ilişkin önlemlere yer verilmiş midir?
5. Verilerin korunmasına yönelik önlemler hangi boyutlarda ve nasıl alınmaktadır? Bilgi yönetim stratejileri ve risk yönetimi planı var mıdır?
6. Kişisel verileri işleyen personel, kişisel verilerin hangi amaçla, ne kadar süreyle ve kim tarafından işleneceği konusunda eğitim almış mıdır? Bu konudaki meslek içi eğitim durumu ve ihtiyacı nedir?
7. Kütüphanecilerin bilgi güvenliği ve kişisel verilerin korunması konusundaki farkındalığı ve görüşleri nelerdir?

Bulgular ve Değerlendirme

Araştırma sonucunda nicel bulguların yanı sıra açık uçlu sorulara verilen yanıtlardan ve görüşmeden de veriler elde edilmiştir. Açık uçlu sorular ile elde edilen veriler ilgili konu başlıkları altında gruplandırılarak birlikte değerlendirilmiştir.

Araştırma verilerinden elde edilen bulgulara bağlı olarak; hukuksal düzenlemelerin yeterliliği, kişisel verilerin korunmasına ilişkin bilgi güvenliği politikaları, üniversite kütüphanelerinde kişisel verilerin toplanması, düzenlenmesi ve güncellenmesi, kişisel

verilerin kullanımı ve paylaşımı, kişisel verilerin korunması amacıyla alınan bilgi güvenliği önlemleri ve bunların hukuksal düzenlemelere uyumluluğu, verilerin korunmasına ilişkin sorumluluklar, bilgi güvenliğine ilişkin risk durumu ile eğitim ve farkındalık durumu değerlendirilerek araştırma sorularına cevap aranmaktadır. Soruların tamamı tüm katılımcılar (N=15) tarafından yanıtlanmıştır.

Üniversitelerde Hukuksal Düzenlemeler ve Kişisel Verilerin Korunmasına İlişkin Bilgi Güvenliği Politikaları

Üniversite kütüphanelerinde kişisel verilerin korunmasına ilişkin olarak kütüphane daire başkanlarına (KDB) ne gibi sorumlulukları olduğu sorulmuş ve bunu hukuksal düzenlemeler çerçevesinde belirtmeleri istenmiştir. Katılımcıların Tablo I'de yer alan hukuksal düzenlemeler içerisinde birden fazla seçeneği işaretlemelerine olanak sağlanmıştır.

Tablo I: Hukuksal Düzenlemeler Çerçevesinde Sorumluluklar

Kişisel verilerin korunmasına ilişkin olarak hangi hukuksal düzenlemeler çerçevesinde sorumluluklarınız olduğunu düşünüyorsunuz?		
	N	%
T.C. Anayasası	7	46,7
Türk Ceza Kanunu	6	40
5651 Sayılı Kanun	4	26,7
KVKK Tasarısı	7	46,7
AB Veri Koruma Kanunu	2	13,3
Hukuksal çerçevede sorumluluğumun olduğunu düşünmüyorum	2	13,3
Fikrim Yok	3	20
Değerlendirme Dışı	-	-

Kişisel verilerin korunmasıyla ilişkili olarak katılımcıların yaklaşık olarak yarısı (%46,7) Anayasa ve KVKKT (%44,2) çerçevesinde sorumluluklarının olduğunu düşünmektedirler. Katılımcıların %73,3'ü 5651 sayılı kanun çerçevesinde sorumluluklarının bulunmadığını düşünürken; KVKKT kapsamında daha fazla sorumluluklarının olduğunu düşünmeleri dikkat çekicidir. Katılımcılar içeriği hakkında tam olarak bilgi sahibi olmadıklarını belirtmekle birlikte, KVKKT ile uygulamakta oldukları etik kuralların daha fazla ortak yönünün olabileceğini düşünerek bu seçeneği işaretlediklerini ifade etmişlerdir. Görüşme esnasında hukuksal düzenlemeler çerçevesinde sadece Anayasa ve TCK ile ilgili sınırlı sorumlulukları olduğunu düşünen katılımcılar, hukuksal düzenlemelerin yetersiz olduğunu ve bu nedenle kişisel verilerin korunmasına ilişkin olarak daha çok etik kurallar kapsamında sorumluluk hissettiklerini ifade etmişlerdir. Hukuksal düzenlemeler üzerinde yapılan inceleme sonuçları da mevcut yasal düzenlemelerin üniversite kütüphanelerinde kişisel verilerin korunmasına ilişkin kişisel hak ve özgürlüğü

koruyabilecek yeterliliği taşımadığını göstermektedir. Kişisel verilerin korunmasına yönelik hukuksal düzenlemelerin yetersizliği göz önüne alındığında, mesleki etik kurallara olan ihtiyacın önemi daha fazla anlaşılmaktadır. Görüşme esnasında katılımcıların büyük çoğunluğu bu konunun hukuk mevzuatı içinde çok dağınık bir şekilde işlendiği ve bu nedenle mevzuat içerisinden sorumluluklarının belirlenmesinin kendileri için mümkün olmadığını da ifade etmişlerdir. İki katılımcı hukuksal düzenlemeler çerçevesinde herhangi bir sorumluluğunun bulunmadığını belirtmektedir. Üç katılımcı ise kişisel verilerin korunmasıyla ilgili olarak hukuksal düzenlemelere hiç bakmadıklarını ve bu nedenle fikir sahibi olmadıklarını belirtmektedir.

Görüşme esnasında katılımcıların %77'sinin hukuksal düzenlemelerin içeriği hakkında bilgi sahibi olmadıklarını ifade etmeleri, yapılan işlemler ve alınan önlemler içerisinde hukuksal düzenlemelerin dikkate alınmasında da eksikliklerin bulunduğunu göstermektedir. Görüşmelerde hukuksal düzenlemelerin dağınık olmasına vurgu yapılsa da, hukuksal düzenlemeleri inceleme konusunda eksikliklerin bulunduğu belirgin olarak gözlenmiştir. Araştırmada elde edilen bulgular göz önüne alındığında, genel olarak hukuksal düzenlemeler katılımcılar için anlaşılması ve uygulanması zor belgeler olarak nitelendirilebilir. Bu nedenle teknik önlemlerin yanı sıra üniversite kütüphanelerinde hukuksal düzenlemelerin de dikkate alınabilmesi için, katılımcıların hukuk okuryazarlığı konusunda daha iyi seviyede olmaları sağlanmalıdır. Katılımcıların %40'ının özellikle kişisel verilerin korunması konusunda etik kuralları hukuksal düzenlemelerden daha uygulanabilir bulmalarında, hukuksal düzenlemeleri inceleme konusundaki çekincelerinin de etkisi olduğu söylenebilir. Bu konuda örnek alınabilecek AB KVKK gibi hukuksal belgelerin katılımcıların büyük bölümü (%90) tarafından hiç incelenmemiş olması, katılımcıların bu konudaki düzenlemelere olan ilgilerinin düşük olduğunu göstermektedir.

Üniversitelerde yazılı bilgi güvenliği politikalarına ilişkin mevcut durumun tespit edilmesi amacıyla araştırma kapsamında yer alan üniversitelerin web sayfaları üzerinde içerik analizi yapılmıştır. Ancak üniversite birimleri tarafından sorumlulukların paylaşıldığı bir yazılı bilgi güvenliği politikası bulunamamıştır. Üniversite web sayfalarından elde edilen veriler, üniversitelerde bilgi güvenliği sorumluluğunun sadece teknik boyutu ile değerlendirildiğini ve bu konudaki sorumluluğun BİDB birimi tarafından üstlenildiğini göstermektedir. Üniversitelerin BİDB birimlerine ait web sayfalarında görülen bilgi güvenliği politikaları ise, kişisel verilerin korunmasına ilişkin ihtiyacı karşılayabilecek maddeleri içermemektedir. Katılımcıların yazılı bilgi güvenliği politikasının varlığıyla ilgili olarak vermiş oldukları yanıtlar da web sayfaları üzerinden yapılan ön araştırma sonuçlarını doğrulamaktadır. Üniversitelerde yayınlanmış kapsamlı bilgi güvenliği politikalarının bulunmaması, bilgi güvenliğine ilişkin olarak alınan güvenlik önlemlerinin sadece teknik önlemlerle sınırlı kalmasına ve birimler arasındaki koordinasyonun sağlanamamasına neden olmaktadır. Ancak Charette'nin de belirttiği gibi (Charette, 2012a, 2012b); sadece teknik önlemlerin alınması ile bilgi güvenliği ihlallerinin önüne geçilmesi mümkün değildir. Katılımcıların

%86,7'si kişisel verilerin korunmasına yönelik bilgi güvenliği politikalarının iş süreci ve sorumlulukların tanımlanmasına katkı sağlayacağı görüşünde birleşmektedirler. Bir katılımcı bilgi güvenliği politikalarının iş süreci ve sorumlulukların belirlemesine katkı sağlamayacağını düşündüğü halde, uygulamaya dönük açıklamaları ve beklentileriyle vermiş olduğu yanıtı çelişkili hale getirmiştir. Bu katılımcı, 5651 sayılı kanun gibi bazı hukuksal düzenlemelerin üniversitelerin yapısına uygun olmadığı için tam anlamıyla uygulanamadığını ve bu nedenle üniversitelerin bu tür düzenlemeleri dikkate alarak kendi uygulama politikalarını belirgin hale getirmelerinin zorunlu olduğunu ifade etmektedir. Olumlu görüş bildiren katılımcılar, yazılı bilgi güvenliği politikalarının iş sürecini kolaylaştırmanın da ötesinde; sorumlulukların belirlenmesi, birimler arasındaki koordinasyonun sağlanması ve eksikliklerin giderilmesi için bir zorunluluk haline geldiğinin önemini vurgulamaktadırlar.

Hukuksal düzenlemelerin yanı sıra katılımcılara üniversite kütüphanelerinde dikkate alınan mesleki etik ilkeler ve uluslararası standartların olup olmadığı da sorulmuştur. Katılımcıların %40'ı dikkate aldıkları mesleki etik ilkeler ve standartların bulunduğunu belirtmişlerdir. Bu soruya "Evet" yanıtını veren katılımcılar "Türk Kütüphanecileri Derneği (TKD) Mesleki Etik İlkeleri"ni dikkate aldıklarını belirtmektedirler. Katılımcıların mesleki etik ilkelerin uygulanmasına yönelik görüşleri ile üniversitenin yapısı (vakıf ya da devlet üniversitesi) arasında ilişki bulunmamaktadır.

Verilerin Toplanması, Düzenlenmesi ve Saklanması

Üniversite kütüphanelerinde genel olarak kişisel verilerin elde edilmesine ilişkin herhangi bir düzenleme, kriter ya da standart bulunmamaktadır. Katılımcıların %92,3'ü kişisel veriler elde edilirken "gerekli minimum bilginin" toplandığının altını çizmektedirler. Araştırma kapsamında katılımcılardan kişisel hak ve özgürlüklerin korunmasıyla ilişkili olarak, üniversite kütüphanelerinde danışma hizmetleri kapsamında elde edilen verilerin, veri sahibinin bilgisi dışında kişisel verilerle ilişkilendirilip ilişkilendirilmediğini belirtmeleri istenmiştir. Katılımcıların %86,7'si kütüphanelerde danışma hizmetleri kapsamında tutulan bilgilerin kullanıcılarla ilişkilendirilmediğini belirtmişlerdir. Ancak görüşme esnasında katılımcıların %53,6'sı bu uygulamanın kişisel verilerin korunması amacıyla değil, ihtiyaç duyulmaması nedeniyle yapıldığını ifade etmişlerdir. Bu katılımcılar farklı bir soruya vermiş oldukları yanıtta da, "danışma hizmetleri kapsamında edinilen bilgilere ilişkin kayıtların" hassas ya da kişisel veri olarak korunması gerektiğini düşünmediklerini belirtmektedirler. Bu nedenle danışma hizmetleri kapsamında tutulan bilgilerin kullanıcılarla ilişkilendirilmediğini gösteren araştırma bulguları, bilgi güvenliğine ilişkin önlemler kapsamında bilinçli olarak yapılan bir uygulamanın sonucu olduğu söylenemez.

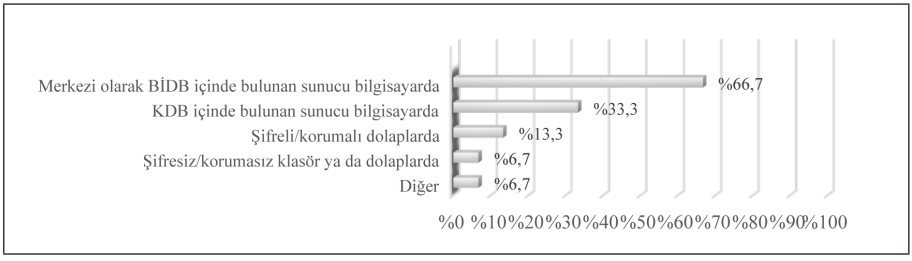
Katılımcılara üniversite kütüphanelerinde kullanıcı kayıtlarının gizlilik derecelerine göre sınıflandırılıp sınıflandırılmadığı sorulmuş ve görüşme esnasında ayrıca uygulamanın gerekçeleri hakkında bilgi alınmıştır. Bu konuda katılımcıların büyük

bölümü (%78,6) kullanıcı kayıtlarının öğrenci ve personel bilgi sistemi üzerinden alındığı gerekçesiyle kendileri tarafından ayrıca sınıflandırma yapılmasına ihtiyaç duyulmadığını ve bu verilerin sahibine karşı sorumluluk hissetmediklerini belirtmektedirler. Elde edilen verilerin sınıflandırılması konusundaki eksikliklerin temelinde bu bilgilerin kişisel veri kapsamında değerlendirilmemesi olduğu söylenebilir. Üniversitelerde kişisel verilerin korunmasına yönelik bir politikanın bulunmaması nedeniyle, hangi verilerin kişisel veri niteliğinde olduğu ve hangi verilerin gizlilik seviyesine göre sınıflandırılması ve korunması gerektiği hakkında belirsizlikler bulunmaktadır. Bununla beraber kişisel bilgilerin farklı bir üniversite birimi ya da personelin kendisi tarafından bir sistem üzerine aktarılmış olmasının bu sisteme erişim sağlayan tüm kurum, kuruluş ya da üniversite birimleri tarafından alınarak herhangi bir kısıtlama olmaksızın kullanılabileceği şeklinde yorumlanması, kişisel hak ve özgürlüğün sınırlandırılmasına neden olabilmektedir. Bu tür uygulamalar; Winter'in kullanıcıların kendilerine ait kişisel bilgilerin ne zaman, nasıl ve ne kadarının başkalarının erişimine açılacağına karar vermeleridir (Winter, 1997) şeklinde tanımladığı ve 95/46/EC sayılı AB direktifinin yaklaşımıyla da örtüşen "gizlilik" anlayışı ile bağdaşmamaktadır. 95/46/EC sayılı AB direktifi, 108 Sayılı Sözleşme, TCK ve KVKKT'de de açıkça belirtildiği gibi, kişisel verilerin diğer kurum, kuruluş ya da üniversite birimleri tarafından nasıl elde edildiğine bakılmaksızın, bu verilerin farklı bir kurum ya da üniversite birimi tarafından kullanılması konusunda kişinin rızasının alınması ve gizliliğinin korunması gerekmektedir.

Üniversite kütüphanelerinde kayıtların ne kadar süre saklandığı ve saklama koşulları için dikkate alınan yazılı politikaların olup olmadığı sorusuna ilişkin olarak sadece dört katılımcı (%26,7) kullanıcı kayıtlarının bir yıl, beş yıl ya da mezuniyet sonrasında silindiği yanıtını verirken; diğer 11 KDB biriminde bu sürenin belirlenmemiş olması ve bir katılımcının kayıtların sonsuza kadar silinmeyeceğini ifade etmesi dikkat çekicidir. Kullanıcı kayıtlarının, kullanıcının bilgi ve rızası olmaksızın sonsuza kadar saklanması ya da bu şekilde bir politikanın belirlenmesinin kişisel hakların ihlaline neden olabileceği düşünülmektedir. Üniversite kütüphanelerinde verilerin elektronik ortamda saklanmasının da bu konudaki belirsizliklerin oluşmasında etkili olduğu düşünülmektedir. Ancak bu durumda hukuksal olarak elektronik ortamda yer alan bilgilerin de yazılı-basılı ortamlarda bulunan bilgilerle aynı saklama ve koruma şartlarına sahip olması (T.C. Başbakanlık, 1988) ve aynı imha süreçlerinin uygulanması gerektiği göz ardı edilmektedir. Aynı hukuksal nitelikte olmasına karşın, elektronik bilgilerin saklanması ve imha koşullarının daha karmaşık olması ve Türk hukuk Mevzuatında bu konuya ilişkin yeterli düzeyde düzenlemelerin bulunmaması, konuyu daha karmaşık ve belirsiz hale getirmektedir. Bu belirsizliklerin giderilmesi için, bilgi merkezlerinde verilerin saklanmasına ilişkin hukuksal sorumlulukları içeren derslere lisans ve mesleki eğitim programlarında daha fazla yer verilmesi gerektiği düşünülmektedir.

Katılımcılara verilerini hangi ortamlarda, nerede ve nasıl sakladıkları sorulmuş ve yanıtlar Şekil 1 üzerinde gösterilmiştir. Katılımcıların Şekil 1'de yer alan birim ve kayıtlara

ilişkin birden fazla seçeneği işaretlemelerine olanak sağlanmıştır.



Şekil 1: Personel ve Kullanıcı Kayıtlarının Saklandığı Ortamlar

Elde edilen bulgular, birden fazla ortamda elektronik ve yazılı-basılı bilgilerin bulunduğunu göstermektedir. KDB birimlerinde elektronik ortamda işlenen kişisel verilerin %66,7'si BİDB sorumluluğunda bulunan veri tabanlarında saklanmaktadır. Beş katılımcı (%33,3), BİDB ile birlikte ya da sadece kendi birimleri içinde yer alan ve sorumluluklarının bulunduğu sunucular üzerinde verilerini sakladıklarını belirtmektedirler. Ancak araştırmada elde edilen bulgular, bu verilerin sorumluluğunun nasıl paylaşılacağı konusunda yazılı politikaların bulunmadığını ve bu konuya ilişkin koordinasyonun yapılmadığını göstermektedir. Bununla birlikte, katılımcılar tarafından üniversitelerde bu tür kapsamlı bilgi güvenliği koordinasyon toplantılarının yapılmasına ilişkin çalışmaların da bulunmadığı ifade edilmektedir. Bu durum, herhangi bir veri ihlali olması durumunda birimlerin ihtilafa düşmesine neden olabileceği gibi, bilişim suçlarında çözüm ve sonuca ulaşmada en önemli unsurlardan biri olan zaman yönetim sürecini de olumsuz etkileyebilecektir. Katılımcıların şifreli ya da korumalı dolap kullanım oranı %13,3'ü geçmemektedir. Katılımcıların yazılı-basılı belgeler için belirtmiş olduğu şifresiz ya da korumasız dolap kullanım oranının da (%6,7) düşük olması dikkat çekicidir. Görüşme esnasında katılımcılar bilgi ve belgelerinin tamamen elektronik ortamda saklandığını ve bu nedenle diğer saklama ortamlarına yazılı-basılı belge için sınırlı olarak ihtiyaç duyduklarını belirtmişlerdir.

Kişisel Verilerin Kullanımı ve Paylaşımı

Üniversite kütüphanelerinde kişisel verilerin (kullanıcı kayıtlarının) hangi koşullarda paylaşıldığı katılımcılara sorulmuş ve katılımcıların bu konudaki görüşleri Tablo II üzerinde gösterilmiştir. Katılımcıların Tablo II'de yer alan tercihlere ilişkin birden fazla seçeneği işaretlemelerine olanak sağlanmıştır.

Tablo II: Üniversite Kütüphanelerinde Kullanıcı Kayıtlarının Paylaşımı

Kullanıcılara ait kayıtların hangi gerekçe ile paylaşımına izin verilmektedir?		
	N	%
Yasal çerçevede savcılık tarafından istenmesi durumunda	9	60
Bilgi Edinme Hakkı Kanunu çerçevesinde	3	20
İstatistiksel amaçlı olarak istenmesi halinde	-	-
Bilimsel araştırmada kullanılmak şartıyla	-	-
Üniversite üst yönetimi tarafından istenmesi halinde	13	86,7
Kamu menfaati görülmesi halinde (kişisel haklar gözetilmeksizin)	1	6,7
Veri sahibinin kendisi hakkında tutulan bilgileri istemesi halinde	11	73,3
Kullanıcı bilgileri hangi sebeple olursa olsun verilmez.	-	-

Üniversite kütüphaneleri tarafından elde edilen kişisel bilgilerin paylaşımı konusunda tüm katılımcıların duyarlı olduğu görülmektedir. Ancak üniversite tarafından belirlenmiş ya da hukuk kaynaklarında bu konuya ilişkin düzenlemelerin bulunmaması, kişisel görüş ve uygulamaların daha fazla öne çıkmasına neden olmaktadır. Katılımcılar, bu bilgilerin istatistiksel amaçlı, araştırmalarda kullanılması amacıyla ya da kişisel haklar gözetilmeksizin kamu menfaati için paylaşılmasını kesinlikle doğru bulmamaktadırlar. Bu sorulara verilen yanıtlarda üniversite kütüphanelerinin uygulamalarından kaynaklanan farklılıklar bulunmaktadır. Örneğin bazı üniversitelerde birimlerin savcılığa doğrudan bilgi vermesi sürecin işleyişine uygun olarak kabul edilirken, bazı üniversitelerde bunun ancak üniversite üst yönetiminin (ya da idari amir) onayı ya da aracılığıyla mümkün olabileceği görüşü benimsenmektedir. Ancak görüşme esnasında elde edilen verilere göre, üst yönetimin ya da idari amirin onayını alma eğiliminin üniversite yapılanması (devlet ya da vakıf) ya da üst yönetimin bu yöndeki tutumu ile ilişkisi bulunmamaktadır.

Tablo II üzerinde katılımcıların Bilgi Edinme Hakkı Kanunu (BEHK) çerçevesinde bilgi paylaşımına ilişkin oranının düşük (%20) olması dikkat çekicidir. Görüşme esnasında bu seçeneği işaretlemeyen katılımcıların bilgi merkezlerinden istenilebilecek verilerin bulunmadığını belirtmeleri ise düşündürücüdür. Kullanıcı bilgilerinin diğer üniversite birimleri tarafından elde edildiği ya da merkezi veri depolama alanlarında saklandığı düşünülse dahi, bu bilgilerin kütüphaneler tarafından verilen hizmetlerle ilişkilendirilmesi yapılmaktadır. Bu koşullarda oluşturulan tüm yeni kayıtların kütüphanelerin sorumluluğunda olduğu değerlendirilmektedir. Üniversite kütüphanelerinin BEHK kapsamında yapılacak başvurulara ilişkin olarak, gerekli idarî ve teknik önlemleri almak suretiyle Kanun'da belirtilen sınırlar içinde bilgi verme yükümlülükleri bulunmaktadır.

Katılımcılara kişisel bilgilerin paylaşılması durumunda veri sahibine bilgi verip vermemeleri konusundaki düşünceleri de sorulmuştur. Katılımcıların %80'i kişisel bilgilerin paylaşılması durumunda veri sahibine bilgi verilmeyeceğini ya da kısmen

bilgi verileceğini belirtmektedir. Ancak görüşme esnasında bunun nedeni olarak, savcılık ya da üniversite üst yönetimi tarafından istenen bilgilerin genellikle soruşturma kapsamında ve gizlilik içerisinde yürütülüyor olması gerekçe gösterilmiştir. Bu açıdan bakıldığında da, katılımcıların durumun önem ve niteliğine bağlı olarak tercihlerini belirlemede tereddüt etmeyecekleri anlaşılmaktadır. Katılımcıların bu konuda göstermiş oldukları sorumluluk almama eğilimi ile meydana gelen olayları öncelikle idari amirlerine yönlendirme ya da idari amirlerle paylaşma eğilimleri arasında doğrusal ilişki bulunmaktadır.

Katılımcılara ayrıca, elde edilen kişisel bilgilerin amaç dışı kullanılmayacağı, izinsiz olarak paylaşılmayacağı ve bu verilerin korunacağına ilişkin olarak veri sahibine yazılı taahhütte bulunup bulunmadıkları sorulmuştur. Katılımcıların %93,3'ü kişisel bilgilerin elde edilmesi sürecinde veri sahibine herhangi bir taahhütte bulunmadıklarını belirtmektedirler. Bu nedenle, uygulamada verilerin korunması, sınırlı hukuksal düzenleme ve üniversitelerin dikkate almış oldukları etik değerlere bağlı olarak sağlanmaktadır. Görüşme esnasında elde edilen verilere göre, katılımcılar ağırlıklı olarak bilgileri mevcut sistemler (personel ve öğrenci bilgi sistemleri gibi) üzerinden alıyor olmaları nedeniyle bu konuda sorumluluklarının bulunmadığını düşünmektedirler.

Kişisel Verilerin Depolanması ve Korunmasına İlişkin Sorumluluklar

Katılımcılardan kişisel verilerin korunmasına yönelik birtakım teknik önlemlerin alınması konusunda kendilerinin ve bu verileri işleyen personelin sorumluluklarının olup olmadığını belirtmeleri istenmiştir. Katılımcıların %46,7'si bu konuda sorumluluklarının bulunduğunu düşünmektedirler. Bu sonuç ile verilerin merkezi olarak KDB içinde saklanma oranları arasında doğrusal ilişki bulunmaktadır. Oysa bilgi işlem sorumlularının bulunmadığı ve merkezi denetim ve kontrollerin yapılamadığı üniversite kütüphanelerinde, bireysel olarak da birtakım sorumlulukların üstlenilmesi gerekmektedir. Bilgisayarların kötü amaçlı kişiler tarafından veri depolama ortamlarına uzaktan erişim aracı olarak kullanılma risklerinin azaltılabilmesi için, sistem güvenlik yamalarının güncellenmesi gibi temel teknik önlemlerin alınması önem taşımaktadır. Kişisel verilerin işlendiği bilgisayarlar üzerinden yapılan erişimlerle, tüm güvenlik duvarlarının aşılması ve istenilen bilgilerin elde edilmesi mümkün olabilmektedir. Katılımcılar tarafından teknik önlemlerin alınmasına ilişkin olarak ifade edilen sorumlulukların bazıları; kişisel verilerin işlendiği bilgisayarlar üzerindeki güvenlik yazılımlarının güncelliğinin korunması için BİDB ile koordinasyonun sağlanması, kütüphanelerdeki kullanıcı erişim kayıtlarının temizlenmesi, sistem erişim yetkilendirmelerinin güncellenmesi ve KDB içinde bulunan sunucuların güvenliğinin sağlanmasdır. Teknik sorumlulukların yerine getirilmesi kapsamında katılımcıların %53,3'ü, kütüphanelerde kullanıcıların araştırma ya da katalog tarama amacıyla kullanmış oldukları bilgisayarların kayıtlarının düzenli olarak temizlendiğini ifade etmektedirler.

Katılımcılara olası ihlaller karşısında uygulanacak yaptırımların belirlenip belirlenmediği ve ne tür yaptırımların uygulanmasının öngörüldüğü de sorulmuştur. Katılımcıların sadece %26,7'si uygulanacak yaptırımların belirlenmiş olduğunu ifade etmektedir. Yaptırımların belirlenmiş olduğunu ifade eden katılımcılar; yazılı ya da sözlü uyarı, disiplin soruşturmaları ve cezaları, idari para cezası, işten uzaklaştırma ve kanunlar çerçevesinde öngörülen diğer yaptırımların uygulanabileceğini belirtmektedirler. Bu yaptırımların bir personelin kişisel verisinin açığa çıkması ya da kötü amaçlı olarak kullanılması karşısında ne kadar yeterli ve etkili olabileceği tartışmalıdır. Ancak Türk Hukuk Mevzuatı incelendiğinde, kişisel verilerin korunması konusunda önleyici tedbir olarak tanımlanabilen ve üniversiteler tarafından uygulanabilecek farklı yaptırımların da bulunmadığı görülmektedir. Bununla birlikte katılımcıların tamamı görüşme esnasında henüz böyle bir durumla karşılaşmadıklarını ifade etmişlerdir.

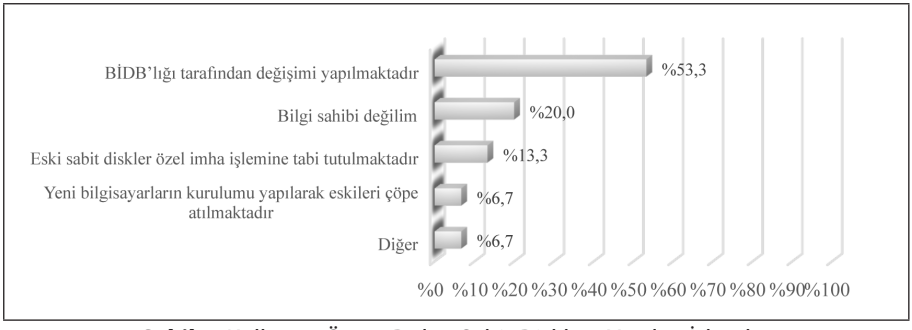
Araştırma kapsamında yer alan ve kendi sunucularını işleten beş üniversite kütüphanesinin dördünde veri yedekleri alınırken; birim içinde bulunan ve üzerinde kişisel bilgilerin de tutulduğu bilgisayarların veri yedeklerinin alınmadığı görülmektedir. Bu nedenle kütüphanelerde işlenen verilerin merkezi veri depolama birimlerine aktarılmasının, veri güvenliği ve yedekliliğinin sağlanması açısından da önem taşıdığı düşünülmektedir. Üniversite kütüphanelerindeki bilgisayarlar üzerinde bulunan verilerin nasıl ve kimin sorumluluğunda yedekleneceğine ilişkin olarak da belirsizlikler bulunmaktadır. Bu belirsizliklerin ortadan kaldırılabilmesi için, üniversitelerin kurumsal bilgi güvenliği politikalarına bağlı olarak kütüphaneler için veri yedekleme politikalarının geliştirilmesi ve kütüphane bilgi işlem sorumluları tarafından veri yedekleme faaliyetlerinin yürütülmesi sağlanmalıdır.

Üniversite kütüphanelerindeki bilgisayarların dışarıdan yapılabilecek saldırılara karşı risk durumunu değerlendirebilmek amacıyla katılımcılara kişisel verilerin de işlendiği bilgisayarların internet bağlantı durumu sorulmuştur. Katılımcıların %86,7'sinden KDB'de kullanılan tüm bilgisayarların internete bağlı olarak çalıştığı yanıtı alınmıştır. Bu durum üniversite kütüphanelerinde bilgi güvenliği açısından risk oranını arttırmaktadır. Bununla birlikte, bilgi varlıklarının değerlendirmesi yapılmayan, risk analiz raporu bulunmayan ve yazılı eylem planı olmayan üniversite kütüphanelerinin risk ve tehditler karşısında sistematik olarak mücadele edebilme gücünün bulunmadığı değerlendirilmektedir. Ayrıca araştırma kapsamındaki üniversite kütüphanelerinin %33'ünde, üzerinde kişisel verilerin bulunduğu ve üniversite kütüphaneleri tarafından işletilen sunucular bulunmaktadır. Düzenli olarak güncellemeleri ve denetimleri yapılmayan bu sunucular da risk alanının genişlemesine neden olmaktadır.

Kişisel Verilerin İmha Edilmesi ve Sistem Kayıtlarının Temizlenmesi

Üniversite kütüphanelerinde verilerin işlem öncelikleri ve kullanım süresi sona eren verilerin imhasına yönelik işlemlerin nasıl yapıldığına ilişkin katılımcılardan elde edilen bilgiler Şekil 2 üzerinde gösterilmiştir. İmha sorumluluğu ve kütüphanelerde buna ilişkin

işlemlerin yapılmasına yönelik soruların katılımcılar tarafından daha iyi anlaşılabilmesi amacıyla, "kullanım süresi dolan sabit diskler" imha edilecek bilgi deposu örneği olarak kullanılmıştır.



Şekil 2: Kullanım Ömrü Dolan Sabit Disklere Yapılan İşlemler

Kullanım süresi dolan sabit diskler konusunda BİDB'nin sorumlu olduğunu düşünen ya da bilgi sahibi olmadığını ifade eden katılımcıların oranı oldukça yüksektir (%73,3). Şekil 2 üzerin3de yer alan verilere göre sabit disk değişiminin BİDB tarafından yapıldığını belirten katılımcıların tamamı, kalıcı silme ve özel imha işlemleri konusunda da BİDB'nin sorumlu olduğunu düşünmektedirler. Elektronik verilerin imha işlemi üniversite birimlerinde çalışan herhangi bir personel tarafından yapılabilecek bir işlem olmadığı gibi, BİDB personeli tarafından da bu tür işlemlerin uygun standartlarda yapılabilmesi için özel bilgi, uzmanlık ve zamana ihtiyaç duyulmaktadır. Bu ve bilgisayar sayısına karşılık personel sayısının yetersizliği gibi nedenlerden dolayı, üniversite BİDB tarafından verilerin imhasına ilişkin olarak birimlere verilebilecek desteğin sınırlı olabileceği değerlendirilmektedir. Bu nedenle üniversite kütüphaneleri için bir veri imha politikasının geliştirilmesi ve BİDB ile koordineli olarak uygulanması daha fazla önem taşımaktadır. Katılımcıların %13,3'ü bu tür sabit disklere kendi birimlerinde özel imha işlemi uygulandığını belirtmektedirler. Ancak tamamen kullanım dışı kalan bilgi sistemlerinin özel imha işlemlerine tabi tutulması gerektiği bilincinin üniversite kütüphanelerinde veri işleyen tüm personelde oluşturulması da önem taşımaktadır.

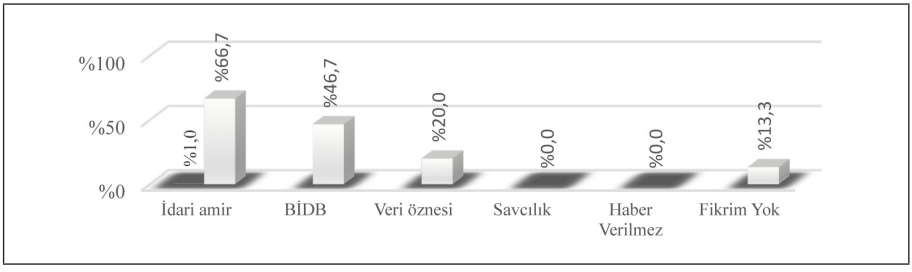
Kanunların belirlediği süre içinde verilerin imha edilmesine ilişkin olarak üniversite kütüphanelerinin hukuksal sorumlulukları da bulunmaktadır. Ancak TCK'nın 138. Maddesinde verileri yok etmeme suçu düzenlenmiş olmakla birlikte; kullanım süresi sona eren verilerin kanunda belirtilen süre sonuna kadar bekletilmesine izin verilmesi ve nasıl bir imha yönteminin kast edildiğinin açık olmaması nedeniyle bu düzenlemenin yetersiz olduğu değerlendirilmektedir. Bununla birlikte, en geç kanunda belirlenen süre sonunda verilerin imha edilmesi açısından hukuksal düzenlemelerin dikkate alınması önem taşımaktadır. Üniversitelerde imha süresi dolan bilgilerin zamanında imha edilmesi konusundaki tutumun değişebilmesi için, üniversitelerin kanun ve yönetmelikler kapsamındaki sorumluluklarını veri imha politikalarında belirlenmesi gerekmektedir.

Bilgi Güvenliğinin Sağlanmasına İlişkin Eğitim ve Farkındalık

Bilgi güvenliğinin sağlanmasına yönelik eğitim ve farkındalığa ilişkin sorular hazırlanırken; katılımcıların konuya ilişkin olarak almış oldukları eğitim, bilgi düzeyi ve farkındalıkları ayrı ayrı ölçülerek, alınan eğitimin farkındalığa dönüşümüne ilişkin bilgilerin de elde edilmesine çalışılmıştır. Sorular hukuksal düzenlemelerin ve alınan teknik önlemlerin yetersizliği karşısında katılımcıların ne tür önlemler aldıkları ve eksikliklerin giderilmesi için hangi yöntemlerin etkin olabileceğini düşündüklerini anlamaya yönelik olarak hazırlanmıştır. Bu amaçla katılımcılara; bilgi varlıklarının korunmasına ilişkin eğitim ve toplantı durumu, veri ihlali olması halinde uygulanacak eylem planı, hassas ve kişisel veri kapsamında değerlendirilen bilgilerin neler olduğu ve kişisel verilerin korunmasına yönelik önlemlerin önceliğine ilişkin sorular yöneltilmiştir.

Katılımcıların %93,3'ü bilgi varlıklarının korunmasına ilişkin olarak herhangi bir bilgilendirme toplantısına katılmadıklarını belirtmektedirler. Sadece bir katılımcı üniversite tarafından bilgi güvenliği konusunda bilinçlendirme toplantıları düzenlendiğini ancak bunun da düzenli aralıklarla yapılmadığını belirtmiştir. Ortaya çıkan bu tablo ve katılımcıların görüşleri değerlendirildiğinde, üniversitelerde bilgi güvenliğine ilişkin farkındalık eğitimlerine ihtiyaç duyulduğu görülmektedir.

Katılımcılara kişisel verilerin ihlal edilmesi durumunda konuya ilişkin olarak kimlerin ya da hangi birimlerin haberdar edileceği sorulmuş ve elde edilen bulgular Şekil 3 üzerinde gösterilmiştir. Katılımcıların bu soruları yanıtlarken birden fazla seçeneği işaretlemelerine olanak sağlanmıştır.



Şekil 3: Kişisel verilerin ihlal edilmesi durumunda haberdar edilme önceliği

Üniversite kütüphanelerinde henüz veri ihlali nedeniyle yaşanmış bir adli olay ya da soruşturmanın olmadığı tüm katılımcılar tarafından ifade edilmektedir. Bununla beraber, kişisel verilerin ihlal edilmesi halinde katılımcıların %66,7'si, öncelikle bağlı bulunulan idari amirin haberdar edileceğini belirtmektedirler. Katılımcıların verilerin ihlal edilmesi durumunda öncelikle idari amirlere haber verilmesine ilişkin tutumları, bilgi güvenliğinin sağlanmasına yönelik farklı çıkarımlarda bulunulmasına da imkân sağlamaktadır. Buna göre, alınan bilgi güvenliği önlemlerinin ve uygulanan

politikaların idari amirler ve üniversite üst yönetimi tarafından benimsenerek birimlere uygulanmasının, personelin algısı üzerinde daha etkili olacağı ve daha kısa sürede davranışa dönüşeceği değerlendirilmektedir. Katılımcıların %46,7'si, BİDB'nin de durum ve gelişmelerden haberdar edilmesi gerektiğini düşünmektedirler. Kişisel verileri ihlal edilen kişilerin bilgilendirilmesi gerektiğine inanan katılımcıların oranı sadece %20'dir. Katılımcılar kendileri tarafından kaydedilmemiş ve diğer sistemler üzerinden (öğrenci/personel bilgi sistemi vd.) almış oldukları bu bilgilere ilişkin olarak veri sahibine karşı kendilerini sorumlu hissetmemektedirler. Bu açıdan bakıldığında, katılımcıların verilerin saklanmasına ilişkin sorumlulukları hakkındaki düşünceleri ile kişisel verilerin ihlal edilmesi durumunda ilgili birim ya da kişilerin haberdar edilmesi konusundaki düşünceleri arasında doğrusal bir ilişki vardır. Ancak bu anlayışın temelde yanlış olan bazı noktaları bulunmaktadır. Verinin elde edilmesi ile kullanılmasına ilişkin hukuksal sorumluluklar arasında farklılık bulunmaktadır. Her ne kadar veriler diğer birimler tarafından elde edilse de, verilere erişim sağlayan ve kullanan birimlerin de bu verileri koruma yükümlülükleri vardır. Kişisel veri ihlalinin kütüphanenin kullanımına bağlı olarak gerçekleşmiş olması halinde, veri sahibinin bilgilendirilmesi sorumluluğunun kütüphane tarafından yerine getirilmesi gerekmektedir. Araştırma verilerine göre üniversite birimlerinde uygulama standardının oluşabilmesi için, öncelikle verilerin korunmasına yönelik olarak üniversite birimlerinin sorumlulukların belirlenmesi ve kurumsal bilgi güvenliği politikalarında veri sahibinin haklarına ilişkin unsurlara yer verilmesi gerektiği düşünülmektedir. Katılımcıların hiçbirinin "haber verilmeksizin en kısa sürede sistem yeniden aktif hâle getirilir" seçeneğini işaretlememiş olması ise, bu konudaki farkındalığın olumlu göstergelerinden biridir. Yetkisiz erişimler sonrasında meydana gelen zararın boyutunun çoğu zaman ilk aşamada görülemeyeceği ve sistem üzerinde yapılan değişikliklerin, zararın hukuksal girişimlerle telafi edilme olasılığını da ortadan kaldırabileceği değerlendirilmektedir (Henkoğlu, 2011).

Katılımcılara hassas ve kişisel veri kapsamında hangi bilgilerin korunması gerektiğine ilişkin düşünceleri sorulmuş ve elde edilen bulgular Tablo III üzerinde gösterilmiştir.

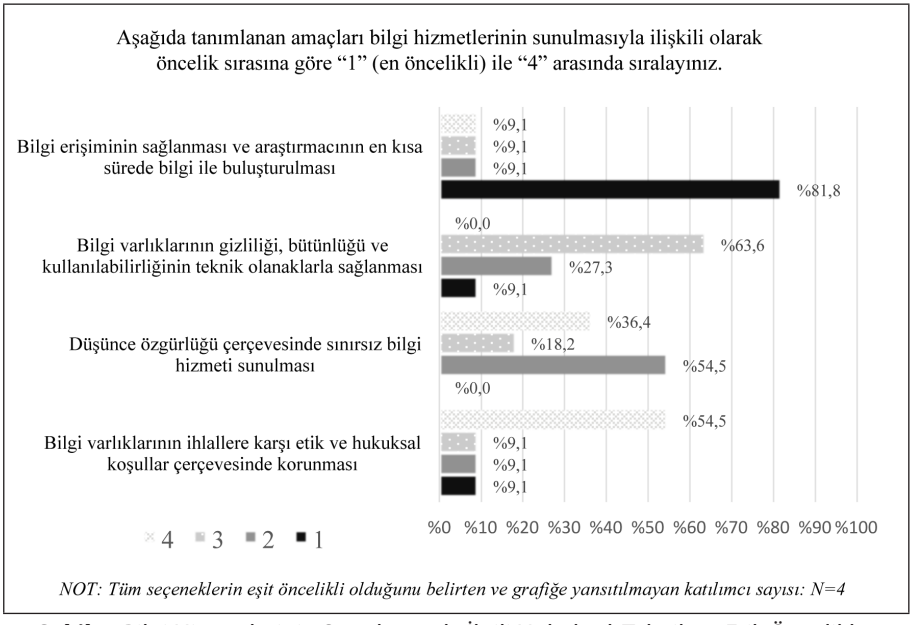
Tablo III: Hassas ya da Kişisel Veri Kapsamında Korunan Bilgiler

Aşağıdaki seçeneklerden hangilerinin kullanıcı ile ilişkilendirilmesi halinde "hassas" ya da "kişisel veri" kapsamında korunması gerektiğini düşünüyorsunuz?		
	N	%
Kullanıcının araştırma konusu	11	73,3
Kullanıcının danışma hizmetleri kapsamında edindiği bilgiler	8	53,3
Ödünç alınan yayınların listesi	5	33,3
Web sayfasına yapılan ziyaretlere ilişkin kayıtlar	9	60
Kütüphane kaynaklarına ve veri tabanlarına bağlandığı IP adresi	8	53,3
Kullanıcının kimlik bilgileri (Ad-Soyad, TC kimlik numarası vd.)	14	93,3
Kullanıcının iletişim bilgileri (adres, telefon, e-posta adresi vd.)	14	93,3
Hiçbiri	-	-

Katılımcıların hassas ve kişisel veri kapsamında korunması gereken bilgilerin neler olabileceğine ilişkin düşüncelerinde farklılıklar bulunmaktadır. Bu nedenle seçeneklerde sunulan tüm bilgilerin kişisel veri olarak korunması gerektiğine yönelik görüş bildiren katılımcı oranı düşük seviyededir (%26,7). Katılımcıların hassas ya da kişisel veri kapsamında korunmasına ilişkin olarak en fazla tereddüt ettikleri bilgiler, ödünç alınan yayınların listesi (%33,3), danışma hizmetleri kapsamında edinilen bilgilerin listesi (%53,3) ve IP adresleridir (%53,3). Ancak "TKD Mesleki Etik İlkeleri" (TKD, 2010), "TKD Düşünce Özgürlüğü Bildirgesi" (TKD, 2008) ve IFLA (International Federation of Library Associations and Institutions) tarafından yayınlanan "İfade Özgürlüğü ve İyi Kütüphaneciliğin İlkeleri"[4] içinde (IFLA, 2014) bu bilgilerin gizliliğinin kişisel veriler ve özel yaşamın gizliliği kapsamında korunacağı açık olarak belirtilmektedir. Ayrıca bazı ülkelerde kullanıcı ilgi alanlarını ve eğilimlerini gösteren kütüphane kayıtlarının incelenmesine ilişkin hukuksal düzenlemelerin yapıldığı ve toplumsal olaylar sonrasında soruşturmaların kütüphane kayıtlarına başvurularak şekillendirildiği görülmektedir (Starr, 2004). Bu konudaki tereddütlerin, bilgi varlıklarının korunması ve hangi verilerin kişisel veri kapsamında değerlendirileceğine ilişkin farkındalık eğitiminin yapılmamasının bir yansıması olduğu düşünülmektedir. Araştırma esnasında katılımcılarla kimlik, kişilik ve kişinin hayat görüşüne ilişkin birçok bilgiye ulaşılmasını sağlayan hassas verilerin önemine ilişkin kısa bilgi alış verişi yapılması sonrasında katılımcıların konuya bakış açısının değişmesi de bu görüşü desteklemektedir. İletişim ve kimlik bilgilerinin korunması gerektiği konusunda ise katılımcıların büyük bölümünün (%93,3) tereddüdü bulunmamaktadır.

4 IFLA Principles of Freedom of Expression and Good Librarianship, 8th: "Library users shall have the right to personal privacy and anonymity. Librarians and other library staff shall not disclose the identity of users or the materials they use to a third party."

Katılımcıların bilgi varlıklarının korunmasına vermiş oldukları önem ve önceliklerinin daha detaylı olarak anlaşılabilmesi amacıyla, bilgi hizmetlerinin sunulmasına yönelik önceliklerini belirtmeleri istenmiştir. Katılımcılara bilgi hizmetlerinin sunulması esnasında göz önünde bulundurulabilecek ve aynı zamanda hukuksal, teknik, etik ve uygulamaya yönelik mesleki prensipleri içeren seçenekler sunularak aralarında bir öncelik sıralaması yapmaları istenmiştir. Ancak dört katılımcı tüm seçeneklerin kendileri için eşit öneme sahip olduğunu vurgulayarak tercihlerini bu doğrultuda yapmıştır. Bu katılımcıların yanıtları Şekil 4 üzerinde yer alan diğer öncelik değerlerini değiştirmemesi için ayrıca gösterilmiştir. Şekil 4 üzerindeki hesaplamalar, öncelik belirten katılımcıların (N=11) vermiş oldukları yanıtlara bağlı olarak yapılmıştır.



Şekil 4: Bilgi Hizmetlerinin Sunulmasıyla İlgili Hukuksal, Teknik ve Etik Öncelikler

Bu soruyu yanıtlarken katılımcılardan bilgi hizmetlerinin sunulması esnasında "ihmal edilebilirliği" göz önünde bulundurmaları istenmiştir. Ancak yanıtların dağılımı içerisinde katılımcıların %81,8'inin "bilgi erişiminin sağlanması ve araştırmacıların en kısa sürede bilgi ile buluşturulmasını" en öncelikli olarak işaretlediği görülürken; %54,5'inin "bilgi varlıklarının etik ve hukuksal koşullar çerçevesinde korunmasına" en düşük önceliği vermeleri dikkat çekicidir. Katılımcılara bu seçeneğe ilişkin olarak "bilgi varlığı" kavramı ile hassas ve kişisel verilerin kast edildiği bilgisi verilmiştir. Bu seçeneği öncelikler arasında son sıraya yerleştiren katılımcıların oranı, "düşünce özgürlüğü çerçevesinde sınırsız bilgi hizmeti sunulması" seçeneğini son sıraya yerleştiren katılımcıların oranından

(%36,4) daha fazladır. Katılımcıların büyük bölümünün (%63,6) üçüncü öncelikli olarak gördükleri seçenek ise "bilgi varlıklarının gizliliği, bütünlüğü ve kullanılabilirliğinin teknik olanaklarla sağlanması" olmuştur. Bununla beraber, sunulan tüm seçeneklerin öncelikli olduğunu belirten dört katılımcının (%26,6) olması önem taşımaktadır. Bu katılımcılar, sunulan seçenekler arasında bir denge bulunduğunu ve birinin tamamen ihmal edilmesi halinde diğerlerinin üzerinde olumsuz etkisi olabileceğini ifade etmektedirler. Şekil 4'ten elde edilen veriler, genel olarak katılımcılar için bilgi hizmetlerinin sunulmasında hukuksal, etik ve teknik önlemlerin alınmasının daha düşük öncelikli olduğunu göstermektedir. Bu soruya verilen yanıtlar ile katılımcıların kişisel veri kapsamında korunması gereken bilgilere ilişkin görüşlerini ortaya koyan soruya vermiş oldukları yanıtlar arasında doğrusal ilişki olduğu görülmektedir. Kişisel verilerin korunmasına yönelik risk algısının düşük olması ve bilgi ihlallerinin yaratacağı sonuçlara ilişkin endişe duyulmamasının bu sonuçta etkili olduğu düşünülmektedir.

Üniversite kütüphanelerinin varlık nedenleri "kullanıcının en kısa sürede bilgi ile buluşturulması" gibi mesleki ilkelerle açıklanmaktadır. Ancak katılımcılar "kullanıcıların bilgi ile *güvenli olarak* buluşturulması" konusunda sorumluluklarının bulunmadığını düşünmektedirler. Bu yaklaşımın temelinde öğretiden kaynaklanan kabullenmenin bulunduğu düşünülmektedir. Öğretideki "düşünce ve erişim özgürlüğüne" vurgu yapılarak açıklanan bilgi hizmetlerinin sunulması ile uygulamadaki bilgi varlıklarının korunması ve sorumlulukların üstlenilmesi dengesinin sağlanmasında eksikliklerin olduğu düşünülmektedir. Üniversite kütüphanelerinde kullanıcı ile bilginin buluşturulması sürecinde güvenlik önlemlerinin farklı bir birim tarafından alınması ya da bu sorumluluğun üstlenilmesinin teknik ve hukuksal açıdan da mümkün olmadığı göz ardı edilmektedir. Bununla birlikte, güvenlik önlemlerinin alınması gerekçe gösterilerek farklı bir birim tarafından yapılacak bu tür müdahalelerin kullanıcı erişim haklarını daha fazla sınırlandıracağı düşünülmektedir.

Katılımcılara ayrıca kişisel verilerin işlendiği bilgisayarlardaki oturum açma politikalarına ilişkin uygulamaları sorulmuştur. Alınan yanıtların biri haricinde tamamı (%93,3), kişisel verilerin işlendiği bilgisayarlarda her personelin kendi kullanıcı hesabı ile oturum açabildiğini ve böylece yapılan işlemlerin hangi personel tarafından gerçekleştirildiği bilgilerine ulaşılabileceğini belirtmişlerdir. Ortak kullanıcı hesabı kullanıldığını ifade eden katılımcı ise, kurulum aşamasında olduklarını ve henüz yeterli sayıda bilgisayarın bulunmadığını belirtmiştir. Yeterli altyapı, yazılım ve bilgisayar desteği sağlanmadan faaliyete geçen üniversite kütüphanelerinde kolaylıkla yetkisiz erişimlerin yapılabileceği ve bu aşamada bilgi güvenliği zafiyetlerinin daha fazla olabileceği söylenebilir.

Katılımcılardan kullanıcılara ait kişisel verilerin korunmasına ilişkin önlemleri öncelik sırasına göre sıralamaları istenmiş ve elde edilen bulgular Tablo IV üzerinde gösterilmiştir. Bu sıralama ile katılımcıların kişisel verilerin korunmasına yönelik hangi önlemlerin (hukuksal, teknik, idari ve etik) öncelikle alınmasına ihtiyaç duyduklarının

belirlenmesi hedeflenmiştir. Dört katılımcı (%26,6) tüm seçeneklerin ya da içlerinden bazılarının kendileri için eşit öneme sahip olduğunu vurgulayarak tercihlerini bu doğrultuda yapmışlardır. Bu katılımcıların yanıtları Tablo IV üzerinde yer alan öncelik değerlerini değiştirmemesi için hesaplamalarda değerlendirme dışı bırakılmıştır.

Tablo IV: Kullanıcılara ait kişisel verilerin korunmasına ilişkin öncelikler

Kullanıcılara ait kişisel verilerin korunmasına ilişkin önlemleri öncelik sırasına göre "1" (en öncelikli) ile "4" arasında sıralayınız.								
	1		2		3		4	
	N	%	N	%	N	%	N	%
Hukuksal düzenlemeler kapsamında korunmalıdır	8	72,7	1	9,1	1	9,1	1	9,1
Teknik önlemler alınmalıdır	1	9,1	3	27,3	5	45,5	2	18,2
İdari önlemler alınmalıdır	1	9,1	2	18,2	5	45,5	3	27,3
Etik ilkeler çerçevesinde korunmalıdır	1	9,1	5	45,5	-	-	5	45,5
Değerlendirme Dışı	4	-	4	-	4	-	4	-

Katılımcıların %72,7'si kişisel verilerin korunmasına ilişkin olarak alınması gereken önlemlerin hukuksal düzenlemeler kapsamında olması gerektiğine inanmaktadırlar. Seçenekler arasında katılımcıların ikinci öncelikli olarak alınması gereken önlemler konusunda "etik değerler" üzerinde yoğunlaştıkları (%45,5) görülmektedir. Bu sonuç, katılımcıların görüşme esnasında vurgulamış olduğu "hukuksal düzenlemelerin yetersizliği nedeniyle bilgi güvenliği önlemleri etik kurallar çerçevesinde alınıyor" ifadesiyle de örtüşmektedir. Bu bulgulara göre, uygulanabilir nitelikte hukuksal düzenlemelerin yapılması halinde, bu düzenlemelerin kısa sürede üniversite kütüphanelerinde benimsenerek uygulamaya dönüşmesinin sağlanabileceği söylenebilir. Görüşme esnasında elde edilen verilere göre de, uygulamada katılımcılar etik ilkeleri daha fazla dikkate almakta ve bu kapsamda sorumluluklarının bulunduğunu düşünmektedirler. Kişisel verilerin korunmasına ilişkin teknik önlemlerin alınmasının üçüncü öncelikte olması ise dikkat çekicidir. Oysa yapılan farklı araştırma sonuçlarında da görüldüğü gibi (Wolf, Haworth ve Pietron, 2011); şifre değişimi vd. güvenlik önlemlerin alınması konusunda mümkün olduğu ölçüde teknik önlemlerin alınması, zorlayıcı olması yönüyle alınan önlemleri daha etkili hale getirebilmektedir. Kişisel verilerin korunması konusunda sorumluluğunun bulunmadığını düşünen katılımcı bulunmamaktadır. Araştırmadan elde edilen bulgular üniversite kütüphanelerinde hukuksal ve idari önlemlerin alınmasına ne kadar değer verildiğinin görülmesi açısından önemli olduğu gibi; teknik önlemler ve etik değerlerle bu konudaki eksikliklerin giderilebileceğine ilişkin farkındalığı ortaya çıkarması açısından da önem taşımaktadır.

Katılımcıların bilgi hizmetlerinin sunulması esnasındaki öncelikleri ile kişisel verilerin korunmasına yönelik önlemlerin alınmasındaki öncelikleri arasındaki farklılık dikkat çekmektedir. Bu fark katılımcılardaki iki soruya yönelik algı farkının ötesinde, bilgi hizmetlerinin sunulması esnasındaki risklere yönelik algılarından kaynaklanmaktadır. Katılımcılar bilgi hizmetleri kapsamında edinilen bilgilere ilişkin kayıtların hassas ya da kişisel veri olarak korunması gerektiğini düşünmemektedirler. Bilgi hizmetlerinin sunulması esnasındaki risk algısının düşük olması, hukuksal düzenlemelere yönelik önceliği azaltırken; kişisel verilerin korunmasına ilişkin önlem alınması söz konusu olduğunda, katılımcılar öncelikle hukuksal düzenlemeler kapsamında önlem alınmasını öngörmektedirler.

Katılımcıların Kişisel Verilerin Korunmasına İlişkin İlâve Görüş ve Önerileri

Uygulanan anket sonunda katılımcıların konuya ilişkin görüşlerini ifade edebilmeleri için oluşturulan kısımda belirtmiş oldukları ilâve görüş ve önerilerden elde edilen bulgular ve katılımcıların açık uçlu sorulara yönelik değerlendirmelerinde öne çıkan hususlara Tablo V üzerinde yer verilmiştir. Katılımcılar tarafından belirtilen ilâve görüşler ve bu görüşleri sunan katılımcının çözüm önerileri, üzerinde herhangi bir değişiklik ya da ilâve yapılmaksızın Tablo V üzerinde gösterilmiştir.

Tablo V: Kütüphanelerde bilgi güvenliğinin sağlanmasına ilişkin ilâve görüş ve öneriler

Görüş	Çözüm Önerisi
Yazılı kaynakların olmaması, özellikle yeni kurulan üniversiteler için kişisel verilerin korunması sürecini daha uzun ve zorlu hale getirmektedir.	Türkiye'de kişisel verilerin korunmasına yönelik tüm kurum ve kuruluşları kapsayan bir çerçeve düzenlemeye ihtiyaç vardır. Kurum ve kuruluşlar bu çerçeve düzenlemeye dayanarak kendi özel koşullarını içeren kurumsal düzenleme ve politikalarını oluşturmalıdırlar.
Kişisel verilerin korunmasına ilişkin hukuksal dayanakların oluşturulması için birçok farklı hukuksal düzenlemeden faydalanılmaktadır. Hangi hukuksal düzenleme içinde ne tür sorumlulukların bulunduğu hakkında bilgi sahibi olunmadığı gibi, hukuk mevzuatı içerisinden bu sorumlulukların üniversite birimleri tarafından belirlenmesi de çok zor ve uzun bir süreç içinde yapılacak çalışmaları gerektirmektedir.	Hukuksal sorumlulukların da yer aldığı bu tür çalışmalara ağırlık verilmesi üniversiteler için önemli bir kazanım olacaktır.
Hukuksal düzenlemelerin ihtiyacı karşılamaması nedeniyle eğitim ve farkındalık konusu son yıllarda daha önemli hale gelmiştir.	Kişisel verileri işleyen personele yönelik farkındalık eğitimlerine daha fazla önem verilmelidir.
Yasal sorumlulukların belirlenmesi ve uyum sağlanması konusunda sorunlar yaşanmaktadır.	Özellikle yeni kurulan üniversitelerde yasal sorumluluklara daha hızlı ve kolay uyum sağlanabilmesi için bu sorumlulukların belirlenmesi ve yalın bir dille kontrol listesi haline getirilmesine ihtiyaç duyulmaktadır.

Yönetim konumunda olan kişilerin daha duyarlı ve bilinçli olmaları gerekmektedir.	Çalışanların özenle seçilmesi, üst düzey yönetici konumunda olan kişilerin mesleki eğitim ve etik ilkeler konusunda bilgi birikimi olması, orta düzey yönetici konumunda olan kişilerin denetim ve gözetimleri sürekli olarak yapması ve "insanın ve kişisel verilerin öncelikli olduğu" bilincinin oluşması önem taşımaktadır.
Üniversite birimlerinin elde ettiği verilerin kullanımına ilişkin şartların belirlenmesi gerekir.	Öğrencilerin kayıt aşamasında oluşturulan "özlük bilgi formu" kapsamında, kişisel verilerin ailesi ya da diğer üçüncü kişilerle paylaşılmasına ilişkin olarak yazılı onay alınmalı ve üniversite birimleri bu şartlara uymalıdır.
Dağınık ve geçici düzen içerisinde verilen hizmetin kalitesi düştüğü gibi, risk yönetiminin yapılması da zorlaşmaktadır.	Yeni kurulan üniversitelerde öncelikle altyapı planlaması yapılmalıdır.
Kişisel verilerin işlendiği üniversite birimlerinde elektronik ortamlarda yer alan bilgilerin saklanması ve imha edilmesine ilişkin olarak yeterli düzeyde bilgi sahibi olunmadığı için farkındalık da oluşmamaktadır. Elektronik ortamlardaki bilgilerin korunmasına ilişkin standartlar belirlenmemiştir. Kişisel verileri işleyen personel sadece mesleki eğitim kapsamında edindiği etik ilkeleri ve personel katılış bilgilendirmelerini dikkate almaktadır.	Kişisel verileri işleyen personele farkındalık eğitimleri düzenlenmeli ve belirli aralıklarla tekrar edilmelidir. Üniversitelerde verilerin işlenmesi, saklanması ve imha edilmesine ilişkin süreçler belirlenmelidir.
Üniversitelerde sabit disklerin kalıcı olarak silinmesi ve imhasına yönelik olarak hangi standartların kullanılacağına ilişkin politikalar bulunmamaktadır.	Bu konuda üniversite BİDB ile koordinasyon sağlanmalı ve sorumluluklar belirlenmelidir.

Sonuç ve Öneriler

Kişisel verilerin korunmasına yönelik problemin özünde, bu bilgilerin bilgi teknolojileri sayesinde kontrolsüz ve hızlı bir şekilde çoğaltılabilmesi, depolama maliyetlerinin düşük olması nedeniyle gereğinden fazla bilginin kayıt altına alınması, kısa sürede uzak mesafelere transfer edilebilmesi, tehditlere karşı korunamayan bilgilerin kısa süre içinde sınırsız sayıda kişinin erişimine açık hale gelmesi ve bu sürecin kontrol dışına çıktığı andan itibaren geri dönüşü olmayan sonuçlar doğurabilmesi bulunmaktadır. Araştırma verilerinden elde edilen sonuçlar, üniversite kütüphanelerinde bu risk ve problemlerin oluşmaması için gerekli hukuksal temel ilkelerin ve etik değerlerin uygulamaya dönüştürülmesi konusunda yeterince çaba gösterilmediğini ortaya koymaktadır.

Üniveriste kütüphanelerinin Anayasa, TCK ve 5651 Sayılı Kanun vd. hukuksal düzenlemeler kapsamında sorumlulukları bulunmaktadır. Ancak mevcut hukuksal düzenlemeler hassas ve kişisel verilerin üniversite kütüphanelerinde hassasiyet

gösterilerek işlenmesi ve özel hayatın gizliliğinin korunması konusunda yetersiz kalmaktadır. Ayrıca hukuksal düzenlemelerin "önleyici" nitelikte olmadığı da görülmektedir. Türkiye'de henüz veri koruma kanununun olmaması, Türk Hukuk Mevzuatındaki diğer birçok düzenlemelerin içinde yer alan ilgili kısımların dikkate alınmasını gerektirmektedir. Bu işlemin zorluğu ve çoğu zaman ihmal edilmesi nedeniyle, hukuksal anlamda daha fazla ihlal gerçekleşmekte ve hukuksal düzenlemeleri dikkate alan bilgi güvenliği politikalarının geliştirilmesinde eksiklikler bulunmaktadır. Uzun bir süreç içerisinde yapılabilecek bu tür çalışmaların bulunmaması nedeniyle, üniversite kütüphanelerinde kişisel verilerin korunmasına ilişkin olarak hangi hukuksal düzenleme kapsamında ne tür sorumluluklarının olduğu yeterince açık değildir. Bununla birlikte, araştırma sonucunda elde edilen bulgulara göre bu tür çalışmaların üniversite kütüphaneleri tarafından yürütülebilmesinin, özellikle sınırlı personel gücü ile faaliyetleri takip eden vakıf üniversitelerinin %80'inde mümkün olamayacağı değerlendirilmektedir.

Üniversite kütüphaneleri, kişisel verilerin ağ üzerinden iletimi, yetkisiz erişim, değiştirme ve kazara ya da yasa dışı yöntemlerle yapılacak tahribe karşı gerekli teknik ve kurumsal önlemleri almalıdırlar. Bunun yanı sıra, üniversite kütüphanelerinde kişisel verilere erişim hakkı bulunan işleyici ve işleyici yetkisi altındaki kişiler, kendileri için tanımlanan görev ve yetki kapsamında verileri işlemelidirler. Bu konuda 95/46/EC sayılı direktifin 16. ve 17. Maddeleri, 108 Sayılı Sözleşmenin 7. Maddesi ve KVKKT'nin 11. Maddesi dikkate alınarak üniversite kütüphanelerinde kişisel verilerin korunması, sorumlulukların belirlenmesi ve gerekli teknik önlemlerin alınması büyük önem taşımaktadır. Ayrıca uluslararası anlaşmaların kişisel verilerin korunmasına ilişkin maddeleri de göz ardı edilmemelidir.

Üniversite kütüphanelerinde kişisel verilerin işlenmesine ilişkin belirsizliklerin bulunduğu, risk yönetimi yapılmadığı, diğer üniversite birimleriyle sorumlulukların paylaşılmadığı, personele veri korumaya ilişkin bilinçlendirme eğitimi verilmediği ve bu konuda bir denetim mekanizmasının olmadığı görülmektedir. Üniversite kütüphanelerinde hangi verilerin kişisel veri olduğu konusunda dahi tereddütler bulunmaktadır. Bu çalışma kapsamında elde edilen verilere dayanarak, üniversite birimlerinde yapılacak denetim ve kontrollerde, diğer devlet kurum ve kuruluşlarında yapılan denetimlerde elde edilen olumsuz sonuçlarla (DDK, 2013) karşılaşma olasılığının bulunduğu söylenebilir. Üniversite kütüphanelerinde hukuksal düzenlemelerde yer alan yükümlülüklerin yerine getirilmesi ve sorunların önüne geçilebilmesinin en etkin yolu, bilginin durumuna bağlı olarak diğer üniversite birimleriyle birlikte risk yönetimi yapılması ve hukuksal düzenlemeler çerçevesinde kişisel verileri işleyen personelin farkındalığının arttırılmasıdır.

Üniversite kütüphanelerinde kişisel verilerin yeterli düzeyde korunabilmesi için, verilerin elde edilmesi aşamasından itibaren AB veri koruma direktif ve düzenlemelerini dikkate alan üniversitelerde (Stuttgart University, 2013) olduğu gibi hassasiyet

gösterilmesi önem taşımaktadır. Bunun için öncelikle yazılı bilgi güvenliği politikalarının belirlenmesi ve bu kapsamda veri sahibine karşı kişisel verilerin korunacağına ilişkin yazılı taahhütte bulunulmasının zorunlu hale getirilmesi gerekmektedir. Bu tür uygulamaların, gereğinden fazla bilgi elde edilmemesi konusunda da etkili olacağı değerlendirilmektedir. Bilgi sistemleri üzerinde artan veri miktarı, bireylere yönelen tehditler karşısında tüm bilgilerin kriptolanması gibi teknik yöntemlerin uygulanmasını da zorlaştırmaktadır. Bu nedenle mevcut bilgilerin sınıflandırılması, kişisel verilerin korunmasına yönelik olarak alınacak önlemlerin etkinliğini arttırmaktadır. Ayrıca bu verilerin işlenmesi, saklanması, korunması ve imha işlemlerinin kimlerin sorumluluk alanına girdiğinin belirlenmesi ve güvenlik ihlâllerine karşı hazırlıklı olunması gerekmektedir. Böylece bilginin yanlış kullanımından, yönetiminden ya da ihmallerden kaynaklanan kayıplara karşı uygun güvenlik önlemlerinin alınması sağlanabilecektir.

Araştırmada elde edilen bulgular çerçevesinde, üniversite kütüphanelerinde kişisel verilerin ve kişisel hakların korunmasına ilişkin olarak dikkate alınması gereken diğer öneriler şunlardır;

- ◊ Veri sahibinin kişisel hak ve özgürlüğünü koruyacak önlemler, hukuksal düzenlemeler ve üniversite bilgi güvenliği politikası kapsamında alınmalıdır. Veri sahibine verinin kaynağını bilme ve hukuka aykırı işlemlere karşı kanun yollarına başvurma hakkı sağlanmalıdır.
- ◊ Üniversite kütüphaneleri tarafından elde edilen kişisel veriler hukuka uygun olarak ve meşru amaçlar için elde edilmelidir. Gereğinden fazla kişisel veri toplanmamalıdır. Elde edilen veriler için veri sahibinin rızası bulunmalıdır. Bu veriler doğru ve güncel olmalı, amacına uygun olarak kullanılmalı ve veri sahibi tarafından erişilebilir olmalıdır. Ayrıca kullanım süresi sonunda imha edilmesi sağlanmalıdır.
- ◊ Üniversite kütüphanelerinde depolanan kişisel veriler için gerekli fiziksel, doküman ve personel güvenliği sağlanmalıdır. Bu veriler, kanun gereği bir hakkın tespiti, korunması, suçun önlenmesi ya da soruşturulması dışında (kamu kurum ve kuruluşları da dahil olmak üzere) paylaşılmamalıdır.
- ◊ Erişim yetkilendirmeleri önceden belirlenmiş politikalar kapsamında yapılmalı ve bunun dışında internet altyapısı üzerinden kişisel veri transferi yapılmamalıdır.
- ◊ Kişisel verilerin korunması amacıyla bilgi güvenliği politikaları oluşturulurken; kişisel verilerin korunmasına ilişkin Türk Hukuk Mevzuatının yanı sıra, uluslararası standartlar, denetleme raporları ve evrensel ilkeler gibi farklı kaynaklardan yararlanılmalıdır.
- ◊ Kişisel verilerin işlendiği sistemlerin tasarımı esnasında ve verilerin işlenmesi sırasında teknik ve kurumsal önlemler alınırken, korunacak verilerin yapısı, risk durumu ve maliyetler de dikkate alınmalıdır.
- ◊ Üniversite kütüphanelerinde merkezi veri tabanlarına aktarılmayan bilgilerin bulunduğu bilişim sistemlerinin zincirin zayıf halkası olabileceği değerlendirilerek, alınan önlemler içerisinde bu sistemler de göz önünde bulundurulmalıdır.

- ◊ Üniversite kütüphanelerinde kişisel verilerin işlendiği bilgi sistemlerinin tüm güvenlik, saklama, yedekleme ve imha işlemleri BİDB ile koordineli olarak belirlenen standartlar çerçevesinde yürütülmelidir.
- ◊ Üzerinde kişisel veri bulunan bilgisayarların denetimlerinin yapılması ve kullanıcılarda farkındalığın arttırılması için, birim içinde bilgi işlem sorumlusu görevlendirilmelidir.
- ◊ Mesleki etik kuralları ile birlikte yabancı hukuk mevzuatları ve etik kuralları da dikkate alınmalı ve konuya ilişkin güncellemeler mesleki iletişim kanalları üzerinden duyurularak bütün kütüphanelerde hayata geçirilmesine katkı sağlanmalıdır.
- ◊ Bilgi yöneticilerinin konuyla ilgili bilgi, beceri ve farkındalıklarının artırılması amacıyla müfredat programlarında konuyla ilgili derslere yer verilmeli ve uygulamacılara hizmet içi eğitim sağlanmalıdır.

Kaynakça

Aksoy, H. C. (2008). The right to personality and its different manifesttations as the core of personal data. *Ankara Law Review, 5*(2), 235-249.

Anayasa Mahkemesi. (2011). Türkiye İstatistik Kurumu Başkanlığının ilgili Bölge Müdürlükleri tarafından verilen idari para cezalarına karşı yapılan itirazlar. 5 Aralık 2013 tarihinde http://www.hukukturk.com/fractal/hukukTurk/pages/find_n.jsp?pLayerOk=1&pObjectId=509&pViewId=486&pMainCategoryId=Anayasa&pEsasNo1=2010&pEsasNo2=12&pMercilId=4091&i1.x=10&i1.y=7 adresinden erişildi.

Avrupa Komisyonu. (2012a). MEMO/12/41. 19 Aralık 2013 tarihinde http://europa.eu/rapid/press-release_MEMO-12-41_en.pdf adresinden erişildi.

Avrupa Komisyonu. (2012b). Türkiye 2012 yılı ilerleme raporu. 19 Kasım 2013 tarihinde http://www.ab.gov.tr/files/2012_ilerleme_raporu_tr.pdf adresinden erişildi.

Avrupa Konseyi. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 21 Ocak 2015 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF adresinden erişildi.

Avrupa Konseyi. (2012). Proposal for a Regulation of theEuropean Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 22 Ocak 2015 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF adresinden erişildi.

Charette, R. (2012a). This week in cybercrime: Data breaches at Yahoo, Formspring and Nvidia. 24 Ocak 2014 tarihinde http://spectrum.ieee.org/riskfactor/telecom/security/this-week-in-cybercrime-data-breaches-at-yahoo-formspring-and-nividia adresinden erişildi.

Charette, R. (2012b). Zappos.com customer database breached, info on more than 24 million customers potentially accessed. 24 Ocak 2014 tarihinde http://spectrum.ieee.org/riskfactor/telecom/security/zapposcom-customer-database-breached-info-on-more-than-24-million-customers-potentially-accessed adresinden erişildi.

Chirillo, J. ve Danielyan, E. (2005). *Sun Certified Security Administrator for Solaris 9 & 10 Study Guide*. California: McGraw-Hill.

DDK. (2013). *Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları*. Ankara: Cumhurbaşkanlığı Devlet Denetleme Kurulu.

Fischer-Hübner, S. (2001). *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms*. Berlin: Springer.

Henkoğlu, T. (2011). *Adli bilişim: Dijital delillerin elde edilmesi ve analizi*. İstanbul: Pusula Yayıncılık.

Henkoğlu, T. ve Yılmaz, B. (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları. *Türk Kütüphaneciliği, 27*(3), 451-471.

IFLA. (2014). *Principles of freedom of expression and good librarianship*. 29 Aralık 2014 tarihinde http://www.ifla.org/faife/mission adresinden erişildi.

Kaptan, S. (1995). *Bilimsel araştırma ve istatistik teknikleri* (10 ed.). Ankara: Rehber Yayınevi.

Karasar, N. (2012). *Bilimsel araştırma yöntemi* (23 ed.). Ankara: Nobel Yayıncılık.

King, N. ve Raja, V. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Elsevier Computer Law & Security Review*, 308-319.

Küzeci, E. (2010). *Kişisel verilerin korunması*. Ankara: Turhan Kitabevi.

Miller, A. R. (1971). *Assault on Privacy: Computers, Data Banks and Dossiers*. Ohio: The University of Michigan Press.

OECD. (2013). Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. 21 Ocak 2015 tarihinde http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf adresinden erişildi.

Preisig, A. V., Rösch, H. ve Stückelberger, C. (2014). *Ethical dilemmas in the information society: Codes of ethics for librarians and archivists*.

Starr, J. (2004). Libraries and national security: An historical review. *First Monday, 9*(12).

Stone, E. F., Gueutal, H. G., Gardner, D. G. ve McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology, 68*(3), 459-468.

Stuttgart University. (2013). Change of user data. 2 Şubat 2014 tarihinde http://www.ub.uni-stuttgart.de/downloads/formulare/benutzerstatus/aenderungsmeldung.en.pdf adresinden erişildi.

T.C. Anayasası. (1982). Türkiye Cumhuriyeti Anayasası. 28 Ekim 2013 tarihinde http://www.tbmm.gov.tr/anayasa/anayasa_2011.pdf adresinden erişildi.

T.C. Başbakanlık. (1988). *Devlet Arşiv Hizmetleri Hakkında Yönetmelik*. 13 Nisan 2014 tarihinde http://www.devletarsivleri.gov.tr/icerik/309/yonetmelik/ adresinden erişildi.

T.C. Başbakanlık. (2014). Kişisel Verilerin Korunması Kanun Tasarısı ve Gerekçesi. 22 Ocak 2015 tarihinde http://web.tbmm.gov.tr/gelenkagitlar/metinler/362939.pdf adresinden erişildi.

TKD. (2008). Düşünce Özgürlüğü Bildirgesi. 29 Aralık 2014 tarihinde http://www.kutuphaneci.org.tr/sites/default/files/tkd_dusunce_ozgurlugu_bildirgesi.pdf adresinden erişildi.

TKD. (2010). *Mesleki etik ilkeleri*. 3 Ekim 2014 tarihinde http://www.kutuphaneci.org.tr/meslekietik-ilkeleri adresinden erişildi.

Whitman, M. E. ve Mattord, H. J. (2011). *Principles of information security*. Boston: Course Technology.

Wildermann, P. (2014). *Şeffaf okur kâbusu – Kütüphanelerde veri koruma*. 22 Ocak 2015 tarihinde http://www.goethe.de/ins/tr/tr/lp/kul/mag/bib/12623526.html adresinden erişildi.

Winter, K. A. (1997). Privacy and the rights and responsibilities of librarians. 09 Ocak 2014 tarihinde http://www.cstone.net/~kwinter/articles/ksr4_winter.pdf adresinden erişildi.

Wolf, M., Haworth, D. ve Pietron, L. (2011). Measuring an information security awareness program. *Review of Business Information Systems, 15*(3), 9-21.