Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Bilgi ve Belge Yönetimi Anabilim Dalı

ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLERİN KORUNMASI: ANKARA'DAKİ ÜNİVERSİTE KÜTÜPHANELERİNİN DEĞERLENDİRİLMESİ

Dilan Şerife ŞİŞKİN

Yüksek Lisans Tezi

Ankara, 2020

ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLERİN KORUNMASI: ANKARA'DAKİ ÜNİVERSİTE KÜTÜPHANELERİNİN DEĞERLENDİRİLMESİ

Dilan Şerife ŞİŞKİN

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü
Bilgi ve Belge Yönetimi Anabilim Dalı

Yüksek Lisans Tezi

Ankara, 2020

KABUL VE ONAY

Dilan Şerife Şişkin tarafından hazırlanan "Üniversite Kütüphanelerinde Bilgi Güvenliği ve Kişisel Verilerin Korunması: Ankara'daki Üniversite Kütüphanelerinin Değerlendirilmesi" başlıklı bu çalışma, 07.02.2020 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından yüksek lisans tezi olarak kabul edilmiştir.

Prof. Dr. Özgür Külcü (Başkan)

Dr. Öğr. Üyesi Türkay Henkoğlu (Üye)

Dr. Öğr. Üyesi Tolga Çakmak (Danışman)

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Prof. Dr. Musa Yaşar Sağlam

Enstitü Müdürü

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinleri yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan ***"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"*** kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H.Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- Enstitü / Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir. [1]
- Enstitü / Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren ..... ay ertelenmiştir. [2]
- Tezimle ilgili gizlilik kararı verilmiştir. [3]

07/02/2020

Dilan Şerife ŞİŞKİN

[1] *"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"*

(1) *Madde 6. 1. Lisansüstü tezle ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu** iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.*

(2) *Madde 6. 2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulunun** gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.*

(3) *Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, **tezin yapıldığı kurum** tarafından verilir *. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, **ilgili kurum ve kuruluşun önerisi** ile **enstitü** veya **fakültenin** uygun görüşü üzerine **üniversite yönetim kurulu** tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.*
Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

** Tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu tarafından karar verilir.***

ETİK BEYAN

Bu çalışmadaki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi, görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, yararlandığım kaynaklara bilimsel normlara uygun olarak atıfta bulunduğumu, tezimin kaynak gösterilen durumlar dışında özgün olduğunu, **Dr. Öğr. Üyesi Tolga ÇAKMAK** danışmanlığında tarafımdan üretildiğini ve Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesine göre yazıldığını beyan ederim.

07/02/2020

Dilan Şerife ŞİŞKİN

TEŞEKKÜR

Keyifli ve uzun bir yol olduğunu düşündüğüm bilim ve ilim sahibi olma sürecinde her zaman yanımda olan, bana yol gösteren, sabrı, hoşgörüsü, ilgisi, anlayışı ve tez araştırmama sağladığı destek ve katkılarından dolayı sayın hocam, danışmanım, Dr. Öğr. Üyesi Tolga Çakmak'a minnettarım.

Yüksek lisans tez öneri sürecimde fikirleriyle ve görüşleriyle tez konumu şekillendiren bölüm hocalarıma çok teşekkür ederim. Aynı zamanda, tez savunma sınavımda düzeltmeleri ve geri bildirimleriyle tezime ışık tutan ve tezimi geliştirmeme destek olan Sayın Prof. Dr. Özgür Külcü ve Sayın Dr. Öğr. Üyesi Türkay Henkoğlu hocalarıma ne kadar teşekkür etsem azdır.

Araştırmanın uygulanabilmesi için hazırlanan ön testlerde ve veri toplama aşamasında, birebir tanışma fırsatı yakaladığım, bana arkadaşça davranan meslektaşlarıma, Ankara'daki üniversite kütüphaneleri yöneticilerine ve kütüphanecilerine tüm destek ve yardımları için şükranlarımı sunarım.

Bu araştırmada yazıya dökülen satırların ve paragrafların iki yıllık bir birikime dayandığını söylemek benim için oldukça zor. Her birini örnek aldığım, her birinden farklı farklı bilgiler ve fikirler edindiğim ve bu aşamada da bana destek olan tüm hocalarıma çok teşekkür ederim.

Bu süreçte, beni yalnız bırakmayan ve hayata karşı farklı yönlerden bakmamı sağlayan tüm arkadaşlarıma teşekkür ederim. Yüksek lisans tezinin bana kattığı güzel insanlardan birisi olan Abdurrahman Kuşçu'ya maddi ve manevi desteklerinden dolayı teşekkür ederim.

Hayat yolumu çizmemde her zaman benim yanımda duran, sahip olduğum kültürü, bilgiyi ve deneyimi bana kazandıran, her zaman beni destekleyen ve bana gösterdikleri sevgi ve saygıdan dolayı anneme ve babama çok teşekkür ederim. Bu yolda da beni yalnız bırakmayan İrem'e, Yasin'e ve Yusuf'a teşekkür ederim.

Bana ilham veren değerli hocam
Esin Sultan OĞUZ'a…

ÖZET

ŞİŞKİN, Dilan Şerife. *Üniversite Kütüphanelerinde Bilgi Güvenliği ve Kişisel Verilerin Korunması: Ankara'daki Üniversite Kütüphanelerinin Değerlendirilmesi*, Yüksek Lisans Tezi, Ankara, 2020.

Sanayi devrimi olarak adlandırdığımız endüstri 4.0'la şekillenen, gelişen ve değişen dünyamızda, verinin, bilginin, belgenin, insanın, mekânın korunmasını ve güvenilirliğini sağlamak oldukça önem arz etmektedir. Bu canlı ve cansız varlıkların her türlü tehdit, tehlike, hasar ve saldırılara karşı korunması bilgi güvenliğinin sağlanması ve oluşturulmasıyla mümkün olabilmektedir. Bununla birlikte, bilgi güvenliğinin temelinde insan olgusunun yer alması, insana dayalı olarak ortaya çıkan bilgi güvenliği sorunlarıyla birlikte insana yönelik kişisel verilerin korunması konusunun da ciddiyetini katlanarak arttırmıştır.

Bu çalışmada Ankara'daki üniversite kütüphanelerinin bilgi güvenliği uygulamalarına ve kişisel verilerin korunmasına ilişkin mevcut durumlarını tespit etmek amaçlanmıştır. Bu kapsamda, Ankara'da bulunan üniversite kütüphaneleri yöneticilerinin ve kütüphanecilerinin bilgi güvenliği ve kişisel verilerin yönetimi konusunda bilgi ve farkındalıkları görüşme ve anket tekniğiyle incelenmiştir. Bununla birlikte, Ankara'daki üniversite kütüphanelerinde bilgi güvenliği uygulamalarına yönelik (bina, koleksiyon, personel, vb.) gerçekleştirilen düzenlemeler araştırma çerçevesinde değerlendirilmeye çalışılmıştır.

Araştırmanın sonucunda; Ankara'da yer alan üniversite kütüphanelerinde kişisel verilerin elde edilmesi, toplanması, kaldırılması, saklanması olmak üzere kişisel verilerin yönetimine yönelik düzenleme ve politikaların eksik olduğu, kişisel verilerin yönetiminden sorumlu bir personelin bulunmadığı, kullanıcılardan kişisel verilerin işlenmesine yönelik onay alınmadığı ve aydınlatma metinlerinin içeriğinde kişisel verilerin saklanması, silinmesi ve aktarılmasına yönelik bilgilere yer verilmediği, kütüphane yöneticilerinde ve kütüphanecilerinde kişisel verilerin yönetimi ve korunmasına yönelik yaklaşım ve farkındalık eksikliği tespit edilmiştir. Ayrıca, araştırma bulgularında üniversite kütüphanelerinde bina, koleksiyon, yazılım ve donanım olmak üzere bilgi güvenliği uygulamalarına yönelik yetersizlikler olduğu belirlenmiştir. Bu

bağlamda “Üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin yönetimine dönük karar verme ve uygulama düzeyindeki eksiklikler (politika, konuyla ilgili bilinç ve farkındalık, risk değerlendirmesi gibi konularda) bulunmaktadır.” şeklinde olan hipotezimiz doğrulanmıştır. Son olarak araştırmada, üniversite kütüphanelerinin bilgi güvenliği ve kişisel verilerin korunmasını içeren yapılandırılmış bir politika oluşturmaları ve konuya yönelik bilinç ve farkındalık çalışmalarının yapılmasıyla ilgili önerilere yer verilmiştir.

Anahtar sözcükler

Bilgi güvenliği, kişisel veri, kişisel verilerin korunması, kişisel verilerin yönetimi, üniversite kütüphaneleri

ABSTRACT

ŞİŞKİN, Dilan Şerife. *Information Security and Protection of Personal Data in University Libraries: Evaluation of University Libraries in Ankara*, Master's Thesis, Ankara, 2020.

In our world which has been shaped, developed and changed by Industry 4.0, it is quite important to ensure the protection and reliability of data, information, document, human and place. Protecting all living and non-living beings against all kinds of threats, dangers, damages or attacks and ensuring information security make it possible to reach this aim. Nevertheless, the fact that human phenomenon underlies the information security has incrementally increased the significance of data protection issue along with the information security problems arise from human factor.

The aim of this study is determining the current situations related with personal data protection and information security implementations of university libraries in Ankara. Within this scope, the executives' and librarians' knowledges and awareness on the information security and personal data management issue in universities' libraries in Ankara are examined with interview and survey technique. In addition to this, regulations oriented at the information security implementations (building, collection, personnel, etc.) at the universities' libraries were taken to evaluation in the scope of the research.

Results of the research have determined that regulations and policies on the personal data management which consists of obtaining, gathering, disposing and retaining the personal data were inadequate; there were no personnel in charge to manage the personal data, no permission for processing the personal data received from users, no information on the retention, disposal and transmission of the personal data were included in the content of clarification texts, and no sufficient level of approach and awareness on the management and protection of personal data observed among the libraries' executives and librarians. Moreover, it has been specified in the research findings that there were some inadequacies with information security implementations in terms of building, collection, software and hardware in universities' libraries. In this context, our hypothesis which follows as that "There are inadequacies (in issues such as policy, consciousness and awareness on the topic, risk assessment) with the enacting and implementing level regarding the

information security and personal data management in universities' libraries," has been confirmed. Lastly, suggestions were made in the research, in order for the universities' libraries to develop a structured policy which includes information security and the personal data protection, and make studies of consciousness and awareness regarding the issue.

Key Words

Information security, personal data, protection of personal data, management of personal data, university libraries

İÇİNDEKİLER

KISALTMALAR DİZİNİ

ACRL	Association of College & Research Libraries
ALA	American Library Association
APA	Amerikan Psychological Association
BİDB	Bilgi İşlem Daire Başkanlığı
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BSI IT	Bundesamt für Sicherheit in der Informations technikz
CCTV	Close Circuit TeleVision
CIA	Confidentiality, Integrity, Availability
COBIT	Control Objectives for Information and Related Technology
DPA	Data Protection Act
FFIEC	Federal Financial Institutions Examination Council's
FERPA	Family Educational Rights and Privacy Act
FTC	Federal Trade Commission
GASSP	Generally Accepted System Security Principles
GDPR	General Data Protection Regulations
GLBA	Gramm-Leach-BlileyAct
GMITS	The Guidelines for the Management of IT Security
HIPPA	Health Insurance Portability and Accountability Act
IBM	International Business Machines
IEC	International Electrotechnical Commission
ITIL	Information Technology Infrastructure Library
ISO	International Standards Organization
IFLA	International Federation of Library Associations
IoT	Internet of Things
İKM	İnsan Kaynakları Merkezi
KDB	Kütüphane ve Dokümantasyon Başkanlığı
KVKK	Kişisel Verileri Koruma Kurumu
NIST	National Institute of Standards and Technology
NSTISSI	National Training Standard for Information Systems Security
OECD	Organization for Economic Co-operation and Develoment

ÖİDB	Öğrenci İşleri Daire Başkanlığı
PCI DSS	The Payment Card Industry Data Security Standard
PDB	Personel Daire Başkanlığı
PIPEDA	Personal Information Protection and Electronic Documents Act
SPSS	Statistical Package Social Sciences
TCDDK	Türkiye Cumhurbaşkanlığı Devlet Denetleme Kurulu
TCK	Türk Ceza Kanunu
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırmalar Kurumu
TSE	Türk Standartlar Enstitüsü
UPS	Uninterruptible Power Source
VERBİS	Veri Sorumluları Sicili

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

BİRİNCİ BÖLÜM

GİRİŞ

1.1. KONUNUN ÖNEMİ

Endüstri 4.0'ın etkisinde fiziksel ve elektronik varlıkların birbirleri ile entegre olduğu eğitim, sağlık, bankacılık gibi farklı sektörlerde bilgi güvenliği önemli gündem konuları arasında yer almaktadır (Genç, 2019, s.65). Bilginin elektronik ortamda yoğun bir şekilde kullanılması ve paylaşılması ise kurum ve kuruluşların çeşitli güvenlik ve risk sorunlarıyla karşılaşmasına neden olmaktadır (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009, s.597).

Bilginin aşırı ve yoğun kullanımıyla gelen güvenlik ve risk sorunları ise kurumdaki pazar, ürün, teknoloji ve organizasyona ait bilgilerin tamamı olarak adlandırılan bilgi varlıklarının zarar görmesine neden olmaktadır (Yılmaz, 2014, 47). Bununla birlikte, bilgiye yetkisiz veya izinsiz bir biçimde erişilmesi, bilginin kullanılması, değiştirilmesi, ortadan kaldırılması ve üçüncü kişilerle paylaşılması bilgi güvenliğini tehdit eden unsurlar arasında yer almaktadır (Çam, Aslay ve Özen, 2019, s. 1).

Endüstri 4.0 olarak adlandırılan sanayi devriminin dördüncü aşamasıyla gelen (yapay zekâ, büyük veri, vb.) yeniliklerle birlikte kişisel verilerin güvenilirliğinin sağlanması zorunlu hale gelmiştir (Şişkin ve Çakmak, 2019, s. 467). Bununla birlikte, kamu verilerinin elektronik ortamda hizmet sunumuna başlanması, bireylere yönelik kişisel verilerin sayısallaştırılmasına neden olmuştur. Sayısallaştırılmayla birlikte, verilerin gizliliğinin, bütünlülüğünün ve erişilebilirliğinin korunması gerekmektedir. İnsanların temel hak ve özgürlüğünün sağlanması noktasında, bilgi güvenliği unsurlarının yerine getirilmemesi kişisel verilerin önemini gün geçtikçe artırmaktadır. Kişisel veriler ile bilgi güvenliği arasındaki gizlilik, bütünlük ve kullanılabilirlik ilişkisi, kişisel verilerin bilgi güvenliği alanında ele alınmasına neden olmuştur. Söz konusu, iki kavram literatür çalışmalarına da birlikte anılmıştır (Ağıralan, 2015; Henkoğlu, 2015a; Erdinç, 2017; Başdinkçi, 2017; Turan, 2018; Genç 2019).

Toplumsal gelişme ve değişme noktasında eğitim kurumları bireylerin ve toplumun yapısının ilerleme kaydedebilmesinde önemli bir değişkendir. Bu rolde önemli bir rol üstlenen yükseköğretim kurumları, bilgi ekonomisi olarak da adlandırılan dijital devrimin "hammaddesi" ve "sermayesi" olan bilginin üretiminden ve paylaşılmasından sorumlu kurumlardır (Vardal, 2009, s.4). Bu kurumlarda, kişisel verilerin işlendiği, tutulduğu ve bireylerin bilgi kullanımlarının ve bilgi aramaya yönelik davranışlarda bulundukları birim ise bilgi merkezleridir. Bireylerin bilgi arama davranışlarının kayıt altına alınması, ödünç-alma verme işlemlerindeki kayıtlar, veri tabanı kullanım analizleri ve elektronik ortamdaki veri girişleri (kişisel bilgiler, taranan web sayfaları vb.) gibi kişisel bilgi yönetimi olarak da adlandırılan bilgi yönetimi davranışlarını oluşturmaktadır. Söz konusu bilgi arama davranışlarına yönelik katma değerli hizmetlerin sunulmasını odağına alan bu birimlerde söz konusu hizmetlerin geliştirilebilmesi ve etkinliğinin sağlanabilmesi için birçok kişisel veriden yararlanılmaktadır.

Bilgi güvenliği alanının geniş bir kapsama sahip olması Kütüphanecilik ve Bilgi Bilimi alanında konuyla ilgili çalışmaların çeşitlilik ve farklılık göstermesine neden olmuştur. Örneğin konuyla ilgili olarak hırsızlık, hasar, küflenme vb. risk konuları koleksiyon güvenliğinde ele alınırken, kullanıcıların kişisel eşyalarının kaybolması veya kütüphane personelinin sağlık koşulları gibi konular personel ve kullanıcı güvenliği başlığı altında incelenebilmektedir. Son on yılda uluslararası alanda üniversite kütüphanelerinde bilgi güvenliği üzerine yapılan çalışmalar, kütüphane bilgi ve bilgi kaynaklarının korunması, kullanıcı ve personel güvenliği, bilgi sistemlerinin güvenliği gibi konularda çeşitlilik göstermiştir (Kanyengo, 2009; Harris ve DiMarco, 2010; Abioye ve Rasaki, 2013). 2009 yılında bilgi kaynaklarının korunması konusu üzerine gerçekleştirilen bir araştırmada, dijital formattaki bilgilerin nasıl korunacağına ilişkin politikanın bulunmayışı, kullanıcıların aşırı kaynak kullanımı sonucunda kaynaklardaki artan aşınma ve yıpranma sebebiyle koleksiyonların yetersiz olması, yaz ve kış aylarında değişen iklim koşullarının eserlere zarar vermesi, nitelikli personel eksikliği, finansal yetersizlikler, koruma yöntemleri konusunda eğitimin eksik oluşu, kütüphanedeki haşere/böcekler, kütüphanedeki teknolojik araçların çok eski olması nedeniyle kütüphanede bilgi varlıklarının yeterli düzeyde korunamadığı belirlenmiştir (Kanyengo, 2009, 118-126). Kişisel güvenliğe yönelik tehditleri ele alan bir çalışmada ise (Harris ve DiMarco, 2010,

s. 27-36), güvenlik önlemi olarak adlandırılan kilitleme kavramından hareketle, hangi durumlarda kilitlemeye ihtiyaç duyulacağı ve güvenliğin kütüphanede kim tarafından sağlanacağı, kütüphanede herhangi bir olayla karşılaşıldığında nasıl davranılması gerektiği ve herhangi bir olayla karşılaşıldığında kütüphanelere düşen görev ve sorumlulukların neler olacağı gibi konular üzerinde durulmuştur. Üniversite kütüphanelerinde koleksiyon güvenliği uygulamasının durumunu değerlendirilerek, koleksiyon güvenliği uygulamalarında etkileyici faktörleri tespit etmeye çalışan bir araştırmada da (Maidabino ve Zainab, 2011, s.15-33), koleksiyon güvenliği yönetimi değerlendirme aracı geliştirilmiştir. Bu araçta, üniversite kütüphanelerinde koleksiyon güvenliğini sağlamaya yönelik altı kriter[1] tespit edilmiştir. Nijerya'daki dört üniversite kütüphanesi yöneticilerine uygulanan bu aracın sonucunda, kütüphanenin koleksiyon güvenliği uygulamalarının birbirinden farklı olduğu tespit edilmiştir. 2013 yılında gerçekleştirilen başka bir araştırmada ise, Güneybatı Nijerya'daki üniversite kütüphanelerinde güvenlik sorunları incelenmektedir. Araştırma sonucunda elde edilen verilere göre, üniversite kütüphanelerinin hırsızlık, kütüphane materyallerinin tahrif edilmesi, eserlerin yırtılması ve koparılması, kütüphane raflarında kitapların gizlenmesi, cep telefonu yoluyla yapılan gürültü gibi güvenlik sorunlarıyla karşı karşıya olduğu tespit edilmiştir (Abioye ve Rasaki, 2013, s.1). Araştırma sonuçlarına ek olarak, ders kitaplarının, seri yayınların ve referans materyallerinin kullanıcılar tarafından kötüye kullanıma karşı son derece duyarlı malzemeler olduğu belirlenmiştir. 2012 yılında yapılan başka bir araştırmada (Anday, Francese, Huurdeman, Yılmaz ve Zengenene, s.117), dijital kütüphanelerin kaynakların yönetiminde göz önünde bulundurması gereken güvenlik sorunlarına ilişkin literatür ortaya koyulmuştur. Yapılan araştırma sonucunda (Anday ve diğerleri, 2012, s.134);

- Kütüphanelerde güvenli bir altyapının sürdürülmesinin gerektiği belirlenmiştir.
- Kütüphanelerin ağ güvenliğine sahip olma ihtiyacı dijital kütüphanelerde bir zorunluluk olduğu ortaya çıkarılmıştır.
- Güvenlik riskleri ve özellikle web uygulaması güvenlik açıklıklarının sebebinin insan hataları olduğundan dolayı kütüphanelerde ciddiye alınmadığı ifade edilmiştir.

[1]Yönetim, işlemler ve süreçler, insan sorunları, fiziksel, aracılık faktörleri.

- Dijital bilginin giderek artması ve buna bağlı olarak dijital verilerin korunmasının zorlaştığı göz önüne alındığında, veri kayıplarını önlemek için yedeklemelerin yapılması ve koruma politikalarının bulundurulması gerektiği tespit edilmiştir.
- Bilgisayar sistemlerinin güvenliği farklı yollarla ihlal edilebildiğinden ve devlet kurumları kütüphane kullanıcıları hakkında soruşturma yapabileceğinden, kullanıcı bilgilerine yönelik farklı tehditler olduğu vurgulanmıştır.
- Kütüphaneler her zaman kullanıcı verilerinin korunmasına çok fazla dikkat etmemektedir. Bu noktada, kütüphanelerin güvenlik okuryazarlığına yatırım yapmaları ve kütüphane kullanıcılarının sistemlerini ve hizmetlerini korkmadan kullanılabilirliğini sağlamak için kullanıcı mahremiyetine yönelik uygulamaların ve düzenlemelerin gerekliliği dile getirilmiştir.

Türkiye'de elektronik bilgi güvenliğinin sağlanmasını hukukî ve etik sorumluluklar açısından inceleyen bir araştırmada (Henkoğlu ve Uçak, 2012, s. 377), bilgi profesyonellerinin bilgi güvenliği farkındalıklarının arttırılması ve bu hususta sorumlu oldukları mesleki etik değerler ve hukuk kuralları hakkında bilinçlenmelerinin sağlanmasının önemi vurgulanmıştır. Başka bir araştırmada ise, Ankara'daki 14 üniversite kütüphanesi yöneticilerinin bilgi güvenliği farkındalığı tespit edilmeye çalışılmıştır. Araştırmanın sonuçlarında, yöneticilerin bilgi güvenliği farkındalığına yönelik yeterli düzeyde bilgi sahibi olmadıkları belirlenmiştir (Öztemiz ve Yılmaz, 2013, s. 87).

Uluslararası alanda üniversite kütüphanelerde kişisel verilerin korunması üzerine pek çok çalışma yapılmıştır (Eric, 1997; Sturges, Teng ve Iliffe, 2001; Firarek, 2002; Sturges ve diğerleri, 2003; Shuler, 2004; Coombs, 2004; Bowers, 2006; Ness, LaPorte-Fiori ve Engwall, 2015; Noh, 2014; Noh, 2017). Bu çalışmalarda üniversite kütüphanelerinde veri korumaya yönelik yasal düzenlemelerin kütüphane yönetimine etkileri, kütüphanelerde mevcut koruma politikaları, uygulamaları ve farkındalık düzeyleri, dijital ortamda kullanıcı mahremiyetinin sağlanması ve kütüphane kayıtlarının gizliliğinin oluşturulması yönünden ele alınmıştır. Türkiye'de 2015 yılında doktora tezi olarak kabul edilen *"Hassas bilgi varlıklarının ve kişisel verilerin hukuksal düzenlemeler ile korunması ve bu kapsamda üniversiteler için bilgi güvenliği politikasının geliştirilmesi"* başlıklı yayında Ankara'daki 15 üniversite kurumunun Bilgi İşlem Daire Başkanlığı'nın (BİDB),

Kütüphane Daire Başkanlığı'nın (KDB) ve Personel Daire Başkanlığı'nın (PDB) mevcut bilgi güvenliğine yönelik durumu tespit edilerek, kişisel verilerin korunması ve bilgi güvenliği politikası geliştirilmiştir (Henkoğlu, 2015b, s.9-11). Söz konusu yayın, üniversite kütüphanelerinde kişisel verilerin korunması konusuyla ilgili başka bir yayına (Henkoğlu ve Uçak, 2015) kaynaklık etmektedir. Henkoğlu ve Uçak tarafından hazırlanan makalede (2015), mevcut hukuksal düzenlemeler ekseninde Ankara'daki 15 üniversite kütüphanesinin bilgi güvenliği önlemleri incelenmiştir. Yapılan araştırmanın sonuçlarına göre, Ankara'daki üniversite kütüphanelerinin kişisel verilerin korunmasına yönelik uygulamalarında (eğitim, politika, risk yönetimi gibi) eksiklikler ve yetersizlikler tespit edilmiştir (Henkoğlu ve Uçak, 2015, s. 45).

Yukarıda verilen bilgiler ışığında bu araştırmada, Ankara'daki üniversite kütüphanelerinde kullanıcılara güvenilir ortam ve hizmetlerin sunulabilmesi için karar vericilerin ve verilen kararları uygulayıcı pozisyonunda bulunan aktörlerin (yönetici ve personel) konu ile ilgili uygulamaların betimlenmesinin yanı sıra yönetici ve kütüphanecilerin mevcut koşullara yönelik yaklaşımlarının saptanması hedeflenmiştir.

1.2. ARAŞTIRMANIN AMACI, PROBLEMİ VE HİPOTEZİ

Üniversite kütüphanelerinde bilgi varlıklarının gizliliği, bütünlüğü, kullanılabilirliği kurumun imajını etkilemektedir. Bu sebeple, kurumun hassas bilgi varlıklarının gizliliğinin, güvenliğinin ve korunmasının sağlanması için kütüphane yöneticilerinin ve personelin bilgi güvenliği konusunda farkındalık sahibi olmaları ve bunun sağlanması için bilgi güvenliği eğitimlerini almaları gerekmektedir. Bu doğrultuda çalışma ile ulaşılması planlanan amaçlar aşağıda sıralanmaktadır:

- Ankara'daki üniversite kütüphanelerinin bilgi güvenliği uygulamalarına ilişkin mevcut durumlarını tespit etmek,
- Ankara'daki üniversite kütüphanelerinin kişisel veri yönetimi ve kişisel verilerin korunması kapsamındaki uygulamalarını betimlemek,
- Ankara'daki üniversite kütüphanelerinde kullanıcıların bilgi ile etkileşim kurdukları ortamlarda (bina, elektronik ve basılı ortamdaki koleksiyon, referans hizmetleri ve ödünç hizmetleri gibi bireysel etkileşim ortamları) kişisel bilgi yönetimi bağlamında kişisel verilerin elde edilmesi, işlenmesi, düzenlenmesine

yönelik koşulları betimleyerek konuyla ilgili iyileştirme gerektiren alanları tespit etmek,

- Literatür çalışmalarından yola çıkılarak, üniversite kütüphanelerinde kişisel verilerin korunması konusunda karar vericilerin ve bilgi profesyonellerin yaklaşımlarını saptamaktır.

Buradan hareketle, kütüphanelerin sürdürülebilir kalkınma noktasında yenilik süreci içerisinde yer alması, teknolojik gelişmelerin etkisinin kütüphanelere yansıması gibi koşullar göz önünde alındığında kütüphanelerin bir yenilik süreci içerisine girdiği söylenebilmektedir. Bilgi ve belge merkezleri olarak adlandırılan kütüphanelerin de sadece bir alanda değil, farklı alanlarda, farklı konularda ve farklı uygulamalarla teknoloji çağına adapte olması ve uyum sağlaması gerekmektedir. Belirtilen amaçlardan hareketle **araştırmada odaklanılan problemler şunlardır:**

1. Ankara'daki üniversite kütüphaneleri temel bütçe, bina, koleksiyon, kullanıcı ve personel gibi temel bileşenlere yönelik olarak bilgi güvenliği açısından ne tür sorunlar yaşamaktadır?
2. Ankara'daki üniversite kütüphanelerinin yöneticileri kurumlarındaki kişisel verilerin yönetimini nasıl gerçekleştirmektedir?
3. Ankara'daki üniversite kütüphaneleri kişisel verilerin yönetimi konusunda ne tür yetersizliklerle karşılaşmaktadır?
4. Ankara'daki üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin yönetimine yönelik karar verme ve verilen kararın uygulanması aşamasındaki yaklaşımlar nelerdir?
5. Ankara'daki üniversite kütüphaneleri bilgi güvenliği ve kişisel verilerin yönetimine dönük koşullarda en çok hangi noktalarda iyileştirmelere ihtiyaç duymaktadır?

Araştırmada belirlenen amaç ve problemlerden hareketle temel hipotezimiz *"Üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin yönetimine dönük karar verme ve uygulama düzeyindeki eksiklikler (politika, konuyla ilgili bilinç ve farkındalık, risk değerlendirmesi gibi konularda) bulunmaktadır."* şeklinde kurulmuştur. Bu hipotez doğrultusunda alt hipotezlerimiz ise şunlardır:

1. Ankara'daki üniversite kütüphanelerinin temel bileşenlerine (bina, koleksiyon, personel ve kullanıcı) yönelik bilgi güvenliği uygulamaları yetersizdir.
2. Kişisel verilerin düzenlenmesi, silinmesi, saklanması ve aktarılması konusunda Ankara'daki üniversite kütüphanelerinde politika eksiklikleri bulunmaktadır.
3. Ankara'daki üniversite kütüphanelerinde genel kişisel veri yönetimi uygulamalarında (personellere yönelik görev tanımlamalarının olmaması, kişisel verilerin kütüphanenin farklı birimlerinde işlenmesi ve kişisel verilere işlenmesine ve kullanılmasına yönelik kullanıcıların onaylarının alınmaması gibi) yetersizlikler bulunmaktadır.
4. Ankara'daki üniversite kütüphanelerinin kullanıcılara yönelik kişisel verilerin korunması ile ilgili aydınlatma metinlerinde eksiklikler (tutulması, silinmesi, aktarılması vb.) bulunmaktadır.
5. Ankara'daki üniversite kütüphanelerinde hangi kişisel verilerin toplanması gerektiğine yönelik bir düzenleme bulunmamaktadır.

1.3. ARAŞTIRMANIN İZNİ VE KAPSAMI

Araştırmanın kapsamını, bilginin sürekli olarak işlendiği, elde edildiği ve paylaşıldığı kurumlar arasında yer alan üniversite kütüphaneleri oluşturmaktadır. Bu bağlamda araştırma Ankara'da bulunan üniversite kütüphanelerinin gerçekleştirdikleri uygulamalarla sınırlandırılmıştır. Belirlenen kapsam doğrultusunda, üniversite kütüphanelerinde konuyla ilgili uygulamaların planlanması ve oluşturulması bağlamında sorumlulukları bulunan karar vericiler (müdür ve müdür yardımcıları) ile verilen kararların uygulanmasında görev alan kütüphanecilerin yaklaşımlarının betimlenmesi hedeflenmiştir. Araştırma kapsamından hareketle analizlerin aşağıdaki üniversitelerdeki kütüphanelerde gerçekleştirilmesi planlanmıştır:

1. Anka Teknoloji Üniversitesi
2. Ankara Hacı Bayram Veli Üniversitesi
3. Ankara Medipol Üniversitesi
4. Ankara Müzik ve Güzel Sanatlar Üniversitesi
5. Ankara Sosyal Bilimler Üniversitesi
6. Ankara Üniversitesi
7. Atılım Üniversitesi

8. Ankara Yıldırım Beyazıt Üniversitesi
9. Başkent Üniversitesi
10. Çankaya Üniversitesi
11. Gazi Üniversitesi
12. Hacettepe Üniversitesi
13. İhsan Doğramacı Bilkent Üniversitesi
14. Lokman Hekim Üniversitesi
15. Orta Doğu Teknik Üniversitesi
16. Ostim Teknik Üniversitesi
17. Ufuk Üniversitesi
18. Türk Eğitim Derneği Üniversitesi
19. TOBB Ekonomi ve Teknoloji Üniversitesi
20. Türk Hava Kurumu Üniversitesi
21. Yüksek İhtisas Üniversitesi

Araştırma verileri 29 Nisan 2019 - 23 Eylül 2019 tarihleri arasında toplanmıştır. Araştırma kapsamında ele alınan 21 üniversite kütüphanesinin içerisinde yer alan 6 üniversite kütüphanesi (Başkent Üniversitesi, Ankara Hacı Bayram Veli Üniversitesi, Anka Teknoloji Üniversitesi, , Ankara Müzik ve Güzel Sanatlar Üniversitesi, Ankara Medipol Üniversitesi, Ostim Teknik Üniversitesi) üniversite kütüphanelerinin hazırlık aşamasında olması, üniversitenin yeni bir üniversite olması sebebiyle kütüphanenin henüz yapılandırılmaması ve etik kurul izinlerine olumsuz yanıt verilmesinden dolayı araştırma kapsamına dâhil edilmemiştir. Diğer taraftan, araştırmanın yürütülebilmesi için öncelikle 1 Temmuz 2019 tarihinde Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Etik Kurul Komisyonu adı altında etik kurul izni alınmıştır. Ayrıca, araştırma kapsamında Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü tarafından hazırlanan tez araştırmasına yönelik etik kurul izni ve üst yazı ile birlikte, iki üniversite kütüphanesine görüşme başvurusu yapılmıştır. Söz konusu yazılara ilişkin izinler, 17 Temmuz 2019 tarihinde Ufuk Üniversitesi ve 15 Ağustos 2019 tarihinde Orta Doğu Teknik Üniversitesi İnsan Araştırmaları Etik Kurulundan alınmıştır.

1.4. ARAŞTIRMANIN YÖNTEMİ VE VERİ TOPLAMA TEKNİKLERİ

Belirtilen amaçlara ulaşmak, problemlere ve hipotezlere yönelik analizleri gerçekleştirebilmek için araştırmada tercih edilen betimleme yöntemi, *"olayların, objelerin, varlıkların, kurumların, grupların ve çeşitli alanların ne olduğunu açıklamayı sağlayan"* araştırma methodu şeklinde tanımlanmaktadır (Kaptan, 1989, s.34). Bu kapsamda araştırmada belirlenen amaçlara ulaşmak için araştırmanın verileri betimleme yöntemi çerçevesinde *"çok sayıda yöntem ve kaynak kullanarak, insan deneyimlerine ilişkinin sözlü ve yazılı anlatımları ya da kayıtları inceleyen"* nitel veri toplama tekniği kullanılarak elde edilmiştir (Punch, 2005, s.165). Araştırma bir önceki bölümde belirtilen kapsamda ve izinlerin sağlandığı 6 devlet ve 9 vakıf üniversite kütüphanesinde gerçekleştirilmiştir. Söz konusu üniversite kütüphanelerindeki uygulamaların betimlenmesi için araştırma verileri görüşme ve anket teknikleriyle toplanmıştır. Görüşme, "insanların neyi ve neden düşündüklerini, duygu, tutum ve hislerinin neler olduğunu, davranışlarını yönlendiren etkenleri ortaya çıkarmayı sağlayan bir veri toplama aracı" olarak ifade edilmektedir (Ekiz, 2015, s.62). Bu çerçevede çalışmada yarı yapılandırılmış görüşme tekniğinden yararlanılmıştır. Robson'a göre yarı yapılandırılmış görüşme tekniği şu şekilde açıklanmaktadır (2015, s.347):

> *"Görüşmeci, kapsam ile ilgili başlıkların kontrol listesini, varsayılan ifadeleri ve soruların sırasını sunan bir görüşme rehberine sahiptir. Ancak, genellikle, ifadelerin ve soruların sırası görüşmenin akışına göre şekillenmektedir ve ek olarak görüşülen kişinin söylediklerini devam ettirebilmek için planlanmamış sorular da sorulabilmektedir"*

Araştırmada kullanılan bir diğer veri toplama tekniği olan anket ise *"insanların yaşam koşullarını, davranışlarını, inançlarını, görüşlerini veya tutumlarını betimlemeye yönelik bir dizi sorudan oluşan bir araştırma materyali"* olarak tanımlanmakta ve farklı yöntemler (internet ortamında, posta yolu, yüz yüze iletişim) kullanılarak gerçekleştirilebilmektedir (Akalın, 2018, s.15-16).

Bu bilgiler ışığında, üniversite kütüphanelerindeki karar vericilerin (müdür ve müdür yardımcılarının) konu ile ilgili gerçekleştirdikleri uygulamaları tespit etmek amacıyla yarı yapılandırılmış görüşmeleri gerçekleştirmek için bir görüşme formu geliştirilmiştir.

Konuyla ilgili uygulayıcıların (kütüphanecilerin) görüşleri ise anket aracılığıyla analiz edilmiştir. Her iki aracın hazırlanmasında literatürdeki çalışmalardan faydalanılmıştır.

1.4.1. Görüşme Formuna Yönelik Bilgiler

Geliştirilen görüşme formu öncelikle kişisel verilerin kütüphanelerde nasıl elde edildiği, hangi koşullar altında işlendiği, aktarıldığı ve silindiği ve kişisel verilerin nasıl yönetildiği konusunda yapılan uygulamaları ve eksiklikleri belirlemek için 15 Mart 2019 tarihinde Hacettepe Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı/Daire Başkan Vekili Pınar Al ile ön görüşme gerçekleştirilerek hazırlanmıştır. Daha sonraki aşamada ise, dış değerlendirmecilerden (editör, müdür vb.) yararlanılmıştır. 16 Nisan 2019 tarihinde Hacettepe Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı/Daire Başkan Yardımcısı Selahattin Cihan Doğan, 22 Nisan 2019 tarihinde Ankara Yıldırım Beyazıt Üniversitesi Bilgi ve Belge Yönetimi Bölümü Araştırma Görevlisi Müge Akbulut ve 26 Nisan 2019 tarihinde Hacettepe Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı/Beytepe Kütüphanesi Müdürü Çiğdem Topuz ile görüşülerek formdaki sorulara ilişkin ön değerlendirmeler tamamlanmıştır. Bu görüşmelerden alınan geri bildirimlerle araştırma aracına son hali verilmiştir.

Üniversite kütüphane yöneticileri ile yapılacak olan görüşmeler ise, üniversite kütüphanelerinde karar verici konumunda olan müdür ve müdür yardımcıları ile yüz yüze ve telefonla iletişim kurularak gerçekleştirilmiştir. Görüşme tekniği sürecinde hiçbir şekilde ses/video/görüntü kaydı gibi kayıtlar tutulmamıştır. Bu süreçte ise, araştırmanın hipotezi ve yöntemi çerçevesinde açık uçlu/standardize edilmiş sorular hazırlanarak deneklerle yapılan görüşmeler sonucunda elde edilen veriler kayıt edilerek, bilgisayar ortamında bir veri analizi yazılımına girilmiş ve bu yazılımdaki tanımlayıcı istatistiklere yönelik çıktılardan yararlanılmıştır. Araştırmada elde edilecek nitel veriler ise *"insanların söyledikleri ve yazdıklarının açık talimatlara göre kodlanarak nicelleştirilmesi-sayısallaştırılması süreci"* olarak tanımlanan içerik analizi yöntemiyle değerlendirilecektir (Balcı, 2013, s.220).

Yöneticilerin kütüphanelerdeki gerçekleştirdikleri uygulamaları belirlemek amacıyla hazırlanan görüşme formu, demografik bilgiler, kişisel verilerin korunması ve bilgi

güvenliği uygulamalarına yönelik olmak üzere üç bölümden oluşmaktadır. Birinci bölümde, yöneticilerin yaşı, eğitim düzeyi, görevi, çalışma süresi ve lisans eğitimi olmak üzere demografik bilgiler yer almaktadır. Kişisel verilerin yönetimini içeren ikinci bölümde ise, üniversite kütüphanelerinde kişisel verilerin yönetilmesine ve korunmasına yönelik gerçekleştirilen iş ve işlemlere (kişisel verilerin belirlenmesi, toplanması, kayıt altına alınması, saklanması, silinmesi, aktarılması vb.) yönelik olmak üzere yirmi dört soru bulunmaktadır. Bu bölümde yer alan 14 ve 15. sorular, Henkoğlu (2015b, 249-250), tarafından yayınlanan bir çalışmadan alınmıştır. Üçüncü bölüm olan son bölümde ise, üniversite kütüphanelerinde kurumsal, bina, koleksiyon, personel ve kullanıcı, yazılım ve donanım olmak üzere toplam beş soru, alt sorulardan oluşturularak detaylandırılmıştır. Bu bölümün son sorusunu ise, üniversite kütüphanelerinde yöneticilerin, kurumlarındaki bilgi güvenliği uygulamalarının düzeylerinin belirlenmesi ve bu uygulamaları gelecek beş yılın sonunda iyileştirme ve geliştirme etkinlikleri değerlendirilmektedir. Literatür çalışmalarına ve ön görüşmelere dayanılarak oluşturulan görüşme formu ve soruların dağılımı aşağıdaki gibidir:

Görüşme formu;

- Birinci bölüm: Yöneticilerin yaş, eğitim durumu, çalışma süresi vb. özelliklerini tespit etmek amacıyla açık uçlu ve tek şıklı olmak üzere toplamda beş sorudan oluşmaktadır.
- İkinci bölüm: Yöneticilerin kişisel veri yönetimi hakkında uygulamalarını belirlemek amacıyla oluşturulan çok seçenekli ve açık uçlu olmak üzere toplamda 24 soru yer almaktadır.
- Üçüncü bölüm: Üniversite kütüphanelerinde bilgi güvenliği uygulamalarını (kurumsal, bina, koleksiyon vb.) tespit etmek amacıyla oluşturulan 4 seçenekli sorular ve 5'li Likert ölçekli soru olmak üzere toplamda 6 soru bulunmaktadır.

Üniversite kütüphanelerinde bilgi güvenliğine yönelik mevcut durumun tespit edilmesi ve karşılaşılan sorunların belirlenmesi amacıyla geliştirilen görüşme formunda herhangi bir kişisel veri tutulmamıştır. Görüşme formuna yanıt veren yöneticilerin 6'sı 41-50 yaş aralığında, 4'ü 30-40 yaş aralığında iken, 3'ü 51-60 yaş aralığındadır. Yöneticilerin 1'i ise, 61-70 yaş aralığında yer almaktadır. Bu soruyu yanıtlamayan yönetici sayısı ise 1'dir.

Yöneticilerin eğitim düzeyleri incelendiğinde ise 15 üniversite kütüphanesi yöneticisinin

3’ü doktora mezunu, 7’si lisans mezunu, 4’ü yüksek lisans mezunudur. Bir yönetici ise eğitim düzeyine yönelik olan bu soruya yanıt vermemiştir. Yöneticilerin 8’i Daire Başkanı/Başkan Vekili unvanıyla görev alırken, 6’sı Müdür/Direktör unvanıyla görev almaktadır. Bu soruya yanıt vermeyen yönetici sayısı ise 1’dir. Yöneticilerin çalışma sürelerine yönelik olarak verilen yanıtlar analiz edildiğinde; yöneticilerin 7’si 1-9 yıl arası, 5’i 10-19 yıl arası, biri ise 20-29 yıl arasıdır. Çalışma süreleri ile ilgili olarak sorulan bu soruya yanıt vermeyen yöneticilerin sayısı ise 2’dir. Yöneticilerin lisans eğitimlerine ilişkin bulgular araştırmaya katılan 10 üniversitedeki yöneticilerin Bilgi ve Belge Yönetimi Bölümü lisans programından mezun olduğunu göstermektedir. Diğer yandan dört üniversitedeki yöneticilerin ise farklı bir lisans programından mezun olduğu anlaşılmıştır. Bu bölümler Moleküler Biyoloji ve Genetik, Alman Dili ve Edebiyatı ve İstatistiktir. Bir yönetici ilgili soruya yanıt vermemiştir.

1.4.2. Anket ile İlgili Bilgiler

Araştırma aracının gerçekleştirilebilmesi için öncelikle, Hacettepe Üniversitesi kütüphanelerinin abone olduğu veri tabanları, diğer üniversitelerin kütüphane sayfaları, kurum ve kuruluşların konuyla alakalı yayınları ve raporları, konu ile ilgili yayınlanan kitaplar, Yüksek Öğretim Kurumları tez sistemine yüklenen yüksek lisans ve doktora tezleri, Türkiye Belge Sağlama ve Ödünç Verme Sistemi incelenmiştir. Buradan hareketle kütüphanecilere uygulanmak üzere geliştirilen ankette çoktan seçmeli, açık uçlu ve beşli Likert ölçekli sorulardan oluşan 18 soru bulunmaktadır.

Personellerin kişisel verilerin yönetimi ve bilgi güvenliği konusundaki farkındalıklarını ölçmek amacıyla geliştirilen değerlendirme aracı ise, 16 Nisan 2019 tarihinde Hacettepe Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı/Daire Başkan Yardımcısı Selahattin Cihan Doğan, 19 Nisan 2019 tarihinde Ankara Yıldırım Beyazıt Üniversitesi kütüphane personeli Esra Çalış ile görüşülerek anket soruları değerlendirilmiştir.

Bu araştırmada kütüphaneciler ile gerçekleştirilen anket çalışması ise, ankete yanıt verme oranının daha yüksek olması, eksiklikleri tamamlama ve daha sağlıklı veri alarak konu ile ilgili bilinç ve farkındalığı en iyi şekilde tespit edebilme olanağı sunması nedeniyle

her üniversite kütüphanesi yöneticilerinden randevu alınarak kütüphanecilerle yüz yüze görüşme gerçekleştirilmiştir. İş yoğunluğundan dolayı kütüphanecilerin bazısı anket formlarına mail aracılığıyla yanıt vermiştir.

Tez verilerinin toplanması zarfında ise, izin sürecinde olan ve ankete gönüllü katılımı olmayan personeller araştırma kapsamına alınmamıştır. 207[2] kütüphane personeli arasından ankete katılım gösteren 95 kütüphanecinin anketi cevaplama oranı %45'dir. Bu kapsamda Tablo 1'de anket aracına katılım gösteren kütüphanecilerin üniversite kurumlarına göre dağılımları yer almaktadır.

Tablo1. Kütüphaneci sayılarının üniversitelere göre dağılımları

Üniversite	**S**	**%**
Orta Doğu Teknik Üniversitesi	19	20,0
Hacettepe Üniversitesi	14	14,7
İhsan Doğramacı Bilkent Üniversitesi	13	13,7
Atılım Üniversitesi	9	9,5
Gazi Üniversitesi	7	7,4
TOBB Ekonomi ve Teknoloji Üniversitesi	7	7,4
Ankara Üniversitesi	5	5,3
Ankara Yıldırım Beyazıt Üniversitesi	4	4,2
Çankaya Üniversitesi	4	4,2
Türk Eğitim Derneği Üniversitesi	4	4,2
Ufuk Üniversitesi	3	3,2
Ankara Sosyal Bilimler Üniversitesi	2	2,1
Türk Hava Kurumu Üniversitesi	2	2,1
Lokman Hekim Üniversitesi	1	1,1
Yüksek İhtisas Üniversitesi	1	1,1
Toplam	95	100

Literatür çalışmalarına ve ön görüşmelere dayanılarak anketteki soruların dağılımı aşağıdaki gibidir:

- Birinci bölüm: Kütüphanecilerin yaş, eğitim, çalışma süreleri vb. özelliklerinin tespit etmek amacıyla oluşturulan açık uçlu ve tek şıklı sorular olmak üzere toplamda 5 soru yer almaktadır.

[2]Araştırma sürecinde, kapsama alınan üniversite kütüphanelerinin web sayfalarından personel sayıları alınmıştır.

- İkinci bölüm: Kütüphanecilerin kişisel verilerin korunması ve bilgi güvenliği farkındalığını belirlemek amacıyla oluşturulan şıklı, 5'li Likert ölçekli sorular olmak üzere toplamda 12 soru bulunmaktadır.

Üniversite kütüphanelerinde bilgi güvenliğine yönelik mevcut durumun tespit edilmesi amacıyla gerçekleştirilen değerlendirme aracına yanıt veren katılımcıların demografik bilgilerine göre; 30-39 yaş aralığında 43 kütüphaneci, 40-49 yaş aralığında 27 kütüphaneci, 24-29 yaş aralığında 15 kütüphaneci ve son olarak 50-59 yaş aralığında 3 kütüphaneci yer almaktadır. Yaşını belirtmeyen kütüphanecilerin sayısı ise 7'dir.
Değerlendirme aracına yanıt veren kütüphanecilerin 72'si lisans mezunudur. Kütüphanecilerin 17'si yüksek lisans mezunudur. İki kütüphaneci ön lisans ve iki kütüphaneci doktora, bir kütüphaneci ise lise mezunudur. Bir kütüphaneci soruyu yanıtsız bırakmıştır. Kütüphanecilerin eğitim bilgilerine göre 86 kütüphaneci Bilgi ve Belge Yönetimi mezunu iken 6 bu bölümden mezunu olmadığını belirtmiştir. İki kütüphaneci ise, diğer seçeneğini işaretlemiştir. Bu soruya yanıt vermeyen kütüphaneci sayısı 1'dir.

Değerlendirme aracına yanıt veren kütüphanecilerin görevlerine ilişkin dağılımları ise; 63 katılımcı kütüphaneci, 22 katılımcı uzman kütüphaneci, 3 katılımcı teknik personel, 2 katılımcı idari hizmetler, 2 katılımcı birim sorumlusu ve 1 katılımcı diğer olmak üzere toplamda 93 kişi olacak şekildedir. 2 kütüphaneci bu soruyu yanıtlamamıştır.

Kütüphanecilerin 62'si 0-10 yıl arası üniversite kütüphanelerinde görev aldığını belirtirken, geriye kalan bölümü 18 kütüphaneci 11-20 yıl arası ve 12 kütüphaneci ise, 21-30 yıl aralığında görev almaktadır. Bu soruyu yanıtlamayan kütüphanecilerin sayısı ise 3'tür.

1.4.3. Anket ve Görüşme Formlarıyla Toplanan Verilerin Analizi

Anket çalışmasının değerlendirilmesinde IBM SPSS STATISTICS 22 (International Business Machines Statistical Package Social Sciences) programından yararlanılarak her bir bölüm için ayrı ayrı analizler gerçekleştirilmiştir. Analizlerde bu programın kullanılmasında Filiz Ersöz ve Taner Ersöz'ün (2019) "SPSS ile İstatiksel Veri Analizi" ve Abdullah Can'ın (2014) "SPSS ile Bilimsel Araştırma Sürecinde Nicel Veri Analizi" başlıklı çalışmalardan faydalanılmıştır.

Araştırmadaki testten ele edilen puanların geçerli ve güvenilir olması katılımcıların davranışlarını tahmin etmedeki başarı ile orantılıdır. Geçerlik, testin bireyin ölçülmek istenen özelliğini ne derecede doğru ölçtüğüyle ilgili bir kavramdır. Güvenilirlik ise, bireylerin test maddelerine verdikleri yanıtlar arasındaki tutarlılık olarak tanımlanmaktadır ve testin ölçmek istediği özelliği ne derecede doğru ölçtüğü ile ilgilidir (Büyüköztürk, 2018, s. 179-182).

Anket çalışmasının içsel tutarlığına dair güvenilirlik derecesi Crombach Alpha değeri ile belirlenmiştir. Söz konusu değer ise, SPSS güvenilirlik analizi kullanılarak hesaplanmıştır. Sosyal bilimlerde popüler bir bileşik güvenilirlik endeksi olan Crombach Alpha, ilişkili olmayan ölçüm hataları ile sabit benzer bileşenler için güvenilirlik konusunda daha düşük bir sınır olan bir popülasyon miktarını tahmin etmektedir (Boyd, 2002, s.1). 0-1 arasında değer alabilen α katsayısı ile ölçeğin güvenilirliği şu şekilde yorumlanmaktadır (Güriş ve Astar, 2014, s.246):

- *"0≤ α < 0.5 ise güvenilir değil,*
- *0.5≤ α < 0.6 ise düşük güvenilir,*
- *0.6≤ α < 0.7 ise kabul edilebilir derecede güvenilir,*
- *0.7≤ α < 0.9 ise iyi derecede güvenilir,*
- *α>0.9 ise çok iyi."*

Araştırmada personel değerlendirme aracına ait demografik değişkenlere ilişkin sorular çıkarıldığında Cronbach Alpha katsayısı 0,92 çıkmıştır. Söz konusu değer anketin yüksek derecede güvenilir olduğunu belirtmektedir. Demografik değişkenler geçerlilik analizine eklendiğinde ise, Cronbach Alpha katsayısı 0,75 çıkmıştır. Bu değer ise, anketin oldukça güvenilir olduğunu göstermektedir.

Anketlerden elde edilen bulgular genellikle sıklık, ortanca, standart sapma, aritmetik ortalama, yüzde vb. verileri içeren tanımlayıcı istatistiklerle sunulmuştur. Araştırmamızda aritmetik ortalama değerlerinin hesaplanmasında, değerlerin sapmasına grupların verdikleri yanıtlarda tutarsızlık olması yol açabilmektedir (Çakmak, 2011, s.11). Aritmetik ortalama kullanılarak hesaplanan testlerde tüm değerleri hesaba katmamız gerekebilmektedir. Ancak burada, bir iki adet çok yüksek ya da düşük değer söz konusu ise, ortalama suni olarak düşüş ya da artış gösterebilmektedir. Bu gibi

durumlarda, medyan kullanılırken, yanlış yönlendirmelere de sebep olabilmektedir. Bu nedenle tüm değerlerin analiz edildiği durumlarda, serinin değişkenliğinin hesaplanmasında varyans ve standart sapma kullanılmaktadır (Baş, 2003, s.129-130). Aritmetik ortalama değerinden sapmaların ortaya konulabilmesi için ilgili tablolara ilişkin standart sapma değerlerinin belirlenmesi uygun görülmüş; bu hesaplamalarda aşağıdaki ortalama ve standart sapma formülleri dikkate alınmıştır (Ünver, Gamgam ve Altunkaynak, 2019, s.37-51).

- Kitleden seçilen bir örneklemden veri elde edildiyse örnekteki birim sayısı *n* olmak üzere bu örnek için aritmetik ortalama:

$$\bar{X} = \frac{\sum_{i=1}^{N} X_i}{n}$$

- Varyansın pozitif karakökü olarak tanımlanan standart sapma ise:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N} (Xi - \bar{X})^2}{n-1}}$$

Bulgularda sunulan standart sapma değerlerinde (Baş, 2001'den aktaran; Çakmak, 2011, s.12):

- σ < 0,75 ise deneklerin yanıtları belirli bir noktaya yoğunlaştığı ve yanıtlar arasında hiçbir sapma olmadığı,
- σ < 1 yanıtların belirli sonuçlar üzerinde yoğunlaştığı ve sapma olmadığını,
- σ > 1,25 değerinden yüksek olanların dağınık ancak istatistikî açıdan kabul edilebilir nitelikte oldukları,
- σ > 1,50 değerinin üzerindeki değerler için ise yanıt sayısının ya çok küçük bir küme oluşturduğu ya da birbirlerinden oldukça farklı değişkenler üzerinde dağınık olarak sıralandığı dikkate alınarak, bu değerlerin güvenilirlik açısından zayıf düzeyde oldukları göz önünde bulundurulmuştur.

1.5. ARAŞTIRMANIN DÜZENİ

Araştırma kapsamında yapılan araştırmalar ve bulgular altı bölüm başlığıyla sunulmuştur. Bu bölümlerin araştırma içerisindeki bölümlerine yönelik içerikleri şu şekildedir;

I. Bölümde, araştırmanın önemi, araştırmanın amacı, problemi ve hipotezi, araştırmanın kapsamı, yöntemi ve veri toplama teknikleri ve araştırmanın düzeni, araştırmanın gerçekleştirilmesinde kullanılan kaynaklar ve kaynaklara erişimde izlenen yollar ile ilgili bilgiler yer almaktadır.

II. Bölümde bilgi güvenliği kavramı, bilgi güvenliğinin bileşenleri, uluslararası bilgi güvenliği standartları, bilgi güvenliğine yönelik kanunlar ve uygulamalar ve kişisel verilerin korunması anlatılmıştır.

III. Bölümde üniversite kütüphanelerinde bilgi güvenliği uygulamaları ve kişisel verilerin yönetimine değinilmiştir.

IV. Bölümde yöneticilerin ve kütüphanecilerin bilgi güvenliği ve kişisel verilerin korunmasına yönelik bilinç ve farkındalıkları görüşmeler ve anket çerçevesinde incelenmiştir.

V. Bölümde araştırmada ele alınan konular doğrultusunda bulgulardan elde edilen sonuçlar değerlendirilmiştir.

1.6. KAYNAKLAR

Araştırma kapsamında literatür taraması yapılmış; araştırmanın gerçekleştirilmesinde Hacettepe Üniversitesi Kütüphanelerinin abone olduğu veri tabanları, diğer üniversitelerin kütüphane sayfaları, kurum ve kuruluşların konuyla alakalı yayınları ve raporları, konu ile ilgili yayınlanan kitaplar, Yüksek Öğretim Kurumları tez sistemine yüklenen yüksek lisans ve doktora tezleri araştırılmıştır. Ayrıca, veri koruma, veri güvenliği gibi alanlardaki kaynaklarda, kanunlarda, veri tabanlarında açık erişim arşivlerinde araştırma sürecinde tarama yapılmıştır. Araştırma süresince kullanılan bazı kaynakların listesi aşağıda sunulmaktadır;

Aslib Journal of Information Management
Annual Rewiev of Information Science and Technology
Applied Ergonomics
Association of Research Libraries
Bilgi Dünyası (2000 -)
Education Resources Information Center
European Union Law (EUR-LEX)
Hacettepe Üniversitesi Hukuk Fakültesi Dergisi
Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi
International Journal of Management & Information Systems
Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi
Journal of the American Society for Information Science and Technology
Journal of Mobile, Embedded and Distributed Systems
Library & Archival Security (1978-2014)
Library Management
Library Phisophy and Practice
Library Collections, Acquisitions & Technical Services
IEEE Security and Privacy Magazine
International Journal of Advanced Research in Computer Science and Software Engineering
Yüksek Öğretim Kurumları Ulusal Tez Merkezi
Proquest

Türk Kütüphaneciliği (1987-)
Türk Kütüphaneciler Derneği Bülteni (1952-1986)
Yönetim Bilişim Sistemleri Dergisi

Araştırmada kullanılan kaynaklara ek olarak uluslararası ve ulusal alanda üniversite kütüphanelerinin ve konu ile ilgili kurumların (IFLA, ALA, NIST) web sayfaları konu ile ilişkili olarak incelenmiştir. Yapılan incelemelerde kullanılan anahtar kavramlar aşağıda İngilizce-Türkçe olarak sıralanmaktadır;

Personal data,	Kişisel veri,
Protection of personal data,	Kişisel verilerin korunması
Privacy,	Mahremiyeti,
User privacy,	Kullanıcı mahremiyeti,
Personal information management,	Kişisel bilgi yönetimi,
Data Security,	Veri güvenliği,
Data Act,	Veri hukuku,
Information Security,	Bilgi güvenliği,
Information Security Standards,	Bilgi güvenliği standartları,
Information Security of Academic Libraries,	Akademik kütüphanelerin bilgi güvenliği
Collection security,	Koleksiyon güvenliği
Collection security management,	Koleksiyon güvenliği yönetimi
Building security (Pyhsical security),	Bina güvenliği (Fiziksel güvenlik),
Software and hardware security,	Yazılım ve donanım güvenliği
Academic libraries,	Akademik kütüphaneler
Security,	Güvenlik

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü tarafından hazırlanan Tez Yazım Yönergesi (2019) araştırma raporunun yazımında kullanılmıştır. Ayrıca araştırma raporunda yararlanılan kaynak olarak gösterme kuralı olarak Amerikan Psychological Association (APA) Kaynak Gösterme Kuralları 6. Basımı dikkate alınmıştır.

İKİNCİ BÖLÜM

BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLERİN YÖNETİMİ

Nesnelerin interneti (Internet of Things, IoT), yapay zekâ, arttırılmış gerçeklik gibi yenilikler ile şekillenen içerisinde olduğumuz dijital çağ, bilgi ve iletişim teknolojileri ışığında gelişim göstermektedir. Söz konusu bilgi ve iletişim teknolojilerindeki gelişmelerin temelinde ise bilginin ham maddesi olarak nitelendirebileceğimiz veriler ve bu verilerin işlenmesi yer almaktadır. Günlük aktivitelerimizde ve mesleki yaşantımızda çeşitlilik gösteren ve teknolojik olanaklarla birlikte kolaylıkla üretilebilen verilerin önemli bir kısmı bireylere özgü olan kişisel veri niteliği taşımaktadır. Bireylere ait olan kişisel verilerin, teknolojik araçlar ve yazılımlarla kolaylıkla işlenmesi bu verilerin güvenliğine yönelik bazı risk ve tehditlerin ortaya çıkmasına neden olabilmektedir. Bu risk ve tehditleri, bireylere özgü olan kişisel verilerin yetkisiz erişimi, izinsiz bir şekilde kullanılması, değiştirilmesi veya verilerin depolandığı teknik altyapıya yönelik siber saldırılar ve bireylerin herhangi bir şekilde fiziksel olarak zarar görmesi şeklinde sıralamak mümkündür. Genel olarak bireyi tanımlayan verilerin doğruluğunun, güvenliğinin ve güvenilirliğinin sağlanması hem bireysel hem de kurumsal bağlamda son derece hassasiyet taşıyan bir konudur. Günümüz kurumlarındaki iş akışlarının temel yapı taşlarından birinin veri olduğunu söylemek mümkündür. Bu çerçevede verilerin güvenilirliğinin ve doğruluğunun sağlanması iş süreçlerinin etkin yönetimi açısından da önem taşımaktadır. Konuyla ilgili olarak ulusal ve uluslararası standartlar da yayınlanmakta, birçok ülkede kanunlar hazırlanmakta ve kurumlarda da verinin üretimi, kullanımı, paylaşılması, güvenliğinin sağlanması ve korunması için uygulamalar geliştirilmektedir. Kurumsal verilerin yönetimi kapsamında ele alabileceğimiz bu uygulamalarla birlikte verinin kurumlarda stratejik bir varlık olarak değerlendirildiği görülmektedir. Bu durum, kurum ve kuruluşların iş ve iş süreçlerinde kullandıkları kişisel verilerin korunması ve yönetimine dönük girişimlerde bulunmalarını gerektirmiştir. Aynı zamanda, kişisel verilerin korunması, kullanıcı merkezli ve belirli bir güvenilirlik düzeyine sahip hizmetlerin sunulmasında ve kurumsal itibarın sağlanmasında da önem taşımaktadır. Bu bilgilerden yola çıkarak çalışmanın bu bölümünde bilgi güvenliğinin kapsamı ve gelişim evreleri, bilgi güvenliğinin bileşenleri, bilgi güvenliğinin standartları,

bilgi güvenliğine yönelik kanunlar ve düzenlemeler ve üniversite kütüphanelerinde bilgi güvenliği konuları ele alınmaktadır.

2.1. BİLGİ GÜVENLİĞİ, KAPSAMI VE GELİŞİM EVRELERİ

Bilgi güvenliği, "bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci" olarak tanımlanmaktadır (Vural, 2007, s.40). Burada yapılan tanımda, iletişim süreci içerisindeki verinin güvenliğinin sağlanmasında herhangi bir değişiklik yapılmaması gerektiği üzerinde durularak bilgi güvenliğinin bütünlüğü vurgulanmıştır.

Caballoro ise (2014, s.2), bilgi güvenliğini hem teknik hem de stratejik güvenlik kontrollerine dayanan bir iş problemi olarak tanımlamıştır. Caballoro'nun (2014, s.2) yapmış olduğu bu tanımda, bilgi güvenliğinin tek bir güvenlik kontrolüne dayanmadığı anlaşılmakta ve bilgi güvenliğinin bir iş problemi olduğu görülmektedir.

Öztemiz ve Yılmaz'ın aktarımı ile (2013, s.89) bilgi güvenliği, kurumsal bilgi kaynaklarını doğa (sel, deprem, yangın vb.) ya da insan kaynaklı tehditlere karşı korumak anlamına gelmektedir (Qureshi, 2011, s.3). Yapılan bu tanımda ise, bilgi güvenliğini tehdit eden unsurların neler olduğu anlaşılmaktadır. Yıkım, kullanım ve yetkisiz erişimden bilgi ve bilgi sistemlerinin korunması anlamına gelen bilgi güvenliği, aynı zamanda bir kurumda sosyal mühendislik saldırıları, hırsızlık veya doğal afetlere karşı bilgi varlıklarının korunması gibi fiziksel güvenlik ölçümlerini içermektedir (Singh, Vaish ve Keserwani, 2014).

Surwade ve Patil'e göre bilgi güvenliği (2019, s.460), bilgileri güvende tutmak için uygulanan teknolojilerin, standartların, politikaların ve yönetim uygulamalarının toplamı şeklinde tanımlanmıştır. Surwade ve Patil'in bilgi güvenliği üzerine yapmış olduğu diğer bir tanım ise (2019, s.462), fiziksel ve dijital bilgileri yetkisiz erişime ve tahribe karşı koruma uygulaması olarak ifade edilmesidir.

Ulusal Standartlar ve Teknoloji Enstitüsü'nün (National Institute of Standards and Technology - NIST) tanımına göre bilgi güvenliği, bilgi sistemlerinin gizliliğinin,

bütünlüğünün ve kullanılabilirliğinin oluşturulabilmesi için yetkisiz erişim, kullanım, ifşa, bozulma, değişiklik veya imhadan korunması şeklinde tanımlanmıştır ("NIST", t.y.). Bilgi güvenliği ile ilgili bir diğer tanımda ise, kavramın üç temel özelliğine vurgu yapılmıştır. Buna göre bilgi güvenliği bilginin özelliği olan gizlilik, bütünlük ve kullanılabilirliğinin korunması şeklinde ifade edilmiştir (Muharremoğlu, 2013, s.7; Doğantimur, 2009, s.7; Başak, 2018).

Bilgi güvenliğini, "organizasyon içindeki bilgiyi korumaya çalışmak için teknik ve fiziksel kontroller uygulamaktan daha fazla" işlem ve süreci kapsadığını dile getiren Waddell ise (2013, s.27), teknik ve fiziksel kontrollerin yanında insan işgücü tarafından ortaya çıkan güvenlik açıklarının da hesaba katılması gerektiğini vurgulamıştır.

Khoo, Harris ve Hartman'a göre (2010, s.49) bilgi güvenliği, gizlilik, bütünlük ve kullanılabilirliğin korumasıdır ve politika, teknoloji, eğitim, farkındalık uygulamaları yoluyla bilgiyi kullanan, depolayan, işleyen ve ileten yazılım ve donanım bilgi güvenliğinin önemli unsurlarıdır.

Amerika Birleşik Devletleri Federal Bilgi Güvenliği Yönetimi Kanunu'nda (Federal Information Security Management Act) (United States Congress, 2002, s. 49) yer alan bilgi güvenliği tanımına çalışmasında yer veren Güngör ise (2015, s.5), bilgi güvenliğini "en temel manada bilginin korunduğu bilgi sistemlerinin ve sistemin içerdiği bilginin yetkisiz erişimine, kullanımına, ifşa edilmesine, değiştirilmesine, incelenmesine, hasar verilmesine veya yok edilmesine karşı korunması ve buna ilişkin tedbirlerin bütünü" olarak ifade etmiştir.

Bilgi güvenliği genel olarak, kurumun içinde ve kurum dışında bilgiyi tutmak ve korumak amacıyla çeşitli güvenlik önlemlerinin geliştirilmesi (teknik, organizasyonel, insan odaklı ve yasal) ve uygulanması ile ilgilenen çok disiplinli bir çalışma alanı ve mesleki aktivitedir ve sonuç olarak, bilgi güvenliği bilginin yaratıldığı, işlendiği, saklandığı, iletildiği ve imha edildiği tehdit unsuru içermeyen bilgi sistemleridir (Cherdentseva ve Hilton, 2013a, s.5; Cherdentseva ve Hilton, 2013b, s.546).

Yapılan tanımlar ışığında bilgi güvenliği, bir kurum, kuruluş ya da organizasyonda hem fiziki hem de elektronik ortamda yer alan bilgi ve bilgi varlıklarının gizliliğinin,

bütünlüğünün ve kullanılabilirliğinin doğru teknolojiyle, doğru zamanda ve doğru amaçla, doğru bir şekilde kullanılmasını sağlamak amacıyla her türlü tehdit, saldırı, yıkım, kesim, hasar, yetkisiz erişim, kullanım, silme, yok etme, kullanma, ifşa etme, değişime karşı korunmasını sağlamak amacıyla uygulanan politika, uygulama, eğitim ve alınabilecek tedbir ve önlemlerin tümü şeklinde nitelendirilebilir.

Bilgi güvenliği, kesintisiz, nitelikli ve güvenli bir hizmet sunumunun sağlanması amacıyla bilgi sisteminin faaliyetlerini yerine getirmektir. (Güngör, 2015, s.13). Bununla birlikte, kurumsal imaj ve güvenilirliğin sağlanması, kurumlarda işin sürekli olması, felaket olaylarında kaybın en aza indirilmesi, kurumların bilgi kaynaklarının her koşulda gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunması bilgi güvenliğinin temel amaç ve öncelikleri arasında yer almaktadır (Çalıkuşu, Karamehmet ve Denizci, t.y., s.2; Güngör, 2015, s. 13). Bilgi güvenliği kurumsal boyutta ise kurumların bilgi varlıklarının zafiyetlerinin tespit edilmesi ve istenmeyen saldırı ve tehlikelerden korunmasını sağlamak amacıyla güvenlik analizlerinin ve güvenlik testlerinin yapılarak gerekli tedbir ve önlemlerinin alınması olarak tanımlanabilmektedir (Vural ve Sağıroğlu, 2008, s.509; Ülker, Canbay ve Sağıroğlu, 2017, s.30).

Solms yapmış olduğu bir çalışmada (2000, s.615) bilgi güvenliğinin gelişmesinde üç dönemin etkili olduğunu dile getirmektedir. Bu dönemlerden ilki, seksenlerin başına kadar esas olarak bilgi güvenliği için çok teknik bir yaklaşım ile karakterize edilen teknik dalgadır. Daha çok ana bilgisayar tabanlı olan bu dalga, erişim kontrol listeleri, kullanıcı kimlikleri ve şifreler gibi ana bilgisayar işletim sistemlerinin yerleşik tesislerini kullanarak çözülebilecek bir olgu olarak algılanmıştır. Ayrıca bu dönemde, bilgi güvenliği politikaları, kullanıcıların bilgi güvenliği bilinci vb. gibi konuların çok yaygın olmadığı ifade edilmiştir. Yaklaşık 80'lerin başından 90'lı yılların başına kadar görülen ikinci dönem ise yönetim dalgası olarak nitelendirilmiştir. Bu dönemde dağıtık bilgi işleme, internet teknolojilerinin gelişimiyle birlikte kurum ve kuruluşlar bilgi güvenliği konusunda girişimde bulunmaya yönelmiştir. Tüm bu gelişmelerle beraber, yönetim kademelerinin de devreye girmesiyle kurumlarda bilgi güvenliği profili artış göstermiş, bilgi güvenliği politikaları kurumlar için öne çıkmaya başlamıştır. Bu dalganın sonucunda teknik dalgaya paralel olarak, bilgi güvenliği uygulayıcıları istediklerini elde ederek yönetimin farkındalığının artmasını sağlamıştır. Bununla birlikte, kurumların bilgi

güvenliğini sağlamak için üst yönetim bu konuda yaptırımlar yapmaya başlamıştır. Daha sonra, kurum ve kuruluşlara bilgi güvenliği yöneticileri atanarak, politikalar, prosedürler hazırlanarak üst yönetime organize yapılar aracılığıyla rapor edilmeye başlanmıştır. Şirketler, bilgi güvenliğinde ne kadar iyi olduklarını, diğer şirketlerle nasıl kıyaslandıklarını, bilgi güvenliği konusunda çevrimiçi olarak nasıl daha fazla yardım alabileceklerini ve aynı zamanda bilgi güvenliğini en büyük sorununun insan olduğunu öğrenmek istemişlerdir. Bu nedenle, bilgi güvenliği birinci ve ikinci döneme paralel olarak kurumsal bir çaba olarak üçüncü dalgada gelişim göstermiştir. Doksanlı yılların sonlarından itibaren başlayan üçüncü dalga, bilgi güvenliği yönetimi, uluslararası bilgi güvenliği sertifikası, kurum kültürü olarak bilgi güvenliğinin geliştirilmesi ve dinamik ve sürekli bilgi güvenliği ölçümü için en iyi uygulamalar ve uygulama gibi kodları gibi özelliklerle karakterize olmuştur (Solms, 2000, s. 615-616).

Yaşanan gelişmelere bakıldığında aslında her dönemin bir sonraki dönemin oluşumunda etkili olduğunu söyleyebiliriz. Bunun yanı sıra, dönemlerin genel olarak bir ihtiyaçtan beslendiğini ya da bir ihtiyacın fark edilmesiyle şekillendiğini söylemek mümkündür. Tüm bu gelişmelerin ardından Solms bir diğer çalışmasında (2006, s. 168) bilgi güvenliği gelişiminin dördüncü dönemini, bilgi güvenliği yönetimi kavramının olgunlaşması ve bilgi güvenliğinin iyi bir kurumsal yönetişimin[3] ayrılmaz bir parçası olarak açık bir şekilde kurumsal uygulamalara dâhil edilme süreci olarak nitelendirmiştir. Bu bağlamda, dördüncü dönemin iki binli yıllardan itibaren gelişim gösterdiği anlaşılmaktadır. Bununla birlikte, yapılan bu çalışmanın sonucunda bilgi güvenliğinin teknik, yönetimsel, kurumsal ve yönetişimsel[4] olmak üzere toplamda dört evrede geliştiği görülmektedir.

Kurum ve kuruluşlarda bilgi güvenliği politikaları ve standartlarının bulunmayışı, güvenlik konusunda bazı eksikliklere sebep olabilmektedir. Bu nedenle kurumlarda bilgi sistemlerinin güvenilirliği, Bilgi Güvenliği Yönetim Sistemleri'nin kurumlarda uygulanmasıyla olanaklı hale gelmektedir (Vural ve Sağıroğlu, 2008, s. 509). Bilgi Güvenliği Yönetim Sistemleri, bilginin üç ana unsurunu sağlamak üzere, sistemli, ilkeleri belirlenmiş, planlı, sürdürülebilir, yönetilebilir, dokümante edilmiş, yönetimce kabul

[3]Kurumsal yönetişim, kuruluşların büyüklük ve biçimden bağımsız olarak yönlendirildiği ve yönetildiği politikalar kümesinden ve iç kontrollerden oluşmaktadır (Solms, 2006, s.166).

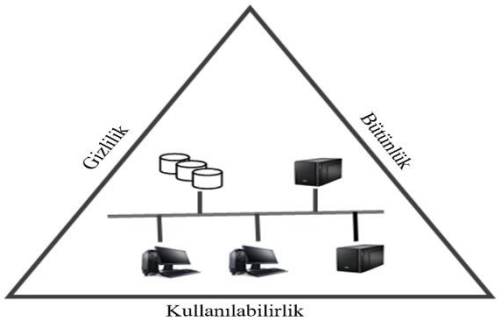
[4] Bilgi güvenliği yönetişimi, bilgi güvenliği yönetiminden daha fazla alanı kapsamaktadır. Bununla birlikte, bilgi güvenliği yönetişimi, bir kurumun bilgi güvenliği ile ilgili olarak üst yönetim ve yönetim kurullarının önemli olduğunu göstermektedir (Solms, 2006, s. 167).

edilmiş ve desteklenmiş, uluslararası güvenlik standartlarının öncül olarak alındığı etkinlikler ve faaliyetler bütünü olarak tanımlanmaktadır (Çek, 2017, s.16). Emiral (2014), "pek çok kullanıcı bilgi ve bilgi kaynaklarının korunmasının önemi konusunda ya çok az anlayışa sahiptir ya da hiçbir anlayışa sahip değillerdir" diyerek bilgi güvenliği yönetim sisteminin kurum ve kuruluşlardaki önemine dikkat çekmiştir. Bu bağlamda, kurum ve kuruluşlarda kullanıcıların oluşturabilecekleri tehdit ve risklere karşı bir bilgi güvenliği yönetim sistemi kurulması zorunlu hale gelmiştir. Kurulan bu sistem kuruluşlara çeşitli yönlerden fayda sağlayabilmektedir. Bilgi güvenliği yönetim sistemi kurum ve kuruluşlardaki riskler, tehditler ve zafiyetler önceden tanımlanarak gerekli tedbirlerin alınmasını, bilgilerin güvenliğinin ve gizliliğinin sağlanmasını ve afet planları oluşturularak iş devamlılığının oluşturulmasına imkân tanımaktadır (Demirok, 2016, s.32). Kurumsal anlamda bilgi güvenliğinin oluşturulması, kurumun kâr etmesi, rekabet ve sürdürülebilir büyüme ve gelişme için sahip olduğu veya sahip olması gereken pazar, ürün, teknoloji ve kuruma ait bilgilerin geniş çaplı tehditlerden ve tehlikelerden korunması anlamına gelmektedir (Seferoğlu, Durak, Yılmaz ve Yılmaz, 2018, s.33; Yılmaz, 2014, s.46). Bunun yanı sıra, bilgi güvenliği, özel sektör başta olmak üzere kamu sektöründe mal varlıklarının korunması ve rekabet üstünlüğünün sağlanması amacıyla da oldukça önem arz etmektedir. Bir kurumun mal varlığı, mali bilgilerden oluşabileceği gibi, kuruluşların donanım ve yazılımlarında saklanan bütün bilgi birikiminden de oluşabilmektedir.

2.2. BİLGİ GÜVENLİĞİNİN BİLEŞENLERİ

Bilginin güvenliğinin sağlandığı ortamlar, yalnızca yetkilendirilmiş kişilerin hassas bilgilere erişebilmesini, bilgilerin doğru bir şekilde işlenmesini ve gerektiğinde kullanılmasını kapsamaktadır (Killmeyer, 2000, s.11). Bu bağlamda bilginin güvenliğinin üç temel özellik olan gizlilik, bütünlük ve kullanılabilirlik özelliğinin korunması ile ilişkilendirildiği anlaşılmaktadır. Bilginin bu özelliklerinin elektronik bir ortamda ve çoğunlukla otomatize edilmiş sistemlerde tutulması geniş bir yelpazede çeşitlilik gösteren güvenlik endişelerini ortaya çıkarabilmektedir. (National Training Standard for Information Systems Security - NSTISSI, 1994). Bununla birlikte, günümüz ihtiyaç ve gereksinimleri bu üç temel özelliği tek başına ilişki kuramamıştır. Çünkü bunlar kapsam ve çerçeve dâhilinde sınırlı olmakla beraber, bilgi teknolojileri

endüstrisinin sürekli değişen ortamını içermektedir. Bilginin bu üç özelliğine yönelik tehditler, kazara veya kasıtlı hasar, yıkım, hırsızlık, istenmeyen veya yetkisiz değişiklik, insan hatası veya diğer tehditlerden kaynaklanan diğer yanlışlıklar da dâhil olmak üzere geniş bir potansiyel tehlike koleksiyonundan oluşmaktadır. Sürekli gelişen tehditlerin, bilginin özelliklerinin güvenliğinin sağlanmasına yönelik bir modelin geliştirilmesini zorunlu kılmıştır (Aydoğmuş, 2010, s.3).



Şekil 1. Gizlilik-Bütünlük-Kullanılabilirlik üçlüsü (Grama, 2011, s.5)

Bilgi güvenliği, bilgiyi koruma ve çalışma uygulamasıdır. Bu bağlamda, bilgi güvenliğinin esas amacı doğru bireyin kısa zamanda doğruluğundan ve kullanılabilirliğinden emin olunan bilgiye erişimini sağlamaktır (Yıldız, 2017, s.23). Diğer bir deyişle, bilgi güvenliğinin üç temel unsuru yeterli düzeyde sağlandığında, bilgi güvenliğinin sağlanabilmesi mümkün hale gelecektir (Yılmaz, 2014, s.46). Bu bağlamda karşımıza bilgi güvenliğinin üç ana unsuru olan gizlilik, bütünlük ve kullanılabilirlik çıkmaktadır (Şekil 1). Profesyoneller genellikle bu üçlü "CIA üçlüsü" bazen de "AIC üçlüsü" olarak nitelendirmektedir. Bir üçlü, tek bir birim olarak kabul edilen üç şeyden oluşan bir gruptur (Grama, 2011, s.5; Surwade ve Patil, 2019, s.461). Arnason ve Willet, (2007, s.2) bu üçlüyü "bilgi güvenliğinin köşeleri" olarak tanımlamaktadır. Bu ögeler, bilgi sisteminin erişilebilir bir vaziyette gizliliğine ve bütünlüğüne hasar gelmemiş bir faaliyet ortamında işlenmesini ve bilgi varlıklarının güvenilirliğini temin etmektedir (Güngör, 2015, s.8). Tüm güvenlik programlarının geliştirdiği temel unsurlar olarak kabul gören CIA (Confidentiality-Gizlilik, Integrity-Bütünlük, Availability-Kullanılabilirlik), bilgiyi koruma fikrinde birbirine bağlıdır. Bilginin, kurumun diğer varlıkları gibi, koruma gerektiren bir varlık olduğu fikri ise, bu unsurları anlamak için temel oluşturmaktadır (Wylder, 2004, s.4). Diğer bir deyişle, bir kurumun varlığı olarak nitelendirilen bilginin

korunması, verinin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanmasına zemin hazırlayacaktır. Hem endüstride hem de hükümette bilgisayar güvenliği için standart haline gelen CIA, her zaman önemli bulunmuştur. Ancak, genellikle sürekli değişen çevreyi ele almada yetersiz görülmektedir (Whitman ve Mattord, 2016, s. 11). Bilgi güvenliğinin kritik bilgi özelliğini oluşturan CIA, otomatik bir ortamda güvenlik kaygılarının tümünü temsil etmektedir. Bununla birlikte, bilgi paylaşımı konusunda felsefi bakış açısına bakılmaksızın herhangi bir kuruluş için geçerli olmaktadırlar (McCumber, 2004, s.102). Bilgi güvenliği ve güvenilirliği genel olarak, bilginin gizliliği (confidentiality) ve bütünlüğü (integrity), korunması (protection), etkin biçimde kullanılabilirliği (availability), içerdiği bilginin kayıtlı formunu, onaylarını, kanıt niteliği (authentication) ve inkâr edilememe (non-repudiation) konularını kapsamaktadır (Külcü, 2017, s.21; Külcü, 2018, s.37). 2002 yılında Donn Parker klasik CIA üçlüsü için altı atomik bilgi unsuru olarak adlandırdığı alternatif bir model önermiştir. Bu unsurlar, gizlilik, mülkiyet, bütünlük, özgünlük, kullanılabilirlik ve faydadır (Singh, Vaish ve Keserwani, 2014, s.1074).

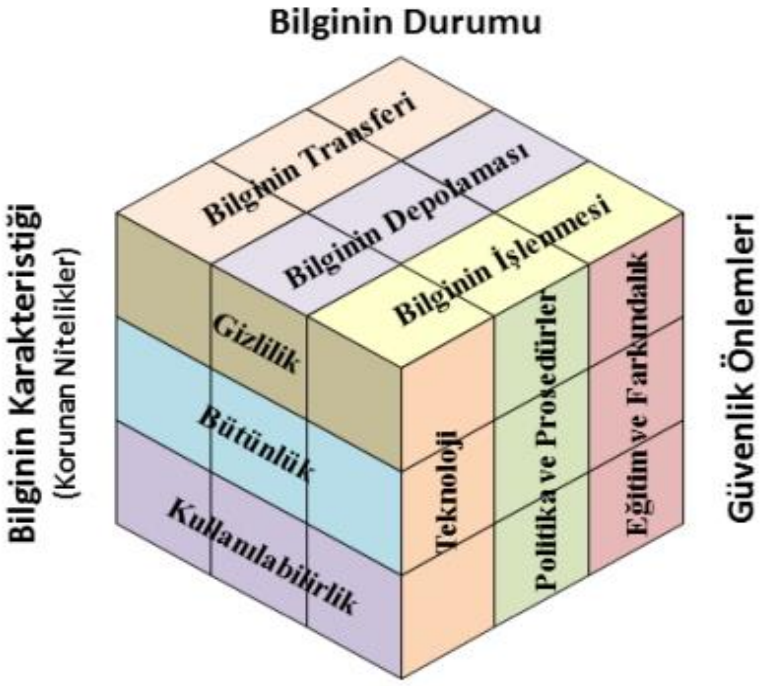
- Gizlilik (Confidentiality): Bilgi veya kaynakların gizlenmesi olarak adlandırılan gizlilik, bilgilerin yalnızca yetkili bireyler tarafından erişilmesini sağlamak anlamına gelmektedir. Bilginin gizli tutulması gereksinimi hükümet ve endüstri gibi hassas alanlarda bilgisayarların kullanılmasından kaynaklanmaktadır. Bir kuruluşun, bilgilerin gizliliğini tehdit eden kötü niyetli eylemlere karşı korunması gerekir (Singh, Vaish ve Keserwani, 2014, s.1074).

- Bütünlük (Integrity): Genellikle yetkisiz değişimi önleme olarak ifade edilen bütünlük, verilerin veya kaynakların güvenilirliğini ifade etmektedir. Aynı zamanda, bilginin bozulmadan ve değişmeden kalmasını sağlamak olarak da tanımlanmaktadır. Verilerin kaynağını içeren bütünlük; veri bütünlüğünü, diğer bir deyişle, bilginin içeriğini ve kaynak bütünlüğünü içermektedir (Singh, Vaish ve Keserwani, 2014, s.1074).

- Kullanılabilirlik (Availability): Bilgi ve kaynakların yetkili kullanıcılar tarafından gerektiği gibi erişilebileceğinin güvencesidir. Kullanılabilirlik, güvenlik

eksikliğinden kaynaklanan hizmetlerin reddedilmesi (örneğin, veri, ekipman veya bilgisayar virüslerinin imha edilmesi) ve doğal afetler (örneğin, fırtınalar, seller veya yangınlar) nedeniyle bilgi kaynaklarından doğan hizmet kaybı olmak üzere iki tür sorunla ilişkilidir (Killmeyer, 2000, s.2).

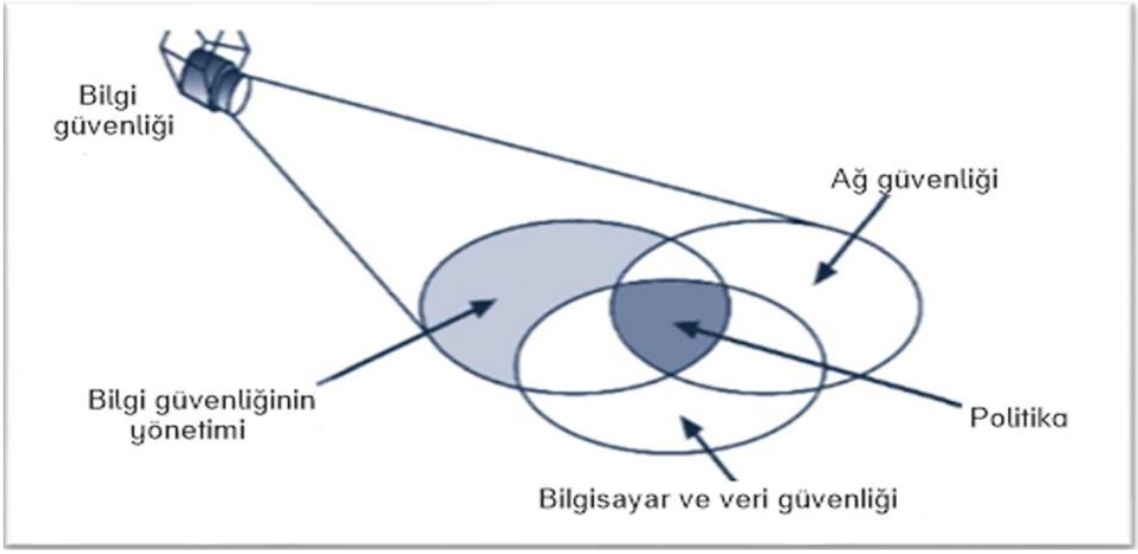
Literatürde CIA üçlüsünden farklı olarak bilgi güvenliği ile ilgili modeller yer almaktadır. Bu modellerin en kapsamlı ve güncel olanı ise, McCumber tarafından 1991 yılında geliştirilen bilgi güvenliği modelidir (Henkoğlu, 2015a, s.40-42). Model, genellikle Rubik küpüne benzemekte ve 3x3x3 hücrelerden oluşmaktadır (Şekil 2). Aynı zamanda model, bilgisayar ve bilgi güvenliğinde yaygın olarak kullanılan mimari yaklaşımın grafiksel bir temsili olarak nitelendirilmektedir (Whitman ve Mattord, 2016, s.18). CIA üçgeninin geleneksel üç unsurunu içeren küp, üç boyutta genişletilerek oluşturulmuştur. Diğer bir deyişle, CIA'ya her biri üç katmana sahip iki ek boyut eklenmiştir (Easttom ve Butter, 2019, s.0944).



Şekil 2. McCumber Bilgi Güvenliği Modeli (McCumber, 2004, s.100; Henkoğlu, 2015a, s.32)

Çok yönlü bir model özelliğine sahip olan küp, bilgi güvenliği çerçevesinde alınacak önlemlerin (teknoloji, politikalar, eğitim/farkındalık), bilginin durumuna (bilginin

transferi, depolanması, işlenmesi), bağlı olarak karakteristik özelliklerinin (gizlilik, bütünlük, kullanılabilirlik) nasıl korunabileceğini en iyi açıklayan ve tek bir çatı altında birleştiren modellerden biridir (Henkoğlu, 2015a, s.40). Kişisel verilerin korunması açısından modele bakıldığında, kişisel verilerin özünde yer alan bireyin kişisel hak ve özgürlüğünün korunmasını da kapsayan ve bu konudaki hukuksal düzenleme ve politikaların amaçlarını bilgi güvenliği şemsiyesi altında birleştirerek dikkate alan bir model olarak nitelendirilmiştir (Henkoğlu, 2015a, s. 40).



Şekil 3. Bilgi güvenliğinin bileşenleri
(Whitman ve Mattord, 2016, s.10; Aydoğmuş, 2010, s.2; Tatar, 2015, s.6)

Şekil 3'e bakıldığında bilgi güvenliği; ağ güvenliği, veri güvenliği ve bilgi güvenliği yönetiminin geniş bir alanını kapsamaktadır (Whitman ve Mattord, 2016, s.10). Şekilde göze çarpan nokta ise, bilgi güvenliği politikalarının üç temel bileşenin kesişim noktasında yer almasıdır. Politikaların bu noktaa yer almasının önemi ise, politikaların kurumların bilgi teknolojilerinin koruma yollarını tanımlayan yazılı bir belge niteliği olarak görülmesidir (Tatar, 2015, s.6). Başarılı bir kurumun, işlemlerini korumak için aşağıda belirtilen çoklu güvenlik katmanlarına sahip olması gerekmektedir (Whitman ve Mattord, 2009, s.8):

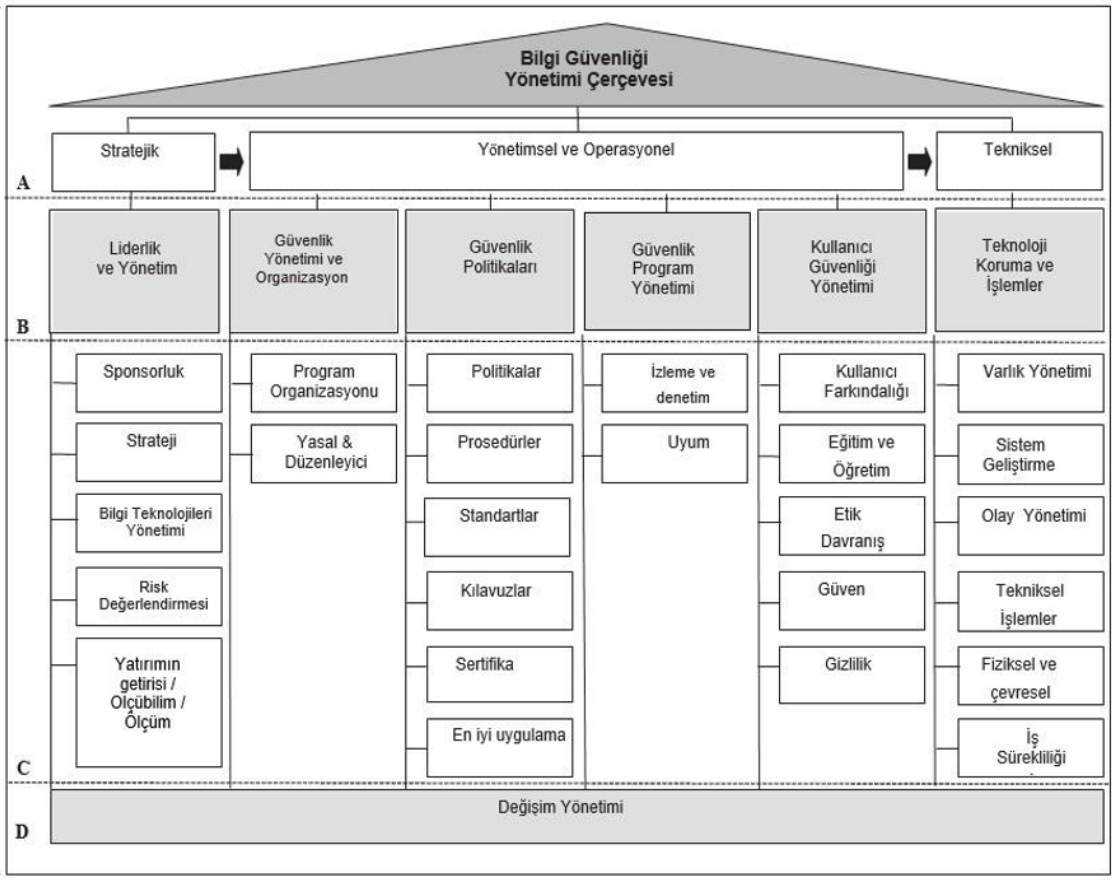
- Fiziksel eşyaların, nesnelerin veya alanların yetkisiz erişime veya başkalarının yanlış kullanmasına karşı korunması için fiziksel güvenlik önlemleri alınmalıdır.
- Organizasyona ve faaliyetlerine erişim yetkisi olan kişi veya bireyi korumak için personel güvenliği oluşturulmalıdır.

- Belirli operasyonun veya faaliyet dizilerinin ayrıntılarını korumak ve sağlamak için operasyon güvenliği kurulmalıdır.
- İletişim ortamını, teknolojiyi ve içeriğini korumak için iletişim güvenliği sağlanmalıdır.
- Ağ bileşenlerini, bağlantılarını ve içeriğini korumak için ağ güvenliği kurgulanmalıdır.
- Bilgi varlıklarını korumak için bilgi güvenliği çalışmaları başlatılmalıdır.

2.3. BİLGİ GÜVENLİĞİ YÖNETİMİ ÇERÇEVESİ

Bilgi güvenliği davranışı, evlerimize uyguladığımız güvenlik yaklaşımı gösterilerek açıklanabilmektedir. Örneğin, bir ev sahibi tüm pencereler için güvenlik önlemlerini almış olabilir ancak evden ayrıldıktan sonra ön kapı açık olabilir. Bu nedenle, güvenlik önlemleri ev sahibinin davranışlarından dolayı etkisiz hale gelmektedir. Aynı şekilde, kuruluşlar virüsten koruma programları, güvenlik duvarları ve şifreler gibi güvenlik denetimlerini uygulamaktadır. Kullanıcılar güvenlik duvarını atlayarak çevirmeli ağ üzerinden internete bağlanır ve şifrelerini paylaşırlarsa bu denetimler işlevsiz kalabilmektedir.

Bir kurumda güvenlik gerekliliklerine uyumu sağlamak için çalışanların davranışlarının yönlendirilmesi ve izlenmesi gerekmektedir. Bu nedenle, yönetimin, çalışanlardan kabul edilebilir bir bilgi güvenliği kültürüne uymalarını ve bilgi güvenliği farkındalığına yönelik davranış sergilemelerini beklemeden önce, bileşen olarak da adlandırılan belirli güvenlik kontrollerini uygulamaları gerekmektedir.



Şekil 4. Bilgi Güvenliği Yönetimi Çerçevesi (Veiga ve Eloff, 2007, s.3)

Bilgi güvenliği bileşenleri, bilgi güvenliği politikası, risk değerlendirmeleri, teknik kontroller ve bilgi güvenliği farkındalığı gibi bilgi güvenliğinin uygulanmasını ve korunmasını sağlayan ilkeler olarak tanımlanabilmektedir. Bu bileşenler, bileşenler arasındaki ilişkinin gösterildiği bir bilgi güvenliği yönetişimi çerçevesinde ele alınabilir. Bilgi Güvenliği Yönetişim Çerçevesi, kuruluşlara bilgi güvenliği için bütünsel bir planın gerekliliklerinin anlaşılmasını sağlamaktadır (Şekil 4). Aynı zamanda bilgi güvenliği yönetimi çerçevesi, uygun bir düzeyde bir bilgi güvenliği kültürü oluşturmak ve bilgi varlıklarına getirilen riskleri en aza indirmek için teknik, prosedürel ve insan odaklı bileşenleri birleştirmektedir (Veiga ve Eloff, 2007, s.363).

Bilgi güvenliği yönetimi genel olarak, riskleri azaltma uygulamasıdır (Veiga ve Eloff, 2007, s.362). Bilgi güvenliği yönetim çerçevesi, bilgi güvenliğinin kapsamlı ve tek bir referans noktasından yönetilebilmesi için tekniksel, prosedürel ve insan davranışsal bileşenlerini dikkate almaktadır. Söz konusu çerçeve, aşağıda yer alan dört farklı yaklaşım değerlendirilerek oluşturulmuştur:

- ISO 17799:2005 Bilgi Teknolojileri Standardı,
- PROTECT Yaklaşımı,
- Yetenek Olgunluk Modeli,
- Bilgi Güvenliği Mimarisi,

Önerilen bilgi güvenliği yönetişim çerçevesi, web taramasının kötüye kullanılması, hırsızlığın tespiti veya verilerin bozulması, gibi kuruluşlar tarafından tanımlanan riskleri gidermek için, kılavuzlar geliştirerek ve kontroller uygulayarak bir kurumda bilgi güvenliğinin yönetilmesi için başlangıç noktası sayılabilir. Bu yeni çerçeve bilgi güvenliğinin tüm yönleriyle çalışan davranışlarını yönetmek ve kabul edilebilir bir düzeyde bir bilgi güvenliği kültürü oluşturmak için kullanılabilir. Bilgi güvenliği yönetim çerçevesi, A, B, C ve D olmak üzere dört seviyeye ayrılmıştır. Seviye A, stratejik, yönetimsel ve operasyonel, tekniksel bileşenlerden oluşmaktadır. Şeklin sol tarafında gösterilen stratejik bileşenler, şeklin orta kısmında gösterilen yönetimsel ve operasyonel uygulama bileşenlerine yön vermektedir. Tekniksel koruma bileşenleri ise Şekil 2'nin sağ tarafında gösterilmiştir. Seviye B, üç seviye A kategorisine göre gruplandırılmış altı ana kategoriden oluşmuştur (Veiga ve Eloff, 2007, s.3):

- Stratejik
  - Liderlik ve Yönetim
- Yönetimsel ve Operasyonel
  - Yönetimi ve organizasyon
  - Güvenlik politikaları
  - Güvenlik program yönetimi
  - Kullanıcı güvenliği yönetimi
- Tekniksel
  - Teknoloji koruma ve işlemler

C seviyesi, altı ana kategorinin (seviye B) her biri altında kategorize edilen kapsamlı bir bilgi güvenliği bileşenlerinden oluşmaktadır. Altı ana kategori, şeklin alt kısmında tanımlanan değişiklikten etkilenmektedir. Bilgi güvenliği bileşenlerini kurumların uygulaması kurumların süreçlerini değiştirecek ve insanların çalışma şeklini etkileyecektir. Verton'a göre buradaki önemli husus, "kuruluşların değişmediği ancak

insanların kurumları değiştirdiğidir" (Verton, 2000). Kurumdaki bilgi güvenliği değişikliklerinin, çalışanlardan bu değişiklikleri çalışmalarına başarıyla dâhil edebilecek şekilde kabul etmeleri ve değişiklikleri yönetmeleri çalışanlarından beklenmektedir. "Değişim" olarak belirtilen bileşenin, bilgi güvenliği bileşenlerinden herhangi birinin uygulanmasında göz önünde bulundurulması gerekmektedir.

2.4. BİLGİ GÜVENLİĞİ STANDARTLARI

Bilgi ve bilişim teknolojilerinin yoğun bir şekilde kullanılması beraberinde bir takım risk unsurlarını taşımaktadır. Kurum ve kuruluşların sistemlerine taşınan bu riskler, kurumları bir takım tedbir ve önlemler almaya doğru itelemiştir. Bu önlemlerin başında ise, ulusal ve uluslararası alanda ortak olarak kabul edilen ve yaygın olarak kullanılan standartlar gelmektedir. Söz konusu bilgi güvenliği standartları, kurum ve kuruluşlarda bulunan bilgi varlıklarının etkin, verimli ve güvenilir bir şekilde yönetilmesi, sistemli bir biçimde korunması ve bilgi güvenliği yönetim sistemlerinin kurulması için oldukça önemli role sahiptir. Üniversite kütüphanelerinde bilgi güvenliği standartlarının oluşturulması amacını taşıyan bu araştırmada, bilgi güvenliği standartları ve içeriğiyle bilgi güvenliğinin sağlanmasına yönelik önemli katkılar sunan standartlar incelenmiştir.

2.4.1. Uluslararası Standartlar Örgütü'nün (International Standards Organization –ISO) Standartları

- ISO/IEC (International Electrotechnical Commission) 27000 Bilgi Teknolojileri – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Genel Bakış ve Sözlük 1/2/3/4/5: 2009 yılında birincisi yayınlanan standart, bilgi güvenliği yönetim sistemini, bilgi güvenliği yönetim sisteminin yapısını ve ailesini ve ilişkili terimleri tanımlamaktadır (ISO/IEC 27000:2009, 2009). Bu sebeple bu standart daha çok bir sözlük görevini üstlenmektedir. 2009 yılındaki standardın iptal edilmesinin ardından 2012 yılında standardın ikinci basımı yayınlanmıştır. Yine 2012 yılındaki standardın gözden geçirilmesiyle birlikte 2014 yılında tekrar bir standart yayınlanmıştır. Daha sonra bu standart iptal edilerek 2016 yılında standardın dördüncü sürümü yayınlanmıştır.

Beşinci kez yenilenmesinin ardından yayımlanan yeni standart, bilgi güvenliği yönetim sisteminin tanımına ve yaygın olarak kullanılan Bilgi Güvenliği Yönetim Sistemi ailesinin standartlarına yer vermektedir. Bu standart ticari işletmeler, devlet kurumları ve kâr amacı gütmeyen kuruluşlar için geçerlidir (ISO/IEC 27000:2018, 2018, s.1).

- ISO/IEC 27001 Bilgi Teknolojileri – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereklilikler 1/2/3: İlk basımı 2005 yılında yayınlanan Bilgi Güvenliği Yönetim Standardı, bir bilgi güvenliği yönetim sisteminin yapılandırılması, sürdürülmesi ve sürekli iyileştirilmesi için gereklilikler sunmaktadır. Bununla birlikte standardın içeriğinde organizasyonların gereksinimlerine göre bilgi güvenliği risklerinin değerlendirilmesi ve tedavisi için gereklilikler de bulunmaktadır. Sadece sistem güvenliğinden değil bilgi güvenliğinden de bahseden bu standart, çeşitli büyüklüklerdeki kurumlara uygulanabilir bir biçimde hazırlanmıştır (Doğantimur, 2009, s.12). 2013 yılında yayımlanan ikinci basımı şu an inceleme altında olup, düzeltmeleri ise ISO/IEC 27001:2013/Cor:2014 ve ISO/IEC 27001:2013/Cor 2: 2015 başlığı altında yapılmaktadır (ISO/IEC 27001:2013, 2013).

- ISO/IEC 27002 Bilgi Teknolojileri – Güvenlik Teknikleri – Bilgi Güvenliği İçin Uygulama Standardı 1/2/3/4: Bu standardın gelişim evreleri şu şekildedir: İlk basımı 2000 yılında yayınlanan standardın geri çekilmesinin ardından beş yıl sonra ikinci basımı yayınlanmıştır. Bu basımda birinci basımdan farklı olarak güvenlik teknikleri ele alınmıştır. Bununla birlikte, bu standart kurumsal güvenlik standartlarını ve etkili güvenlik yönetimi uygulamalarını geliştirmek ve organizasyonlar arası faaliyete güven oluşturmak için ortak bir temel ve kılavuz olarak tasarlanmıştır (ISO, t.y.). Bu standardın üzerindeki değişiklik 2007 yılında, ISO/IEC 17799:2005/Cor 1:2007 başlığıyla yayınlanmıştır. Daha sonra bu standart referans numarasını 17799'dan 27002'ye değiştirmiştir. Standardın referans numarasının değişmesi ise, ISO/IEC 27002:2005 başlığı altında yeni bir standart yayınlanmasını zorunlu kılmıştır. Bu standart ise, ISO/IEC 17799:2005 ve ISO/IEC 17799:2005/Cor.1:2007 standartlarından oluşmaktadır. Bunun yanı sıra standart, bir organizasyonda bilgi güvenliği yönetimini oluşturmak,

uygulamak, sürdürmek ve iyileştirmek için genel ilkeler sunmaktadır (ISO/IEC 27002:2005, 2005).

İkinci basımı 2013 yılında yayınlanan standart, bilgi güvenliği yönetiminden ziyade bilgi güvenliği kontrollerini ele almaktadır. Bu standart organizasyonların kendi bilgi güvenliği yönetim rehberini oluşturmaları için ilkeler sunmaktadır (ISO/IEC 27002:2013, 2013). 2014 ve 2015 yılında değişikliği yapılan bu standardın yerini ise şu anda geliştirilme aşamasında olan ISO/IEC CD 27002 başlığı altından yayınlanacak olan standardın alacağı planlanmaktadır.

- ISO/IEC 27003 Bilgi Teknolojileri – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemi Uygulama Kılavuzu 1/2: Birinci basımı 2010 yılında yayınlanan standart, Bilgi Güvenliği Yönetim Sisteminin başarılı bir şekilde tasarlanması ve uygulanması için gerekli kritik yönlere odaklanmakla beraber, BGYS tasarım süreci hakkında uygulama planları sunmaktadır (ISO/IEC 27003:2010, 2010). İkinci basımı 2017 yılında yayınlanan standart, ISO/IEC 27001:2013 standardı hakkında bir rehber ve açıklama sağlamaktadır (ISO/IEC 27003:2017, 2017).

- ISO/IEC 27004 Bilgi teknolojileri – Güvenlik teknikleri – Bilgi güvenliği yönetimi – Ölçüm 1/2: Birinci basımı 2009 yılında yayınlanan standart, uygulanan bilgi güvenliği yönetim sistemini ve kontrollerinin veya kontrol gruplarının etkinliğini değerlendirmek için önlemlerin ve ölçümlerin geliştirilmesi ve kullanımı hakkında rehberlik sağlamaktadır (ISO/IEC 27004: 2009). İkinci basımı 2016 yılında yayınlanan standart, birinci basımdan farklı olarak ölçümün yanında, izleme, analiz ve değerlendirme gerekliliklerini yerine getirmek için kuruluşların bilgi güvenliği performansını ve bir bilgi güvenliği yönetim sistemini etkinliğini değerlendirmeye destek olmak için tasarlanmıştır (ISO/IEC 27004:2016, 2016).

- ISO/IEC 27005 Bilgi teknolojileri – Güvenlik teknikleri – Bilgi güvenliği risk yönetimi 1/2/3: 1998 ve 2000 yılında yayınlanan standartların yerini alan ISO/IEC 27005: 2008 bilgi güvenliği risk yönetimi standardı, risk yönetimi için kurallar sağlamaktadır (ISO/IEC 27005:2008, 2008). Bu standardın çekilmesinden sonra, 2011 yılında yeni bir standart yayınlanmıştır. Yedi yıl süre ile kullanılan bu

standarttan sonra ise, standardın üçüncü basımı yayınlanmıştır (ISO/IEC 27005:2018, 2018).

- ISO/IEC 27006 Bilgi Teknolojileri – Güvenlik teknikleri – Bilgi Güvenliği Yönetim Sistemlerinin Denetim ve Belgelendirmesini Sağlayan Kuruluşlar İçin Şartlar 1/2/3: Kurum ve kuruluşların belgelendirilmesini sağlayan bu standart, bilgi güvenliği yönetim sisteminin oluşturulması için kılavuzluk etmektedir. 2007 ve 2011 yıllarında birinci ve ikinci basımı yapılan standardın üçüncü basımı 2015 yılında yayınlanmıştır (ISO/IEC 27006: 2015, 2015).

- ISO/IEC 27007 Bilgi teknolojileri – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri Denetimi İçin Rehber 1/2: İlk basımı 2011, ikinci basımı ise 2017 yılında yayınlanan standart, bir bilgi güvenliği yönetim sistemi denetim programının yönetilmesi, denetimlerinin yapılması ve bilgi güvenliği yönetim sistemi denetçisinin yeterliliği hakkında rehberlik etmektedir (ISO/IEC 27007:2017, 2017).

2.4.2. Diğer Standart ve Spesifikasyonlar

- BS 7799-1/2/3 Bilgi Güvenliği Yönetimi – Bilgi Güvenliği Yönetim Sistemleri İçin Uygulama Standardı: Bilgi varlıklarının gizlilik, kullanılabilirlik ve erişilebilirliğini garanti altına almak için uygulanması gereken güvenlik ölçümlerini düzenleyen ve belgelendiren İngiliz Standartları iki kısımdan oluşmaktadır. Standardın birinci kısmı 1995 yılında yayınlanmıştır. Daha sonra bu standart tekrar revize edilerek 2002 yılında ikinci kısmı yayınlanmıştır. Standardın ikinci kısmında birinci bölümden farklı olarak bilgi güvenliği yönetim sistemine ait belgelendirme (sertifikasyon) yer almaktadır (Vural ve Sağıroğlu, 2008, s.511). Yine bu bölümde, bir bilgi güvenliği modeli ele alınmıştır. Bu modelde bileşenler planlama, uygulama, kontrol etme ve önlemlerin alınması olarak belirlenmiştir.

  2006 yılında üçüncü kısmı yayınlanan standart, risk analizini ve yönetimini kapsamaktadır. Bu standardın kaldırılmasının ardından 2017 yılında yeni bir

standart yayınlanmıştır. Bu standartta ise, ISO/IEC 27001 standardının uygulanması için temel destek sağlanmaktadır (British Standards Institution, 2018). Aynı zamanda standart, bilgi güvenliği politikalarında hangi unsurların kesinlikle bulunması gerektiği konusunda bilgi içeren ilk bilgi güvenliği standartlarından biri olması yönüyle önem taşımaktadır (Henkoğlu, 2015a, s.34).

- Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri (Control Objectives for Information and Related Technology – COBIT) : COBIT, Bilgi teknolojisi (BT) yönetimi ve kontrolleri için olgunluk modeli sağlamaktadır. Güvenlik temeli, küçük ve büyük kuruluşlar için takip edilmesi ve uygulanması basit bir şekilde güvenlik etrafındaki özel risklere odaklanmaktadır (Kocamustafaoğulları, 2013, s.14).

- Bilişim Teknolojileri Altyapı Kütüphanesi (Information Technology Infrastructure Library - ITIL): Bilgi teknolojisi, altyapısını, gelişimini ve süreçlerini yönetmek için bir dizi kavram ve teknikleri kullanan ITIL, bilgi teknolojileri dağıtımı süreçleri ve servis yönetimi ile dünyada yaygın olarak kullanılmaktadır (Haklı, 2012, s.17).

- Genel Kabul Görmüş Sistem Güvenliği Prensipleri (Generally Accepted System Security Principles - GASSP): 1990 yılında Amerika Birleşik Devletleri Ulusal Araştırma Konseyi tarafından yayınlanan ilkeler, “risk altındaki bilgisayarlar” raporunun önerilerine dayanan genel kabul görmüş bir sistem güvenlik ilkesi olarak nitelendirilmektedir (Poore, 1990, s.28; Höne ve Eloff, 2002, s. 406). Bilgi teknolojilerini güvence altına almak için kullanılan bu ilkeler, bir sistemi geliştirirken ya da sürdürürken herkesin bunları uyguladığına dayanmaktadır (Swanson ve Guttman, 1996, s.4).

- Bilgi Güvenliği Teknolojileri İçin Temel İlkeler (The Guidelines for the Management of IT Security – GMITS): ISO Ortak Teknik Komitesi (ISO Joint Technical Committe) tarafından hazırlanan kurallar, bilgi güvenliğinin planlanması, yönetilmesi ve uygulanması hususunda rehberlik sağlamaktadır.

Bununla birlikte, kuruluşlar için önerilen politika ilkeleri tanımlanmaktadır (Höne ve Eloff, 2002, s. 407).

- Bilgi Güvenliği Forumu'nun İyi Uygulama Standardı (Information Security Forum's Standard of Good Practice) : İki yılda bir yayımlanan ve her yıl yenilenen bu standart, 1996 yılında Bilgi Güvenliği Forumu (ISF) tarafından yayımlanmıştır. Bilgisayar kurulumları, kritik iş uygulamaları, güvenlik yönetimi, ağlar, sistem geliştirme ve son kullanıcı ortamı olmak üzere altı temel husus etrafında toplanmıştır (Tofan, 2011, s. 132).

- SP800 Standart Serisi: 1901 yılında kurulan NIST, Amerika Birleşik Devletleri Ticaret Bakanlığı içinde düzenleyici olmayan bir federal ajanstır. 1990 yılında kurulan NIST Özel Yayınları 800 belge grubu, tüm bilgi güvenliği standartlarının en eskisidir (Tofan, 2011, s.131). Seride, NIST'in siber güvenlik faaliyetlerinin yıllık raporları, teknik özellikleri, önerileri ve rehberleri yer almaktadır. Yayınlar, ABD Federal Hükümeti bilgi ve bilgi sistemlerinin güvenlik ve gizlilik ihtiyaçlarını ele almak ve desteklemek için geliştirilmiştir (NIST, 2018).

- BSI IT (The Bundesamt für Sicherheit in der Informations technik/ Federal Bilgi Güvenliği Bürosu)-Grundschutz – IT baseline Protection : Federal Bilgi Güvenliği Ofisi (BSI) tarafından hazırlanan standartlar, bilgi güvenliği ile ilgili, yöntemler, süreçler, prosedürler, yaklaşımlar ve alınacak önlemler hakkında tavsiyeler içermektedir (BSI). Bilgi teknolojisi kullanıcılarına teknik destek sağlamak için kullanılan standart, dört bölümden oluşmaktadır.

  BSI Standard – 100- 1 Bilgi yönetimi sistemleri olarak adlandırılan ilk standart, bilgi güvenliği yönetim sistemi için genel gereksinimleri tanımlamaktadır. ISO 27001 ile tamamen uyumlu olan standart, ISO 13335 ve 27002 standartlarındaki önerilerini de dikkate almaktadır (Tofan, 2011, s.134). BSI-Standard 100-2:IT Grundschutz olarak isimlendirilen ikinci standart ise, bilgi güvenliği süreçlerinin oluşum aşamalarını, güvenlik kavramının uygulanması, bilgi güvenliğinin bakımı ve sürekli iyileştirilmesi gibi konular üzerinde durmaktadır (BSI-Standard 100-2, 2008 s.4). Standardın üçüncü versiyonu ise, ikinci versiyonun 2005 yılında

uyarlanmasıyla oluşmuştur. Bu standartta temel olarak, güvenlik süreçleri içerisindeki risk analizleri konu olarak ele alınmıştır (BSI-Standard 100-3, 2008). İş sürekliliği yönetimine odaklanan dördüncü standart ise, iş sürekliliği yönetim süreçlerini, risk analizlerini, operasyonel yapıları, testler ve alıştırmaları ele almaktadır (BSI Standard 100-4, 2008).

2.5. KİŞİSEL VERİLERİN KORUNMASI

Bilgi güvenliği ve kişisel verilerin korunması başlığıyla ele alınan ikinci bölümde, bilgi güvenliği ile ilgili olan konulara önceki sayfalarda değinilmiştir. İkinci bölümün alt başlığı olan 'Kişisel verilerin korunması' başlığı altında ele alınan bu bölümde ise, kişisel veri, kişisel verilerin işlenmesi, kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi, kişisel verilerin aktarılması, kişisel verilerin korunmasına yönelik kanunlar ve düzenlemeler ve son olarak Kişisel Verileri Koruma Kurumu (KVKK) irdelenecektir.

2.5.1. Kişisel Veri

Kişisel veriler, gelişen teknolojinin sunmuş olduğu olanaklar doğrultusunda etkileşimde bulunulan uygulama ve araçlarla paylaşılan bir veri türlerinden biridir. Bu verilerin kullanımının artması, kişisel özelliklere yönelik örüntüleri yansıtması, kurumsal boyutta ticari ve stratejik bir araç olarak kullanılması bu veri türünün kapsamını belirlemeye ve tanımlamaya yönelik çalışmaların yapılmasını gerektirmiştir. Bu doğrultuda kişisel veri kavramının uluslararası düzenlemeler de dâhil olmak üzere birçok çalışmada tanımlandığı görülmektedir. Kişisel veri kavramının ortaya çıkışında, insan hak ve özgürlüklerinin korunması ve özel hayatın gizliliği gibi konulardaki uluslararası düzenlemelerin etkili olduğunu söylemek mümkündür. 4 Kasım 1950 tarihinde Roma'da imzalanan ve üç sene sonra yürürlüğe giren İnsan Hakları ve Temel Özgürlükleri Korumaya Dair Avrupa Sözleşmesi (Convention for the Protection of Human Rights and Fundamental Freedoms) içeriği bakımından kişisel verilerin korunması süreçleriyle ilgili bir düzenlemelerden biri olarak gösterilebilir (Council of Europe, 1950). Sözleşme çerçevesinde kişisel veri üzerine herhangi bir tanım yapılmamış olmasına karşın kişisel veri kapsamında ele alınabilecek temel unsurların (haklar ve özgürlükler) üzerinde durularak, bu unsurların hangi koşullarda sağlanabileceğine yer verilmiştir.

Kişisel veri konusunun ele alındığı bir diğer uluslararası belge ise 23 Eylül 1980 tarihinde Ekonomik Kalkınma ve İş birliği Örgütü (The Organization for Economic Co-operation and Development - OECD) tarafından yayımlanan *"Özel Yaşamın Korunması ve Sınır Ötesi Akışına İlişkin Rehber İlkeler" (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)* başlıklı rehberdir. Bu rehberde yer alan birinci ilke kapsamında kişisel veri, tanımlanmış veya tanımlanabilir bir kişiye ilişkin herhangi bir bilgi olarak ifade edilmiştir (OECD, 1980, s.13).

Kişisel veri kavramının tanımlandığı bir diğer çalışma ise, 28 Ocak 1981 tarihinde Strazburg'da imzalanan Avrupa Konseyi'nin hazırlamış olduğu 108 sayılı *"Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması (Protection of Individuals with regard to Automatic Processing of Personal Data)* başlıklı sözleşmenin ikinci maddesinde kimliği belirli veya belirlenebilir bir gerçek kişi ("ilgili kişi") hakkındaki tüm bilgiler kişisel verilerin kapsamına dahil edilmiştir (108 Sayılı Kişisel Verilerin, 2016, s.2).

24 Ekim 1995 tarihinde *"95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi*" başlığıyla yayınlanan direktifte kişisel veri, "özellikle bir kimlik numarasına, konum verisine veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla faktöre atıfta bulunarak doğrudan ya da dolaylı olarak tanımlanabilen kişi olmak üzere; tanımlanan veya tanımlanabilir gerçek kişi ile ilgili herhangi bir bilgi" olarak tanımlanmaktadır (Avrupa Konseyi, 1995). Bu Direktif Avrupa Parlementosu ve Avrupa Konseyince 27 Nisan 2016 tarihinde yürürlükten kaldırılarak yerine GDPR yayınlanmıştır. Önceki düzenlemede yer alan kişisel veri tanımının (madde 4/fıkra 1) bu yönetmelikte de tekrarlandığı dikkat çekmektedir (GDPR, 2018).

Kişisel veri üzerine yapılan başka bir tanım ise, 23 Ocak'ta Avrupa Komisyonu Japonya'nın Kişisel Bilgilerin Korunması Hakkında Kanun (Act on the Protection of Personal Information) kapsamında kişisel verilerin korunması konusuna yönelik yeterlilik düzeyine ilişkin Komisyon Uygulama Kararını yayımlamıştır. Bu karara göre kişisel veri, "bir kişisel bilgi veri tabanını oluşturan kişisel veriler" şeklinde ifade edilmiştir. Diğer bir deyişle, "bir bilgisayar kullanarak belirli kişisel bilgileri arayabilmek

için sistematik olarak organize edilmiş kişisel bilgileri içeren kolektif bir bilgi organı" kişisel veri olarak nitelendirilmiştir (European Commission, 2019, s.5). Bu tanıma göre kişisel veri kavramı kapsamında sadece belirli bilgi türlerine yer verilmektedir. Yine bu tanımdan hareketle, kişisel verinin aslında bir bilgi kümesinin içerisinde yer alan bireylerin haklarına ve özelliklerine yönelik veriler olduğunu söylemek mümkündür.

Uluslararası kurumlarca yayınlanan çalışmaların yanı sıra ülkelerin de kişisel verileri korumaya yönelik komisyonlar kurdukları görülmektedir. Bu komisyonlardan biri olan Singapur Kişisel Veri Koruma Komisyonu (Personal Data Protection Commission Singapore) kişisel veriyi, bir kişinin isimlerinden ve iletişim numaralarından, diğer veri türlerine kadar değişiklik göstererek bir kişiyi tanımlayan tüm verileri 'kişisel veri' olarak tanımlamıştır (Personal Data Protection Commission Singapore, 2015, s.3). Bu bağlamda, bir kişi ile ilişkilendirilmiş isim, pasaport numarası, bireysel fotoğraf veya video, parmak izi ve ev adresi gibi içerikler kişisel veriler kapsamına dâhil edilebilemektedir.

Kanada Mahremiyet Komisyonu (Office of Privacy Commissioner of Canada) ise PIPEDA'da, tanımlanabilir bir birey hakkında kaydedilmiş veya kaydedilmemiş her türlü gerçek veya öznel bilgiyi kişisel veri olarak belirtmiştir (PIPEDA, 2019). Bu noktada ise, tanımlanabilir bir kişi ile ilişkilendirilerin yaş, isim, kimlik numaraları, gelir, etnik köken veya kan grubu, görüşler, değerlendirmeler, yorumlar, sosyal statü veya disiplin işlemleri, çalışan dosyaları, kredi kayıtları, tıbbi kayıtlar, bir tüccar ile bir tüketici arasındaki anlaşmazlıklar, niyetler (mal veya hizmet edinmek, iş değiştirmek) gibi veriler kişisel veri kapsamına dâhil edilmiştir. Küzeci de (2010, s.11), verinin bir kişiye ilişkin (i) ve bu kişinin de belirli ya da nelirlenebilir nitelikte olmasını (ii) kişisel veriyi, kişisel olmayan verilerden ayıran iki temel ölçüt olarak nitelendirmiştir.

İsviçre Federal Konseyi ise, 19 Haziran 1992 tarihli Federal Veri Koruma Kanunun'da (*Federal Act on Data Protection)* (s.2), kişisel veriyi tanımlanmış veya tanımlanabilir bir kişiyle ilgili tüm bilgiler şeklinde ifade etmiştir (Federal Act..., 1992). İsviçre Federal Konseyi tarafından yapılan bu tanım, OECD'nin 1980 yılında yapmış olduğu tanımla örtüşmektedir. Ancak, bu iki tanım arasında kapsam bakımından bir farklılık bulunduğu görülmektedir. Bu farklılık OECD'nin tanım kapsamına kişileri nitelendirecek olan herhangi bir bilgiyi dâhil etmesinden kaynaklanmaktadır.

24 Mart 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. Maddesinde kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" şeklinde ifade edilmiştir (Kişisel Verilerin Korunması Kanunu, 2016). Türkiye'de yayınlanan bir diğer yasal uygulama olan 28363 sayılı ve 24 Temmuz 2012 tarihli Resmî Gazete'de yayınlanan "*Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik"*te, kişisel veri, belirli veya kimliği belirlenebilir gerçek veya tüzel kişilere ilişkin bütün bilgiler şeklinde tanımlanmıştır ("Elektronik Haberleşme Sektöründe…", 2012).

Kişisel veri konusu üzerine yapılan bilimsel çalışmalarda insanların kimliklerini tespit etmeye yarayan ad, soyad, adres, sendikal veya siyasal faaliyetler, kredi kartı bilgileri gibi bir kişiyi doğrudan ya da dolaylı olarak tanımlayabilecek her türlü bilgi ve enformasyonun kişisel veri olduğuna değinilmiştir (Çelebioğlu, 2005, s.16; Ersoy, 2009, s.16; Toğuz, 2010, s.25; Yüksel Civelek, 2011, s.16; Kılınç, 2012, s.1095; Ünsal, 2013, s.101; Borazan, 2015, s.204; Başalp, 2016, s.16; Gürsel, 2016, s.34). Benzer tanımlara kişisel verilerin korunması ile ilgili yayınlanan rehberlerde de verilmiştir (European Data ProtectionSupervisor, 2018, s. 12; Information Commissioner's Office, 2018).

Kavram üzerine yapılan ulusal ve uluslararası düzenlemeler ve bilimsel çalışmalardaki tanımların bazı noktalarda belirsizlikler içerdiği görülmektedir. Bu belirsizliklerin genellikle kişisel verinin belirlenebilirlik, tanımlanabilirlik ve aitlik (tüzel ya da gerçek kişilere yönelik olma) durumlarıyla ilgili olduğu anlaşılmaktadır.

Kişisel verinin kavramına ilişkin belirsizlikleri gidermek ve ulusal mevzuatlarda kişisel veri yönetim uygulamalarının nasıl uygulanacağına ilişkin ortak bir anlayış oluşturmak amacıyla AB'nin 95/46 sayılı yönergesinin 29. Maddesince bir veri koruma çalışma grubu oluşturulmuştur (Uygun, 2010, s.41). Bu çalışma grubunda[5] 28 ülkeden yetkililer görev almıştır (European Commission, 2018). Çalışma Grubu'na göre kişisel veri, "herhangi bir bilgi", "bir kişiyle ilgili", "kimliği belirli veya belirlenebilir" ve "gerçek kişi olmak üzere dört unsurdan oluşmaktadır (Uygun, 2010, s.42-44).

[5] (Ayrıntılı bilgi için bkz. http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=50061).

Yılmaz'a göre (2002, s. 497) kişileri birbirinden ayıran vasıf olarak tanımlanan kimlik, bir bireyle ilgili cinsiyet, doğum yeri, yılı, baba, anne, eğitim ve iş durumu gibi nüfus kayıtlarındaki adli bilgiler ve kişinin fiziksel özelliklerini çıkartabilecek boy, vücut ağırlığı, yara izi gibi tıbbi bilgilerden oluşmaktadır.

Kişisel veriler tür ve özelliklerine göre, özel ve genel nitelikli veriler olmak üzere ikiye ayrılmaktadır. Kişisel verilerin bir nokta ötesini oluşturan özel nitelikli veriler, kapsamına giren türler yoluyla da tanımlanabilmektedir (Kartal, 2018, s.3). Öte yandan, kişisel veri kavramını tanımlamada görülen belirsizlikler gibi özel nitelikli olan verileri tanımlamada da belirsizlikler görülmektedir. Bazı uluslararası düzenlemelerde[6] 'hassas veri', 'özel türde veri' olarak da tanımlanabilen özel nitelikli kişisel veriler (sensitive data), kendine özgü özellikleri olan ve genel nitelikli kişisel verilere göre daha korunaklı bir veri grubu olarak tanımlanmıştır (Taştan, 2017, s.43). Sert'e göre (2019, s.39), açıklanması hâlinde kişinin başkalaştırılmasına ya da ötekileştirilmesine neden olacak veriler hassas nitelikli veri kapsamına dahil edilebilmektedir. Bu çerçevede, hassas kişisel veri kişilerin özel hayatlarını ve aile hayatlarının gizliliğini ihlal edebilecek ya da verilerin açığa çıkartılması halinde kişilerin başkalaştırılmasına sebep olabilecek değerli verilerdir. Kişilerin inançları, siyasi düşüncesi, felsefi inancı, dini, etnik kökeni, mezhebi veya diğer inançları, dernek, vakıf ya da sendika üyeliği, kılık ve kıyafeti, cinsel hayatı, sağlığı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri biyometrik ve genetik verileri 6698 sayılı Kişisel Verileri Koruma Kanun'unun 6. Maddesi'nde özel nitelikli kişisel verilere örnek olarak gösterilmiştir (Kişisel Verilerin Korunması Kanunu, 2016). Genel nitelikli veriler ise, özel nitelikli veri kategorisine dâhil edilmeyen verilerdir (Taştan, 2017, s.4).

[6]Örneğin, Alman Federal Veri Koruma Kanunu'nda özel kategorili kişisel veri (special categories of personal data) olarak tanımlanırken, Hollanda Veri Koruma Kanunu'nda özel kişisel veriler (special personal data) ve Avusturya Federal Kişisel Verilerin Korunması Kanunu'nda özel korumaya layık olan veriler (data deserving special protection) kavramları kullanılmaktadır (Kaya, 2011, s.318; Kartal, 2018, s.4).

2.5.2. Kişisel Verilerin İşlenmesi

Kişisel verileri işleme yöntemlerine ve ilkelerine geçmeden önce kişisel verilerin işlenmesini tanımlamakta yarar vardır. Kişisel verilerin işlenmesi, bir sürece ve bir yaşam evresine dayanmaktadır. Verilerin işlenmesi, bir ya da birden çok kişi veya kurumu kapsayan bir sürece ilişkin düzenlemeyi ve kişisel verilerin birbirine bağımlı olarak devam eden yaşamsal bir döngüyü kapsamaktadır (Dinkçi, 2014, s.5). Bu döngü, verinin ilk defa elde edilmesiyle başlayıp veri üzerinde gerçekleştirilen her türlü faaliyeti temsil etmektedir (Akıncı, 2017, s.27).

Kişisel Verileri Koruma(KVK) Kanunu'nun 3. maddesinde ise, *"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem"* kişisel verilerin işlenmesi olarak tanımlanmaktadır (Kişisel Verilerin Korunması Kanunu, 2016).

Genel Veri Koruma Tüzüğü'nde ise kişisel verilerin işlenmesi otomatik yöntemlerle olsun veya olmasın kişisel veri üzerinde gerçekleştirilen herhangi bir işlem ya da işlem dizisi veri işleme şeklinde tanımlanmıştır (Avcı, 2019, s.49).

Avrupa Konseyi'nin 108 Sayılı Sözleşmesinin 2. maddesinde otomatik işleme, *"Tamamı veya bir kısmı otomatik yöntemlerle gerçekleştirilen verilerin kaydı, bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanışı, verilerin değiştirilmesi, silinmesi çıkarılması veya dağıtılması"* şeklinde tanımlanmaktadır (108 Sayılı Kişisel Verilerin, 2016, s.2)

Bunun yanı sıra özel nitelikli verilerin, kendi bünyelerinde risk taşıdığı ve bu bilgilerin iç hukukta uygun güvence sağlanmadıkça ve ilgili kişinin rızası alınmadıkça otomatik işleme tabi tutulamayacağı temel ilke olarak belirtilmiştir (Şimşek, 2008, s.86; Akdağ, 2013, s.31; Henkoğlu ve Uçak, 2015, s.19; Taştan, 2017, s.44). Örneğin, 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşmenin 6. Maddesinde, 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki yönergenin 8.

Maddesinde ve Türk Ceza Kanunu'nun (TCK) 135. maddesinde, özel nitelikli kişisel verileri kaydeden kişilerin cezalandırılacağına değinilmiştir. Otomatik olmayan yollarla veri işleme ise, veriler hem elektronik ortamda (bilişim sistemleri üzerinden) hem de fiziki ortamda işleme olarak ifade edilmektedir (Erdinç, 2017, s.23).

Kişisel verilerin işlenmesi belirli adımlara dayanmaktadır. İlk olarak, kişisel verileri işlenmesi ile ilgilenecek olan kişinin Veri Sorumluları Siciline (VERBİS) kayıt olması gerekmektedir. Ancak, VERBİS'e kayıt olunmadan önce kişisel veri işleme envanterinin, kişisel veri saklama ve imha politikası belgesinin hazırlanması lazımdır. Daha sonra gerçekleştirilecek olan adımda ise, kişisel verilerin toplanacağı fiziksel veya elektronik ortam kişilerin erişimine açılmaktadır. Veri sorumlusu ilgili kişi hakkında topladığı kişisel verileri, hangi doğrultuda kullanacağı konusunda veri sahibine bilgiler vererek kişiden onay talep etmektedir. Bu noktada, veri sorumlusunun, ilgili kişiye kendini tanıtması da gerekmektedir. Son olarak, kişinin onayı doğrultusunda kişisel veriler işlenmektedir. Diğer taraftan, sicile kayıt olunduktan sonra veri sorumlusunun ve kişisel verileri işlenilecek olan kişinin değişmesi halinde sicilde değişiklik için başvurulması gerekmektedir. Diğer bir aşamada, veri sorumlusunun işlemiş olduğu kişisel veriler, verileri işleyen kurum ve kuruluşlarla paylaşılmaktadır. Kişisel verilerin işlenme şartlarını ortadan kaldıran en son işlem ise, kişisel verilerin yok edilmesi ve anonimleştirmedir. Silme işleminde tüm işlemler bittikten veya kişisel verilerin işlenme hakkı durduktan sonra gerçekleştirilmektedir. Silinmesi istenmeyen veriler ise, anonim hale getirilmektedir. Bununla birlikte, kişisel verilerin işlenmesi ve verilerin korunması aşamasında dikkate alınması gereken birtakım prensipler bulunmaktadır. Eroğlu'nun (2018, s.134), OECD'den aktardığı bilgiye göre (2013) bu prensipler temel olarak; sınırlılık, kalite, açıklık, amaca özgülük, güvenlik, kullanım sınırlaması, bireyin rızası ve hesap verilebilirlik olmak üzere sekiz ana bileşene ayrılmaktadır.

Verilerin, kişisel veri olarak nitelendirilebilmesi veya belirli bir kişiyi temsil etmesi için veri işleme süreçlerinde kesinlik kazandırılması gerekmektedir (Eroğlu, 2018, s.134). Söz konusu süreçler ise, verilerin elde edilmesi, kaydedilmesi, uyarlanması, dönüştürülmesi, kullanımı, açıklanması, sıralanması, birleştirilmesi, silinmesi ve anonim hale getirilmesi gibi süregelen adımlardan oluşmaktadır (Kaya, 2011, s.317). Kişisel verilerin işlenmesine örnek olarak bir bireyin fotoğrafının veya parmak izinin elde edilmesi, sesinin veya

görüntüsünün kaydedilmesi veya bu kayıtların başkalarıyla paylaşılması veya yayınlanması gibi eylemler gösterilebilmektedir (Uygun, 2010, s.48). Kişisel verilerin işlenmesi sürecinde gerçekleştirilen her bir işlem, birbirinden bağımsız olarak gerçekleştirilmektedir. Diğer bir deyişle, her bir verinin ayrı olarak işlenmesi tek başına bir veri işleme sayılmaktadır (Çokmutlu, 2014, s.37). Kişisel veriler, bireyin açık rızası olmadan ve belli şartlara dayanmadan işleme tabi tutulamamaktadır. Bu bağlamda, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (2016) 5. Maddesi'nin (2) fıkrasında verilen aşağıda yer alan koşullardan herhangi birisinin varlığı hâlinde, ilgili bireyin açık rızası olmaksızın kişisel verilerin işlenmesi mümkün hale gelmektedir:

- Kanunlarda açıkça öngörülmesi,
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

Kişisel veriler, uygun yasal düzenlemeler çerçevesinde işlenebilmektedir. Bu çerçevede, 6698 sayılı Kişisel Verilerin Korunması Kanunu (2016) 4. Maddesi gereğince kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

- Hukuka ve dürüstlük kurallarına uygun olma,
- Doğru ve gerektiğinde güncel olma,
- Belirli, açık ve meşru amaçlar için işlenme,
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

Kişisel verilerin işlenmesi işlemelerinin bir dizi işlemlere dayandığından söz etmiştik. Bu işlemlerde ise, veri sorumluları işlenen verilere dair sistemlerde veri kayıtları oluşturabilmektedir. Bu kayıtların, kullanma sürelerinin oluşturulması ve kullanılmayan verilerin silinmesi hem sistem güvenilirliği açısından hem de bireylerin güvenilirliği açısından önem taşımaktadır.

2.5.3. Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonimleştirilmesi

Kişisel veriler, kullanım süreleri geçtikten sonra silme, yok etme veya anonimleştirme gibi işlemlere tâbi tutulmaktadır. 30224 sayılı ve 28 Ekim 2017 tarihli "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkındaki Yönetmeliğin" 8. Maddesince "kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini kişisel verilerin" silinmesi; 9. Maddesince kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getiririlmesi işlemini kişisel verilerin yok edilmesi; 10. Maddesine göre ise, "kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi" işlemini kişisel verilerin anonim hale getirilmesi olarak tanımlamaktadır (Kişisel Verilerin Silinmesi, 2017).

Kişisel veriler, kullanıldığı kurum ve kuruluşlarda ilgili kanun ve mevzuatlarda geçen süre boyunca saklanmalı ve silinmelidir. Söz konusu bahsedilen kişiye ait hassas nitelikli veriler olduğundan dolayı silme, yok etme ve anonimleştirme işlemlerinin veri sorumluları tarafından yapılması gerekmektedir. Aksi halde, kişisel verilerin gereksiz yere saklandığı sürece temel hak ve hürriyetlerin ihlali tehlikesi devam edecek ve kişilerin zarara uğramasına sebep olacaktır (Ersoy, 2009, s.111).

Kişisel verilerin silinmesi, veri sorumlusunun yasal uygunluğa dayanarak "kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirmesi" işlemidir. Bu süreçte silinecek verilerin tespiti, erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi, ilgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi, ilgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması işlemlerine dayanmaktadır ("KVKK", 2018, s.10).

Kişisel veriler, bulut sistemi üzerinde, kâğıt ortamında, merkezi sunucuda yer alan ofis dosyalarında, taşınabilir medyada ve veri tabanları gibi farklı ortamlarda yer aldıklarından dolayı farklı yöntemlerle silinmektedir. Ofis 365, Salesforce ve Dropbox gibi bulut çözümlerinde yer alan veriler ilgili kullanıcının verileri geri getirme yetkisinin

olmadığına dikkat edilerek silme komutu ile kişisel veriler silinmektedir. Kâğıt ortamında yer alan kişisel veriler ise, karartma yöntemi kullanarak yapılmaktadır. Karartma yöntemi, mümkün olan durumlarda kesilmesi veya kişisel verilerin üzeri okunmayacak şekilde çizilerek / boyanarak / silinerek yapılmaktadır. Ofis dosyalarında yer alan veriler dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması yöntemiyle gerçekleşmektedir. Taşınabilir medyada yer alan veya flash tabanlı saklama ortamlarındaki kişisel veriler, parola olarak saklanmalıdır ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir. Veri tabanlarında yer alan veriler ise, ilgili satırların veri tabanı komutları ile (delete vb.) silinmesi gerekmektedir ("KVKK", 2018, s.7-9).

Kişisel verilerin silinmesi işleminin ardından devam eden bir süreç ise kişisel verilerin yok edilmesi işlemidir. Ortadan kaldırma işlemi olarak tanımlanan kişisel verilerin yok edilmesi, KVKK tarafından hazırlanan "Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi" isimli rehberde *"Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi"* olarak tanımlanmaktadır ("KVKK", t.y., s.9). Kişisel verilerin silinmesi işleminde olduğu gibi, yok etme işleminde de uygulanan yöntemler bulunmaktadır. Öncelikle verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre uygun yöntemlerin seçilmesi gerekmektedir. Bu bağlamda veriler yerel sistemler, çevresel sistemler, kâğıt ve mikrofiş ortamları, bulut ortamında yer alan verilere göre yok edilmektedir. Yerel sistemlerde bulunan veriler de-manyetize etme, fiziksel yok etme, üzerine yazma yöntemlerinden bir ya da birkaçı kullanılarak yok edilmektedir. Ağ cihazları, flash tabanlı ortamlar, manyetik bant, manyetik disk gibi üniteler, mobil telefonlar, optik diskler, veri kayıt ortamı çıkartılabilir/sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri ortamın türüne göre yok edilmektedir.

Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi ise kişisel verilerin anonim hale getirilmesidir. Bu durumun sağlanabilmesi için, kişisel verilerin, veri sorumlusu veya alıcı grupları tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle

ilişkilendirilemez hale getirilmesi gerekmektedir ("KVKK", 2018, s.16). Veri ile bu verinin tanımladığı kişi arasındaki bağın kopartılması amacıyla yapılan anonimleştirme, daha önce gerçek kişi olarak kişisel verileri tanımlanan bireyin daha sonra verilerin ilgili kişi ile bağının kopartılması yoluyla gerçekleştirilmektedir.

Anonim hale getirme yöntemleri, değer düzensizliği sağlayan, değer düzensizliği sağlamayan ve anonim hale getirmeyi kuvvetlendirici istatiksel yöntemler olmak üzere üçe ayrılmaktadır. Değer düzensizliği sağlamayan anonim hale getirme yöntemleri, kümede bulunan verilerin sadece satır veya sütunlarında değişikliklerin yapılması ile elde edilmektedir. Yani, veri kümesinin sahip olduğu bir değerde ekleme veya çıkartma işlemi yapılmamaktadır. Bu yöntem, veri kümesini daha güvenilir hale getirmek ve tahmin edilebilirlik riskini azaltmak amacıyla kullanılmaktadır. Değişkenleri çıkartma, bölgesel gizleme, kayıtları çıkartma, alt ve üst sınır kodlama, genelleştirme, küresel kodlama ve örnekleme gibi işlemler bu yöntemde yapılmaktadır. Veri değiş tokuşu, mikro birleştirme ve gürültü ekleme gibi anonimleştirme yöntemlerinin uygulandığı değer düzensizliği sağlayan anonimleştirme yönteminde var olan değerler değiştirilerek veri kümesinin değerlerinde bozulma yaratılmaktadır. Anonimliği güçlendirmek ve veri kümesinden sağlanan faydayı belli bir seviyede tutmak amacıyla gerçekleştirilen istatistiksel yöntemler (K-Anonimlik, T-Yakınlık, L-Çeşitlilik) veri kümesi içindeki kayıtların tekilliğini minimum seviyeye indirmektedir. Veri sorumluları tarafından gerçekleştirilen anonim hale getirme yöntemlerinde verinin niteliğine, büyüklüğüne, fiziki ortamda bulunma yapısına, çeşitliliğine, işleme amacına, işlenme sıklığına ve verinin anonimliğinin bozulması halinde ortaya çıkacak zararın büyüklüğü gibi özelliklerine bakılarak hangi yöntemin uygulanacağına karar verilmektedir ("KVKK", 2018, s.17).

2.5.4. Kişisel Verilerin Aktarılması

Kişisel verilerin yer aldığı belge ve dokümanlar üretim ve kullanım amaçlarına göre kişi, kurum/kuruluş ya da yurt dışında kullanılabilmektedir. Ancak, sadece veri sorumlularının ve yetkili kişilerin kişisel veriye erişim sağlayabilmeleri kişisel verilerin korunması bağlamında ele alınmaktadır. Bu nedenle, kişisel verilerin korunması başlığı altında alınan verilerin ilgili kişi ya da kişilerle paylaşımında belirli şartların geçerli olduğunu ve bu şartlar dâhilinde yalnızca yetkili kişilere aktarabilmektedir (Ersoy, 2009, s.111).

Kişisel Verilerin Korunması Kanunu'nun 8. Maddesinde kişisel verilerin aktarılması, ilgili kişinin açık rızasının olması şartıyla özdeşleştirilmiş ancak ikinci fıkrasında kişisel verilerin transfer edilmesi, kişisel verilerin işlenmesi şartlarına tabi tutularak ilgili kişinin açık rızası olmaksızın aktarılabileceğine yer verilmiştir. İlgili Kanun'un 9. Maddesinde ise, kişisel verilerin gerekli görüldüğü koşullar sağlandığı takdirde aktarım söz konusu olabileceğine değinilmiştir.

Kullanıcılara ait kişisel verilerin, yeterli düzeyde bilgi güvenliğini sağlayamayan Avrupa Birliği ekonomik alanı dışındaki ülkelere aktarılması ve paylaşılması, 95/46/EC sayılı direktifin 25. Maddesince yasaklanmıştır (Henkoğlu ve Yılmaz, 2013, s. 461). Avrupa Komisyonu, bu direktiften yola çıkarak kişisel verilerin kötü amaçla kullanılmasını engellemek ve yurtdışına ihraç edildiğinde verilerin korunmasını sağlamak amacıyla, ABD hükümetiyle birlikte SafeHarbor çerçevesini oluşturmuştur ("FTC", 2015). OECD'nin rehber ilkelerini baz alarak yedi temel ilkeye dayanan SafeHarbor sözleşmesi, gerekli koşulları içererek üye olan şirketin kullanıcılarının elde ettiği kişisel veriler ve bu verileri hangi amaçla kullanacağı hakkında bilgilendirerek, gerekli tüm bilgi güvenliği tedbirlerini ve önlemlerini almalarını üye ülkelere zorunlu kılmıştır (Ünsal, 2013, s.108; Henkoğlu ve Yılmaz, 2013, s.462). Avrupa Birliği Adalet Divanı ise, 6 Ekim 2015 tarihinde bu sözleşmeyi iptal etmiştir. İptal edilen bu sözleşmenin yerini ise, Avrupa Komisyonu'nun 12 Temmuz 2016 tarihinde hazırlamış olduğu Avrupa Birliği-Amerika Birleşik Devletleri Gizlilik Kalkanı çerçevesi almıştır (Borazan, 2015, s.206; "FTC", 2015). Gizlilik kalkanı çerçevesi ise, Atlantik'in her iki tarafındaki şirketlere kişisel veri aktarırken veri koruma gerekliliklerine uyma mekanizmasını ele almıştır ("Privacy Shield", t.y.).

2.5.5. Kişisel Verilerin Korunması

Gizlilik hakkı, entelektüel özgürlük için temel haktır (American Library Association-ALA, 2017). Diğer bir deyişle, gizlilik hakkı hükümet veya başkaları tarafından gözetleme ya da istenmeyen gözetimden arınmış bir okuma, değerlendirme ve geliştirme hakkı olmak üzere entelektüel özgürlük için temel bir hak olarak nitelendirilmektedir. Bu bağlamda, entelektüel özgürlüğün çerçevesini, özgür konuşma, özgür düşünme ve özgür hareket edebilme oluşturmaktadır. Gizlilik hakkının temelini insan hak ve özgürlüğünün

oluşturduğunu söyleyebiliriz. Hükümet ya da başkaları tarafından gözlem ya da istenmeyen gözetimden arınmış fikir ve inançları okuma, değerlendirme ve geliştirme hakkı olarak adlandırılan kişisel verilerin korunması hakkı Henkoğlu'na göre (2015a, s.129), kişinin rızası ya da yasal düzenlemelerde yer alan zorunlu haller dışında sınırlanamayan, vazgeçilemeyen ve devredilemeyen temel haklardan birisi olmakla beraber, kişinin özel hayatını ilgilendiren kişilik haklarının ve onurunun korunması olarak da nitelendirilen temel haktır. Ünsal (2013, s.103) ise kişisel verilerin korunmasını, bireyin şahsi verilerinin sınırsız bir şekilde elde edilmesi, kullanılması, işlenmesi ve transfer edilmesi karşısında bireyinkorunmasını amaçlayan ve bireyin kendisi hakkındaki enformasyon üzerinde tayin hakkı veren bir hak olarak tanımlamıştır.

Enformasyon çağı olarak da nitelendirilen günümüz çağında, veriler hem fiziki hem de elektronik ortamda işlenerek veri bankalarında depo edilmeye başlamıştır. Kamu ve özel kurumlarda işlenen ve depolanan bu verilerin ise temel bilgi varlığını, kişisel veriler oluşturmaktadır. Öte yandan, sosyal medya platformlarının ortaya çıkmasıyla beraberinde gelen veri artışı ve paylaşımı hayatımızda yeni bir çığır aşan büyük verinin gelişimiyle kişisel verilerin korunmasının üzerinde durmak bir hayli önem arz etmektedir. Dünya üzerinde yaşayan her bir tekil internet ve sosyal medya kullanıcısı, yaptıkları gezintiler sonucunda arkalarında izler bırakmaktadır. Bu izler gerek arama motorlarında kullandıkları sözcükler gerekse sosyal medya platformlarından yaptıkları paylaşımlar olabilmektedir. Ancak, kullanıcıların oluşturdukları her bir iz kendilerine ait kişisel veriler barındırabilmektedir. Bu verilerin gizliliğinin ve bütünlüğünün korunması ise veri koruma kanunlarının ayrı bir boyutunu oluşturmaktadır. Bunlara ek olarak, kamu kurum ve kuruluşlarında sürekli ve güncel olarak kaydedilen, işlenen, düzenlenen ve depolanan kişisel verilerin mahremiyetinin sağlanması, bilginin(kayıtların) gizliliğinin korunmasına temel teşkil edecektir. Diğer taraftan, bu kurumlarda kişisel verilerin korunması yasal düzenlemeler çerçevesinde işlenmektedir. Kamu kurum ve kuruluşlarında, kişisel verilerin korunması ile ilgili yasal düzenlemelerin uygulamaya konulmadığı düşünüldüğünde, bilgi ve belgelerin öznesi olan kişisel verilerin kolay bir şekilde herkes tarafından kullanılması anlamına gelmektedir. Bu durum ise, kişilerin özel hayatlarını tehlikeye atmaktadır. Bu sebeple, veri ihlallerinin önüne geçmek ve kişisel verilerin korunması amacıyla ulusal ve uluslararası alanda bildirge, sözleşme, kanun ve yönetmelikler oluşturulmuştur.

2.6. KİŞİSEL VERİLERİN YÖNETİMİNE YÖNELİK HUKUKSAL DÜZENLEMELER

Kişisel verilerin korunması alanında; kişisel verilerin korunması hakkının anayasal güvenceye kavuşturulması, kişisel verisi işlenen bireylerin haklarının kanun düzeyinde belirlenmesi, kişisel verilerin esas ilkelerine uygun olarak işlenmesi, kişisel veri kütüğü sahiplerinin sorumlulukları ile kişisel verilerin korunması konusunda etkin rol alacak tarafsız, bağımsız ve teknik olarak yeterli veri koruma otoritelerinin hayata geçirilmesi kişisel verilerin ulusal ve uluslararası alanda köşe taşlarını oluşturmaktadır ("TCDDK", 2013, s. 779). Bu bağlamda, özel hayatı gizliliği ve korunması çerçevesinde ulusal ve uluslararası alanda çalışmaların yapılması önem arz etmektedir.

2.6.1. Uluslararası Hukuksal Düzenlemelerde Kişisel Verilerin Korunması

Dünyada bilgi güvenliği ile alakalı pek fazla çalışma bulunmaktadır. Bunlar arasında, önemli etkiye sahip olan ve dünyanın çeşitli yerlerinde yürürlükte olan kanun ve yönetmelikler şöyledir:

- Kişisel Bilgilerin Korunması ve Elektronik Belge Kanunu (Personal Information Protection and Electronics Document Act), Kanada'daki özel sektör kuruluşlarının belirli durumlarda kişisel bilgileri nasıl topladıklarını, kullandıklarını ve işlediklerini düzenleyen mahremiyet kanunudur (PIPEDA, 2019).

- İngiltere'de 23 Mayıs 2018 tarihinde kraliyet onayı alan (Veri Koruma Kanunu 2018 (Data Protection Act- DPA, 2018), kişisel bilgilerin işlenmesi için düzenleyici hükümler içermektedir. Yedi bölümse ayrılan kanunda ele alınan konuların çoğu Genel Veri Koruma Tüzüğü'ne (General Data Protection Regulations – GDPR) bağlı tutulmuştur ("DPA", 2018).

- Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (The Payment Card Industry Data Security Standard - PCI DSS), kart sahipleri için veri güvenliğini teşvik etmek ve veri güvenliği önlemlerinin küresel olarak yaygın bir biçimde

benimsenmesini kolaylaştırmak için geliştirilmiştir. PCI DSS aynı zamanda hesap verilerini korumak için tasarlanmış teknik ve operasyonel gereksinimlerin temelini oluşturmaktadır (PCI DSS Counsil, 2018, s.5).

- Genel Veri Koruma Tüzüğü (General Data Protection Regulation) (2016/679), (madde 1) kişisel verilerin işlenmesiyle ilgili gerçek kişilerin korunmasına ilişkin kuralları ve kişisel verilerin serbest dolaşımına ilişkin kuralları ortaya koymaktadır.[7]

- Federal Finansal Kurumlar Sınav Konseyi'nin (The Federal Financial Institutions Examination Council's - FFIEC) güvenlik rehberleri, bir finansal kurumun bilgi sistemlerine yönelik güvenlik risk seviyelerini değerlendirmek için gerekli faktörleri ele alır ve denetçilere rehberlik sağlar (FFIEC, 2016, s.1).

- Finansal Hizmetler Modernizasyonu Kanunu 1999 olarak bilinen Gramm-Leach-Bliley Kanunu (Gramm - Leach - Bliley Act - GLBA), finansal kurumların topladığı, elinde tuttuğu ve uyguladığı kişisel bilgilerin güvenliğini ve gizliliğini korumak için kurallar ortaya koymaktadır (GLBA, 1999).

- 1998 tarihli İngiltere Veri Koruma Kanunu (The U. K. Data Protection Act), bireylerle ilgili bilgilerin işlenmesini ve yönetilmesini düzenlemek için yeni hükümler ortaya koymuştur (DPA, 1998).

- Sağlık Sigortası Taşınabilirliği ve Hesap Verilebilirlik Kanunu 1996 (Health Insurance Portability and Accountability Act 1996 - HIPPA), tıbbi kayıtların korunması ve sağlık sigortası kapsamındaki sınırlamaları ele almak için oluşturulmuştur (HIPPA, 1996).

- Aile Eğitim Hakları ve Mahremiyet Kanunu (The Family Educational Rights and Privacy Act- FERPA), öğrenci eğitim kayıtlarına ilişkin hukuksal düzenlemeler içermektedir (FERPA, 1974).

[7]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

- Güvenlik İhlali Bildirim Kanunları (Security Breach Notification Laws), kâr amacı gütmeyen kuruluşların ve devlet kurumlarının, kişisel veya tanımlayıcı bilgileri içeren bilgilerin güvenlik ihlallerini kişilere bildirmelerini gerektiren özel veya resmî kurumların hazırlamış oldukları kanunlardır.[8]

- Avrupa İnsan Hakları Sözleşmesinin İlgili Hükümleri: Roma'da 4 Kasım 1950 tarihinde imzalanan ve 3 Eylül 1953'te yürürlüğe giren sözleşme, kişisel verilerin işlenmesi hakkında doğrudan bir düzenleme içermemektedir. Sözleşmenin 8.Maddesinde sadece bireylerin özel ve aile hayatına karşı yapılan düzenlemeler yer almaktadır (108 Sayılı Kişisel Verilerin, 2016, s.11).

- 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi: 1981 yılında kabul edilen sözleşmenin önemli tarafı, kişisel verilerin korunması konusunda hukuksal bağlayıcılığı olan ilk uluslararası belge niteliğine sahip olmasıdır (Boz, 2014, s.46). Toplamda 27 maddeden oluşan sözleşme, kişisel verilerin otomatik sistemler yoluyla işlenmesi karşısında bireylerin haklarının korunması yönünde veri korumanın güçlendirilmesini amaçlamıştır. Kapsam olarak sözleşme, sınır ötesi bilgi akışının yeniden yapılandırılması ve bilgilerin otomatik işleme tabi tutulması ilkelerini kişisel veri odaklı olarak düzenlemektedir (Dinkçi, 2014, s.28).

- 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi : 24 Ekim 1995 tarihinde kabul edilen direktif, gerçek kişilerin temel hak ve özgürlüklerinin korunmasını uyumlaştırmayı ve kişisel verilerin üye devletler arasında serbest akışını sağlamayı amaçlamaktadır (Avrupa Konseyi, 2016). Direktif çerçevesinde ise, kişisel verilerin işlenmesinin yasallaşması hakkında genel kurallar, kişisel verilerin üçüncü ülkelere transferine dair ilkeler konu olarak işlenmiştir. 95/46/EC sayılı direktif, Avrupa Birliği'nde kişisel verilerin

[8]National Conference of State Legislatures. (2018). *Security Breach Notification Laws*. 21 Ağustos 2019 tarihinde http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspxadresinden erişildi.

korunmasına yönelik çıkarılan ilk düzenleme olarak direktifler arasında yer almaktadır (Polater, 2019, s.3).

- 181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol: Taraf devletler ülkelerinde uygulamak üzere kişisel verilerin korunması alanında sorumluluklarını tam bağımsızlıkla tamamlayacak denetleyici makam kurmayı üstlenmiştir. Türkiye, söz konusu protokolü 8 Kasım 2001 tarihinde imzalamıştır ve söz konusu protokol 29703 sayılı ve 5 Mayıs 2016 tarihli Resmî Gazete'de yayımlanarak iç hukuka dâhil edilmiştir (KVKK, 2018, s.4). Veri koruma otoriteleri ve sınır ötesi veri transferine ilişkin hükümleri kabul eden sözleşme, üye ülkelerde uyruğu veya ikametgâhı ne olursa olsun bireylerin, temel hak ve hürriyetleri ile kişisel nitelikteki verilerinin otomatik işlemeye tabi tutulması karşısında mahremiyet haklarının güvence altına alınmasını amaçlamaktadır (Akıncı, 2019, s.62).

- 2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR): Katı kurallar içeren bir düzenleme olarak nitelendirilen tüzük, Avrupa Birliği'nin kişisel verilerin korunması alanında ortaya çıkan gereksinimleri karşılamak amacıyla oluşturulmuştur. 2016 yılında kabul edilen tüzük, 25 Mayıs 2018 tarihinde yürürlüğe girmiştir. Tüzük çerçevesinde (Madde 1), kişisel verilerin işlenmesiyle bağlantılı gerçek kişilerin korunmasına yönelik ilkeler ve kişisel verilerin serbest dolaşımına yönelik serbest ilkeler ele alınmaktadır (Gdpr.eu, 2019).

- Diğer düzenlemeler: Konuyla bağlantılı olarak, OECD'nin 23 Eylül 1980 tarihinde yayınladığı *"Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*" ve Birleşmiş Milletler'in 14 Aralık 1990 tarihinde yayınladığı "Bilgisayarlarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri - Guidelines for the Regulation of Computerized Personal Data Files" yer almaktadır.

Uluslararası alanda bilgi güvenliğine yönelik olarak hazırlanan rehber, yönetmelik, direktif, kanun ve standartlar incelendiğinde, ilgili dokümanların sadece kişisel verilerin mahremiyetine ve korunmasına yönelik olarak düzenlenmediği görülmektedir. Diğer bir deyişle, kamu kurumlarında ve özel sektörlerde kişisel bilgilerin işlenmesi, toplanması, kullanılması, gibi kişisel verilerin yönetimine yönelik düzenlemelerle birlikte, farklı sektörlere (sağlık, eğitim, finans, iletişim vb.) yönelik düzenlemelerin olduğu ortaya çıkmaktadır.

2.6.2. Türkiye'deki Hukuksal Düzenlemelerde Kişisel Verilerin Korunması

- 18/10/1982 tarihli ve 17863 Sayılı Türkiye Cumhuriyeti Anayasası'nın özel hayatın gizliliği ile ilgili olan 20.Maddesine (T.C. Anayasası, 1982, s.135) 2010 yılında ek fıkra getirilmiştir. Söz konusu fıkrada şu hükme yer verilmiştir:

> *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak: kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."*

- 5237 Numaralı TCK'nın, üçüncü kısım/onuncu bölümü bilişim alanında suçlar başlığıyla ele alınmıştır. Bu kapsamda, (Madde 243 ve sonrası) bilişim sistemine girme, sistemi engelleme, verileri yok etme veya değiştirme, yasak cihaz ve programlar, kredi kartlarının veya baka kartlarının kötüye kullanılması ve tüzel kişiler hakkında güvenlik tedbiri uygulanması gibi hukuki ve cezai yaptırımlara kanun içeriğinde değinilmiştir (TCK, 2004, s. 9024). Kişisel verilerin korunması ile dolaylı olarak ilişkilendirilen kanun'da, kredi veya banka kartlarının kötüye kullanılması, verilerin yok edilmesi ya da değiştirilmesi bilgi güvenliğinin sağlanmasına örnek olarak gösterilebilmektedir.

- 5809 Numaralı Elektronik Haberleşme Kanunu'nun 4.Maddesi'nin 1. Fıkrasında, ilgili mercilerce elektronik haberleşme hizmetlerinin sunulmasında ve bu hususta gerçekleştirilecek olan uygulamalarda dikkate alınacak kurallar sunulmuştur. Bu ilkeler altında, (l) haberleşme gizliliğinin ve bilgi güvenliğinin gözetilmesi hükmüne yer verilmiştir (Elektronik Haberleşme Kanunu, 2008, s.10382).

- Bilgi Teknolojileri ve İletişim Kurumu'nun hazırlamış olduğu 13 Temmuz 2014 tarihli ve 29059 Sayılı 'Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği', (Md. 1) bilgi güvenliğinin ve şebeke güvenliğinin sağlanmasına yönelik olarak işletmecilerin esas yükümlülüklerini belirlemek amacıyla oluşturulmuştur (Elektronik Haberleşme, 2014). Söz konusu yönetmelik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun 4., 6., 12. ve 60. Maddeleri esas alınarak hazırlanmıştır (Elektronik Haberleşme, 2008).

- 6698 Sayılı Kişisel Verilerin Korunması Kanunu, 26 Aralık 2014 tarihinde "Kişisel Verilerin Korunması Kanunu Tasarısı" Türkiye Büyük Millet Meclisi Başkanlığına sunulmuştur. Tasarının ortaya çıkarılmasına genel gerekçe olarak, Türkiye'de kişisel verilerin işlenebilmesi hususunda etkin bir denetim mekanizmasının bulunmaması ve özel bir kanunun olmaması, Avrupa Birliği'ne üyelik sürecinde veri koruma alanındaki kanuni boşluk, sağlık kuruluşlarında hastalara ilişkin verilerin tutulmasına ilişkin kanuni dayanağın olmayışı ve verilerin korunmasını sağlamaya yönelik yeterli önlemlerin alınmaması gibi örnekler gösterilmiştir. Tasarının temel amacı ise, kişisel verilerin çağdaş standartlarda işlenmesi ve güvence altına alınmasıdır. 24 Mart 2016 tarihinde kanunlaşan tasarı, 6698 Numaralı Kişisel Verilerin Korunması Kanunu 29677 sayılı ve 7 Nisan 2016 tarihli Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. 95/46/EC Sayılı Yönerge esas alınarak hazırlanan kanun, kişisel verilerin korunmasına yönelik ve genel nitelikli ilk kanuni düzenleme özelliğine sahip olmuştur (Polater, 2019, s.4).

- Sağlık Bakanlığının merkez ve taşra teşkilatı birimleri ile bunlara bağlı olarak faaliyet göstermekte olan sağlık hizmeti sunucuları ile bağlı ve ilgili kuruluşları tarafından süreç ve uygulamalarda uyulacak usul ve esasları bir karara bağlayan Kişisel Sağlık Verileri Hakkındaki Yönetmelik, 21 Haziran 2019 tarihinde yürürlüğe girmiştir. Yönetmelik 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümleri esas alınarak hazırlanmıştır. Bu çerçevede, kişisel sağlık verilerine

erişim, kişisel sağlık verilerinin gizlenmesi, imha edilmesi ve aktarılması, bilimsel amaçlarla işleme ve sağlık verisi, veri güvenliği gibi konular yönetmelik kapsamında (madde 1) ele alınmıştır (Kişisel Sağlık Verileri, 2019).

- 6 Temmuz 2019 tarihli ve 30823 Sayılı 'Bilgi ve İletişim Güvenliği Tedbirleri' Genelgesi, kamu kurum ve kuruluşlarında kritik türdeki verilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunmasını sağlamak için milli güvenliği tehdit edebilecek ve kamu düzenini bozulmasının önüne geçebilmek amacıyla gerekli tedbir ve önlemleri içermektedir. Yirmibir maddeden oluşan genelgede, kamu kurum ve kuruluşlarında kritik veri olarak nitelendirilen tüm bilgi ve bilgi varlıklarının korunmasına yönelik şartlar getirilmiştir (Bilgi ve İletişim…, 2019).

- 5237 sayılı Türk Ceza Kanunu, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 17. Maddesi (1) bendinde göre, "kişisel verilere ilişkin suçlar bakımından 26/09/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140 ıncı madde hükümlerinin uygulanacağına" yer verilmektedir (Kişisel Verilerin Korunması Kanunu, 2016). 5237 sayılı Türk Ceza Kanunu'nunda göre kişisel verilerin hukuka aykırı olarak işlenmesine yönelik uygulanacak hükümler 135.Madde de yer alırken, tüzel kişiler hakkında güvenlik tedbiri uygulanması 140. Maddede yer almaktadır (TCK, 2004, s.9001-9002).

- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, Yönetmeliğin amacı 1. Maddede, "otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları ortaya koymak" şeklinde belirtilmiştir (Kişisel Verilerin…, 2017).

- Kişisel Sağlık Verilerin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik, Kişisel sağlık verilerinin işlenmesi ve mahremiyetinin sağlanması hakkında yönetmeliğin amacı Bölüm 1/Madde 1'de, "kişisel verilerin korunmasına ve veri mahremiyetinin sağlanmasına, kişisel sağlık verilerini toplama, işleme, aktarma, bu verilere erişim için kurulacak sisteme, kişisel sağlık

> verisi kaydı tutulan sistemlerin güvenliği ve denetimi ile sağlık hizmeti sunumundaki personel hareketlerinin Bakanlığa bildirilmesine ilişkin işlemlerde uyulacak usul ve esasları düzenlemek" şeklinde ifade edilmiştir ("Kişisel Sağlık Veri….", 2016).

Ulusal anlamda veri koruma konularının 80'li yıllarda gündeme geldiği görülmektedir. Özellikle, kişisel verilerin mahremiyetine yer veren 1982 Anayasası, Türkiye'de kişisel verilerin korunmasına dair atılmış önemli adımlardan bir tanesidir. Diğer taraftan, bu anayasaya eklenen ek fıkra ile bireylerin hakları güvence altına alınmıştır. Bilgi güvenliği alanında yaşanan diğer gelişmelerle, farklı sektörlere (sağlık, telekomünikasyon ve haberleşme, internet, bilişi vb.) yönelik olarak hazırlanan düzenlemelerde bilgi güvenliği konusunun üzerinde durulmuştur. Aynı zamanda, kamu kurum ve kuruluşları için 2019 yılında hazırlanan Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi bilgi güvenliğine yönelik atılacak adımlara katkı sağlamaktadır. Ancak, Türkiye'deki tüm gelişmelere rağmen söz konusu hukuksal düzenlemelerde bilgi güvenliğini ilgilendirecek konulara ayrı ayrı yer verildiği görülmektedir. Konu ile ilgili olarak tüm sektörleri ve kurumları kapsayacak 'Bilgi Güvenliği Yasası'nın olmadığı görülmektedir. Bu nedenle, bilgi güvenliğinin önemi üzerinde durularak konunun mercek altına alınması gerekmektedir.

Türkiye'de bilgi güvenliğinin sağlanması ve kişisel verilerin korunması hususunda diğer kurum ve kuruluşlara örnek teşkil edebilecek bir çalışma, Sağlık Bilgi Sistemleri Genel Müdürlüğü'ne bağlı Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı tarafından gerçekleştirilmiştir. 11 Ekim 2011 tarihinde kararlaştırılarak yürürlüğe giren 663 numaralı Kanun Hükmünde Kararnamede yer alan görevler çerçevesinde, Bilgi Güvenliği Yönetim Sistemleri Birimi Ankara'da[9] kurulmuştur. Bu kapsamda birimde, bilginin işlenmesi süreçlerinde içeriden ve dışarıdan gelebilecek her türlü tehlike ve saldırılara karşı her türlü önlemi alarak bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak amaçlanmıştır. Hedeflenen bu amaçla beraber, Sağlık Bakanlığı'na bağlı kurum ve kuruluşların kullanabileceği bir web sayfası tasarlanmıştır.[10] Bunlara ek olarak, kişisel verilerin korunması konusu ilgili yönetmelik, politika ve kılavuzlarda yayınlanmıştır.[11]

[9]Söz konusu bilgi, 15 Mayıs 2019 tarihinde Sağlık Bilgi Sistemleri Genel Müdürlüğü Bilgi Güvenliği Birimi ile yapılan telefon görüşmesi sonucu elde edilmiştir.
[10] Bkz. https://bilgiguvenligi.saglik.gov.tr/
[11] Bkz. https://dosyamerkez.saglik.gov.tr/Eklenti/25755,bilgi-guvenligi-politikalari-kilavuzu-ekler-haricpdf.pdf?0 https://dosyamerkez.saglik.gov.tr/Eklenti/15584,bilgi-guvenligi-politikalari-yonergesi20180502pdf.pdf?0

Kişisel verilerin korunması ile ilgili bir diğer çalışma ise, Türkiye Bilimsel ve Teknolojik Araştırmalar Kurumu (TÜBİTAK) Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü tarafından gerçekleştirilen sosyal sorumluluk projesi olmuştur. 'Bilgimi Koruyorum E-öğrenme Projesi' adıyla anılan proje kapsamında, bilgi güvenliği, internet ve ağ güvenliği, bilgisayar ve erişim güvenliği, tehditler ve koruma yöntemleri gibi konularda herkesin erişebileceği temel bilgi güvenliği eğitimi sistem olarak tasarlanmıştır. 2013 yılında Türkiye Cumhurbaşkanlığı Devlet Denetleme Kurulu (TCDDK) tarafından "*Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ile Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları*" başlıklı denetleme raporu yayınlanmıştır. Rapor çerçevesinde, bilgi güvenliği ve kişisel verilerin korunmasıyla ilgili kavramsal çerçeve, uluslararası düzenlemeler, kişisel verilerin işlenmesi ve korunması ile ilgili mevzuat ve değerlendirme, karşılaştırmalı ülke örnekleri, Türkiye'deki mevcut durum üzerinde durularak Türkiye'deki altı[12] kamu kurumunda denetim çalışmaları yapılmıştır. Kurumlarda yapılan analiz ve denetim çalışmaları sonucunda şu eksiklikler tespit edilmiştir ("TCDDK", 2013, s.814-815):

- Kişisel verilerin korunması ve bilgi güvenliği konusunda billinç eksikliği,
- Kişisel verilerin korunmasının kamu bilgi sistemleri ile sınırlı olmaması, özel kesimde kişisel verilerin karşı karşıya bulunduğu risklerin gittikçe artması ve buna karşılık özel kesimde kişisel verilerin korunmasına ilişkin mevzuat ve denetim boşluğunun bulunması,
- Bilgi sistemlerinin güvenliğine yeterince önemin verilmemesi,
- Kurumsal yapılanma eksikliği ve mevzuat alanındaki boşluk,
- Kamu sektöründe bilgi sistemleri güvenliği ile kişisel verilerin korunması hususunda büyük önem taşıyan iç kontrol ve iç denetim müesseselerinin işlememesi tespit edilmiştir.

Afyonluoğlu, 16-18 Kasım 2018 tarihinde Antalya'da "Üniversiteler Teknoloji Zirvesi 2018" başlığıyla düzenlenen etkinlikteki sunumunda, üniversitelerde kişisel veriler

[12] Söz konusu kurumlar, Adalet Bakanlığı, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, Gelir İdaresi Başkanlığı, Sosyal Güvenlik Kurumu, Sağlık Bakanlığı,Tapu ve Kadastro Genel Müdürlüğünden oluşmaktadır.

ışığında üniversite, öğrenci ve öğretim görevlileri ilişkilerinde yüküm ve sorumlulukların kime ait olduğu, verinin ifşası durumundaki sorumlulukların neler olduğu, verinin imhasına ilişkin sorumlulukların neler olduğuna dair örnekler ve sorular üzerinden konuyu ele almıştır. Kişisel verilerin korunması üzerine gerçekleştirilen başka bir etkinlik ise, KVKK 28 Ocak Veri Koruma Günü Konferansı üzerine olmuştur. Konferans kapsamında Afyonluoğlu (2019) tarafından ele alınan E-Devlette Kişisel Verilerin Korunması başlıklı sunumda, e-devlette veri döngüsü, e-devlet hizmetlerinde veriler, veri haritalamanın gereksinimi ve kişisel verilerin imhasının kurumlara yansıması gibi konular üzerinde durulmuştur.

2.6.3.Türkiye Kişisel Verileri Koruma Kurumu

24 Mart 2016 yılında yayınlanan 6698 Sayılı Kişisel Verilerin Korunması Kanunu'yla beraber, Türkiye'de kişisel verilerin korunmasına yönelik ilk defa kurumsal mekanizma oluşturulmuştur (Kutlu ve Kahraman, 2017, s.57). Kurul bağımsız olarak AK'nin 108 sayılı Sözleşmesi ve Avrupa Birliğinin 95/46/EC sayılı Direktifine uygun olarak kurulmuştur (KVKK, 2017). Bu açıdan bakıldığında kurumun ortaya çıkış sebepleri arasında, Türkiye'nin kişisel verilerin korunmasını konu alan uluslararası antlaşmalara taraf olması, AB'ye üye olma sürecinde AB ile hukuksal uyum sağlanmak istemesi, ulusal düzenlemelerinde kişisel verilerin korunmasına ilişkin hükümlere yer vermesi gibi hukukî sebeplerin yanında teknolojik gelişmelerin artışıyla kişisel verilerin serbest dolaşımı ve idarenin kişisel verileri gerektiği gibi korumaması teknolojik sebeplerin yer aldığı görülmektedir (Gürsel ve Düğmeci, 2018, s.318). Kurumun oluşmasında ortaya çıkan diğer sebepler ise, Türkiye'nin AB'ye üye olma sürecinde kişisel verilerin korunmasına yönelik kanunun eksik olması gibi siyasi ve elektronik ticaretin dünya çapında yaygınlaşması gibi ekonomik nedenleri bulunmaktadır. KVKK'nın görevleri ise, Kişisel Verileri Koruma Kanunu'nun (2016) 20. Maddesinde şu şekilde tanımlanmaktadır:

- Sorumluluk alanı itibariyle, düzenlemeleri ve mevzuattaki değişiklikleri izlemek, değerlendirme ve önerilerde bulunmak, inceleme ve araştırmalar yapmak ve yaptırmak,
- Kişisel verilerle ilgili uluslararası gelişmeleri takip etmek ve değerlendirmek, rol alanına giren konularda uluslararası kuruluşlarla koordinasyon ve eş güdüm toplantıları yapmak,

- Yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna sunmak,
- Gereksinim duyulması hâlinde, sorumluluk alanına giren konularda kamu kurum ve kuruluşları, meslek örgütleri, sivil toplum kuruluşları, veya üniversitelerle koordinasyon yapmak,
- Kanunlarla verilen diğer sorumlulukları yerine getirmektir.

ÜÇÜNCÜ BÖLÜM

ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLERİN YÖNETİMİ

3.1. ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ

Yaşadığımız çağ bilgi çağı, içinde yer aldığımız toplum ise, bilgi toplumudur. Bu toplumda en önemli role sahip kurumlardan biri üniversite kurumlarıdır. Bunun sebebi ise, üniversitelerin bilgi ekonomisinin hammaddesi olan bilginin oluşumundan ve dağıtımından sorumlu temel kurumlar olmasıdır (Vardal, 2009, s.20). Bilgi ve bilgi varlıkları yükseköğretim kurumlarının temel hazinelerinden birisidir. Bu sebeple, bilgi varlıklarının korunabilmesi için bilgi güvenliğinin en üst seviyede sağlanması gerekmektedir. Aynı zamanda bilgi ve iletişim teknolojilerinin dünyamızda yarattığı değişiklikler yanında bir takım risk unsurlarını da beraberinde getirmektedir. Bilgi güvenliğinin sahip olduğu gizlilik, bütünlük ve kullanılabilirlik gibi temel bileşenlerin risk kavramına dâhil edilmesi ise, bilgiyi tehlikeli bir noktaya taşımaktadır. Kurum ve kuruluşların bünyesinde barındırdığı veri ve bilgileri koruyabilmesi için öncelikle bilgi güvenliğinin öneminin bilincinde ve farkında olması gerekmektedir.

Bilgi güvenliğinin sağlanması gereken en önemli kurumlardan birisi şüphesiz ki yükseköğretim kurumlarıdır. Çünkü bu kurumlarda veri ve bilgi akışı sürekli olarak devam etmektedir. Bunun yanı sıra, bu kurumların eğitim ve öğretim kurumları olması güvenliğin önemini ve değerini ikiye katlamaktadır. Bu kurumları diğer kurumlardan ayıran önemli bir özellik ise, verinin devamlı işlenmesi, üretilmesi, kullanılması ve paylaşılmasıdır. Temelinde bireylerin yer aldığı, diğer bir deyişle, akademisyen, idari personel ve öğrenci gibi farklı rollerdeki bireylerden oluşan bir kitleye sahip olan bu kurumlarda bilgi güvenliğinin çok yönlü olarak sağlanması önemli görülmektedir. Bu kurumların birimleri arasında yer alan kütüphaneler de bilgi ile ilgili etkileşimin aktif olarak sağlandığı yerlerden biridir. Üniversite kütüphanelerinin bünyesinde temel bilgi kaynaklarını içermesi ve bununla beraber kullanıcılara ilişkin veri kayıtlarını tutması bilgi güvenliği risklerini beraberinde getirmektedir. Buradan hareket edilerek, çalışmanın bu bölümünde üniversite kütüphanelerinde bilgi güvenliğinin ne olduğuna, bilgi

güvenliğinin bileşenlerine ve standartlarına ve üniversite kütüphanelerinde bilgi güvenliğinin nasıl ele alınabileceğine değinilecektir.

3.1.1. Bina Güvenliği (Fiziksel Güvenlik)

Bilgi ve belge merkezlerinin oluşumu için temel ögelerin 'bina, koleksiyon, kullanıcı, personel ve bütçe" olduğu bilinmektedir. Bu noktada, bir kütüphanenin var olması için ilk olarak binanın olması gerekmektedir (Güneş, 2009, s.4; Güneş, Bozkurt, Sönmez ve Çakır, 2015, s.223). Gelişen dünyada her alanda yapılan değişiklikler ve yenilikler kütüphaneleri de bu sürecin bir parçası haline getirmiştir (Değer ve Öztürk, 2017, s. 2577).

Üniversite Kütüphaneleri Çalışma Grubu'nun hazırlamış olduğu bir çalışmada (2014, s.4), kütüphane binalarının önemine, sorunlarına ve çözüm önerilerine yer verilmiştir. Bu kaynakta, kütüphane binalarının mimari yapısının ve teknik donanımlarının modüler sistemde olması gerektiğine ve en az çabayla en etkin kaynak yönetimine olanak sağlayan akıllı binalar olarak tasarlanması gerektiğine değinilmiştir (Üniversite Kütüphaneleri Çalışma Grubu, 2014, s.4). Çalışmada dikkat çeken bir nokta ise, üniversite kütüphanelerinin eğitim, öğretim ve araştırmayı gerektiği biçimde destekleyecek duruma gelebilmeleri için üniversite kütüphanelerine gerçekleştirilebilir bir standart konulması ve bu standartların denetlenmesi ile mümkün olacağına vurgu yapılmıştır (Üniversite Kütüphaneleri Çalışma Grubu, 2014, s.28). Bu konuda Kolej ve Araştırma Kütüphaneleri Derneği (Association of College & Research Libraries – ACRL) (2018, s. 12), kütüphanelerin kullanıcıların etkileşimli olduğu alanlarda, yeni bilgi yaratmayı ve öğrenmeyi kolaylaştırıcı ve çalışmaya ve araştırmaya elverişli emniyetli ve güvenli fiziksel ve sanal ortamlar sağlaması gerektiğini ifade etmiştir.

Kütüphane binasının boyutları ve özellikleri üniversitenin kendi ihtiyaçlarına ve kaynaklarına göre belirlenmektedir (Çelik ve Uçak, 1993, s.118). Kütüphane binalarının önemli yapı taşlarından birisi de kullanıcı sağlığı ve güvenliğini sağlanmasıdır. Bu bağlamda, kütüphane merdivenlerinin durumu, deprem riski için raf sabitleme, halıların ömürleri, erken uyarı sistemleri, bina otomasyon sistemleri bu süreç içerisinde değerlendirilmesi gereken hususlardır (Özel, 2018). Bina güvenliği kavramı yalnızca yapı

güvenliği olarak düşünülmemelidir. Bina güvenliği, yapı, mekân ve araç-gereç(malzeme) üçlüsü bağlamında düşünülebilir.

Üniversite kütüphanelerinin binaları insan, çevresel, biyolojik ve doğal afet gibi pek çok risk faktöründen etkilenmektedir. Diğer bir deyişle, kütüphanelerde bir acil durum meydana geldiğinde tehlike ve risk unsurları da artış göstermektedir. Zincirleme kaza olarak adlandırılan bu olaya örnek verilirse, bir kütüphane binası depremden etkilendiğinde, yapısal ve yapısal olmayan elemanlar zarara uğramakta, kitap dolapları ve rafları devrilmekte, kitap koleksiyonları hasar görmekte, insanlar yaralanmakta ya da hayatını kaybetmekte, altyapı zarar görmekte, yangınlar çıkabilmekte, elektrik su doğalgaz gibi yaşamsal ihtiyaçlar kesintiye uğramakta, kütüphane/müze bir müddet kapalı kalacağından operasyon faaliyetleri durmaktadır (Kuzucuoğlu, 2016, s.125-129). Bu nedenle, kütüphanelerde acil durum planlarının yapılması bina-kullanıcı ve personel güvenliğinin sağlanmasında öncelikle şu çalışmalar yapılmalıdır (Kuzucuoğlu, 2014, s. 24; 2016, s.129):

- "Kütüphane anahtar alanlarının (idari ofisler, okuma salonu, süreli yayınlar bölümü vb.) belirlenmesi ve bu alanlardaki tehlikelere yönelik acil durum planlarının hazırlanması,
- Personel, kullanıcı ve koleksiyonlara yönelik tahliye planlarını yapılması ve acil durum planlarının yapılması,
- Kütüphanenin bulunduğu alanın jeolojik açıdan durumu ile binanın statik açıdan değerlendirilmesi,
- Kütüphane malzemesini hasar riskini en aza indirici önlemler,
- Personelin ve kullanıcının güvenliğini sağlayıcı önlemler"

Üniversite kütüphane binaları tasarlanırken özel bir önem verilmelidir. Bu konuda ise, üniversite kütüphanelerinin, kütüphane binası olarak bağımsız bir yapıda hizmet vermesi gerekmektedir. Bu bağlamda, öncelikle yöneticilerin bir mimar ile iş birliği halinde olması gerekmektedir. Mimarın, kütüphanenin üniversitenin merkezine olan konumu, kütüphanenin çevresel koşulları vb. özellikleri dikkate alarak bina tasarımını yapması gerekmektedir. Aynı zamanda, mimarın üniversite kütüphanelerinin biçimi, kütüphanede verilecek hizmetler, kütüphane personelinin sayısı, kütüphanede hangi tür kaynakların yer alacağı, koleksiyondaki yayınların ve kullanıcı sayısının gelecekte ne oranda artabileceği, kullanıcı sayısı ve kullanım biçimi, gibi konularda bilgi sahibi olması önem taşımaktadır (Çukadar, Gürdal, Çelik ve Kahvecioğlu, 2011, s. 2427). Buna ek olarak,

bina plan ve tasarım aşamasında doğal afet ve herhangi bir risk durumuna karşılık fizibilite çalışmasının ve mekânsal organizasyon modelinin yapılması gerekmektedir. Daha sonra ise, kütüphanenin iç donatım unsurlarının tasarlanması lazımdır. Ancak, burada kütüphane içerisinde kullanılacak olan malzeme ve donatıların 'ergonomik' bir şekilde tasarlanması önem taşımaktadır. Çünkü insanın en iyi çalışma ortamını araştıran ergonomi, bir işyerinde verimliliği, güvenliği ve konforu arttırmayı amaçlamaktadır. Bununla beraber, giriş ve hizmet alanları, bankolar, katalog alanları, kart dolaplarının boyutları, okuma alanları, mobilyalar, aydınlatma, iç hava koşulları ve geleceğe yönelik önlemlerin tümü ergonomik verilerin ve düzenlemelerin ışığında sağlıklı kütüphane mekânları yaratabilecektir (Öz, 1992, s.164).

Türkiye'deki kütüphane binalarında kullanıcı ihtiyaç ve beklentilerini yeteri kadar karşılayamamakla birlikte hizmet sunumlarında da ciddi sorunlar yaşanmaktadır. Buna ek olarak, kütüphane mimarileri kuruluş amaçlarına ve hizmet sundukları kullanıcı kitlesinin gereksinimlerine göre tasarlanmamıştır. Bu bağlamda, yeni yapılacak olan kütüphane binaları ile iyileştirilmesi yapılacak olan üniversite kütüphaneleri, kullanıcıların rahat ve güvenli bir şekilde kullanabilecekleri "Yaşayan Kütüphane" konsepti içinde yapılandırılmalı ve hizmete sunulmalıdır (Yıldız, 2017, s.424). Çalışan ve kullanıcı sağlığını etkileyen fiziksel ve biyolojik etken olmak üzere iki farklı etken bulunmaktadır. Fiziksel etkenler sıcaklık, toz ve neme bağlı olarak ortaya çıkarken biyolojik etkenler bakteriler, virüsler, mantarlar, küfler gibi mikrobiyolojik/makrobiyolojik tehlikelerden oluşmaktadır (Güneş ve diğerleri, 2015, s.224). Kütüphanelerde kalitesiz iç hava koşulları, iklimlendirme sisteminin olmayışı, ısıtma ve havalandırma sistemlerinin kötü oluşu kullanıcıların ve çalışanların çalışma verimini düşürebilmekte veya sağlık sorunlarının yaşanması kütüphane materyalinin fiziksel, biyolojik ve kimyasal nedenlerle bozulabilmesine neden olmaktadır (Güneş ve diğerleri, 2015, s.225). Kuzucuoğlu'na göre (2014, s.33), "kütüphane binalarında kütüphane malzemesini bulunduran kitaplıkların devrilmesi, tavan elemanlarının (aydınlatma ve eğitim amaçlı teçhizat dâhil) olası bir deprem anında düşmesi, tehlikeli malzemelerin sabitlenmemesi/yanlış depolanması, yangın riski iklimlendirme cihazları ve kablolama, yangın söndürme sistemlerinin yetersiz standartlarda olması sıhhi tesisat boruları ve elektrik tesisatı (boru ve kablo sistemleri) kaynaklı risklerin meydana gelme olasılığı genel sorunlar olarak öngörülebilmektedir".

‘Kamusal Alan Olarak Bilgi Merkezleri ve Yenilikçi Yaklaşımlar” başlığıyla yayınlanan bir eserde, kamusal mekân olarak adlandırılan kütüphane binalarında engelli kullanıcılara yönelik tasarım ilkelerine yer verilmiştir. Ataşehir Adıgüzel Meslek Yüksekokulu Öğretim Üyesi Küçükcan ve Uluslararası Kıbrıs Üniversitesi Öğretim Üyesi Öztürk’ün hazırlamış olduğu makalede (2017, s.306), kütüphanelerde temel ilkenin tüm kullanıcılar için bilgiye erişimde fırsat eşitliğinin oluşturulmasından söz edilmiştir. Nitekim çalışmada kütüphanelerin bilgi ve iletişim teknolojileriyle birlikte değişen kütüphaneler kavramına dâhil olması gerektiğine ve bu nedenle kütüphanelerin verilerin toplandığı, üretildiği, erişiminin kolaylaştırıldığı ve çeşitlendirildiği ve toplumsal ve kamusal yaşamda birleştirici ve buluşturucu bir mekâna dönüştüğü ifade edilmiştir (Küçükcan ve Öztürk, 2017, s.295-299). Çalışmanın ‘Kütüphane binası dış ve iç mekân tasarımı’ bölümünde kütüphane binaları için tasarım özellikleri (Küçükcan ve Öztürk, 2017, s.315-317) ise kütüphane binaları tasarlanırken göz önünde bulundurulmalıdır.

Yıldız (2017, s.53), güvenliğin toplumsal bir olgu olması ve insanın fiziksel bir ortamdan bağımsız düşünülemeyeceğinden hareket ederek, fiziksel güvenliğin her türlü güvenlik önlemininin ayrılmaz bir parçası olduğunu vurgulamıştır. Bu bağlamda ise, yangın ve duman, su, yer hareketleri, fırtınalar, sabotaj ve kurum mülkünün bilinçli olarak tahrip edilmesi, patlamalar, binanın yıkılma ihtimali, zehirli malzemeler, kesintiler, iletişim kesintileri, malzeme kaybı, personel kaybı bir kurumda güvenliği tehdit eden unsurlar arasında yer almaktadır. Güvenliğin başlangıç noktası olarak görülen fiziksel önlemler, insanların yanında kurumun diğer varlıklarını da korumaktadır. Ancak, bir kurumda insanlar güven içinde olmadıkları sürece diğer varlıkların ne kadar güvende olduklarının bir önemi yoktur (Yıldız, 2017, s.54).

3.1.2. Koleksiyon Güvenliği

Koleksiyon, kullanıcılarına gerekli hizmetleri sağladığı ve kütüphaneye değer kattığı için kütüphanenin önemli bir bileşenidir. Çok eski zamandan beri, kütüphaneler bünyesinde taşıdıkları koleksiyonları tarafından tanımlanmıştır. Bu bağlamda, kütüphanelerin ev sahipliği yaptığı bilgi varlıkları kütüphane için oldukça önem taşımaktadır. Diğer bir deyişle, kütüphane koleksiyonlarının korunmasının kütüphanenin hayatta kalması

üzerine büyük bir etkisi olacaktır (Yamson ve Cobblah, 2016, s.393). Aynı zamanda kütüphaneler bağlı bulundukları kurumların ve kullanıcılarının araştırma ve eğitimlerini desteklemek için kalite, derinlik, çeşitlilik, format ve para birimi açısından mevcut koleksiyona erişim sağlamaktadır (ACRL, 2018, s. 12). Bu nedenle, kütüphanelerin kullanıcılarının ve bağlı bulundukları kurumun bilgi gereksinimini karşılayabilmek için bünyesinde barındırdığı dermeyi güvende tutması gerekmektedir.

Günümüzde kütüphane materyallerinin güvenliğinin sağlanmasına yönelik birçok çalışma yapılmıştır (Maidabino ve Zainab, 2011; Maidabino ve Zainab, 2012; Abioye ve Rasaki, 2013; Akor, 2013; Yamson ve Cobblah, 2016; Botez ve Repanovici, 2017). Yapılan çalışmalar ise, koleksiyon güvenliği yönetimi, materyallerin kaybolması, çalınması, kitapların sayfalarının yırtılması, tahrif edilmesi, hırsızlığın önlenmesi için uygulanabilecek güvenlik yöntemleri vb. konular üzerine olmuştur. Bununla birlikte, birçok araştırmacı hırsızlık, sakatlanma ve diğer ilgili suçlarla ilgili fikri mülkiyet tehdidinin dünya genelinde kütüphane koleksiyonlarına büyük bir zorluk getirdiğini belirtmiştir. Sonuç olarak, kütüphanelerde koleksiyon güvenliğine ilişkin çeşitli problemler üzerine geniş bir literatür bulunmaktadır; ancak özellikle akademik ve üniversite kütüphanelerinde koleksiyon güvenliği yönetimi konusunda çok az literatür bulunmaktadır (Yamson ve Cobblah, 2016, s.394). Koleksiyon güvenliğine sadece fiziksel anlamda yaklaşılmamıştır. Botez ve Repanovici'ye göre (2017, s. 11), birçok çalışma koleksiyon güvenliği konusuna kullanıcıların ve kütüphane personelinin kişisel güvenliği açısından da yaklaşmıştır.

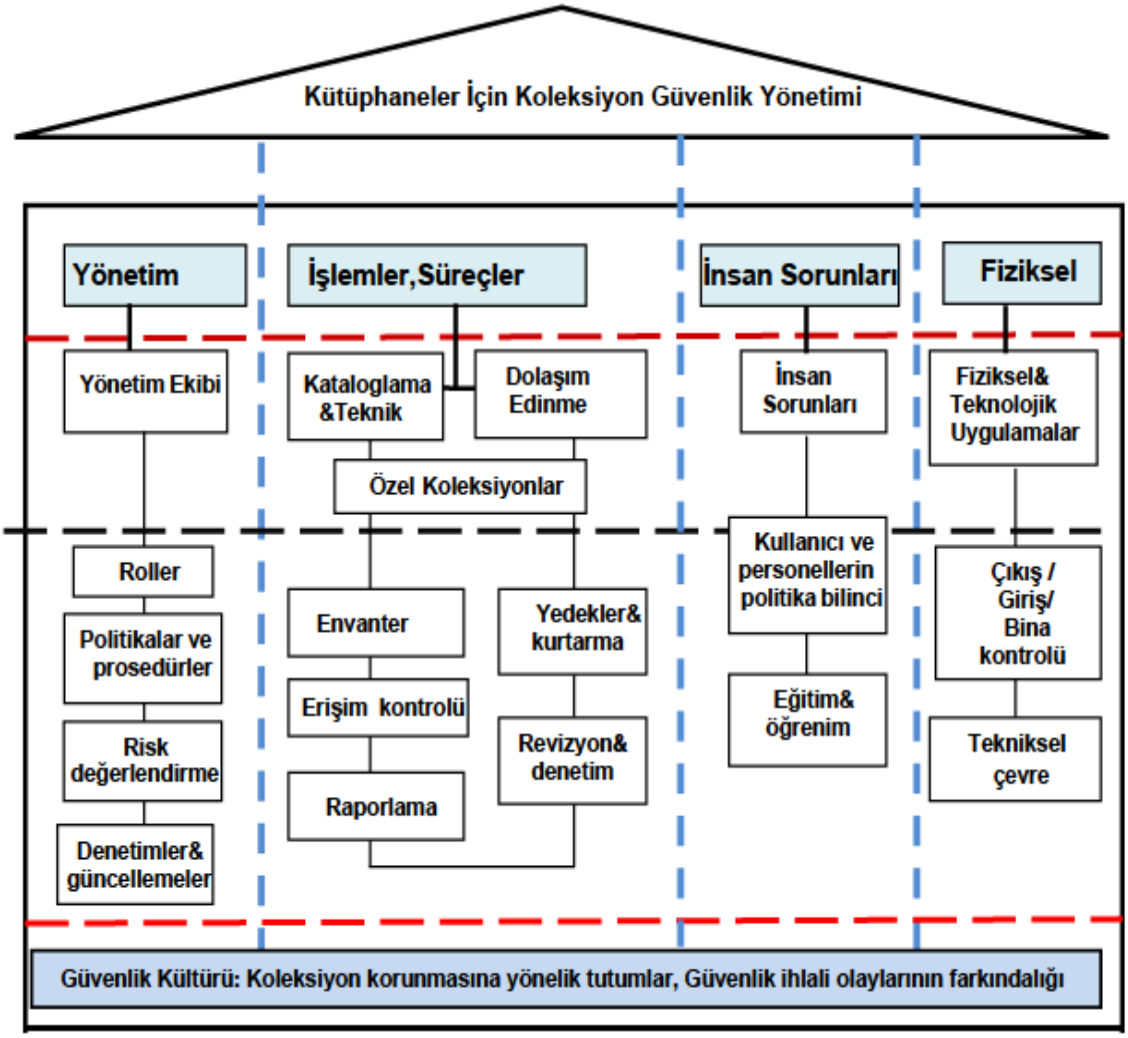
Kitap hırsızlığı, kütüphanelerde uzun yıllarda artmakta olan en yaygın suç olarak görülmektedir. Bununla birlikte kitaplara yönelik hırsızlık ve zararlara karşı mücadele etmek oldukça zordur. Çünkü suçlunun yakalanma riski oldukça düşüktür. Diğer taraftan, akademik kütüphanelerdeki kriminal faaliyetler yalnızca kütüphanenin bilgi materyalleriyle sınırlı olmayıp, el çantaları, cüzdanlar, hesap makineleri ve defterler gibi eşyaların çalınması da yaygın görülen güvenlik sorunları arasındadır. Kütüphanelerde kullanıcılar tarafından işlenen bazı suçlar, diğer kullanıcıları bilgi ihtiyaçlarının tam olarak yerine getirilmesinden mahrum bırakmıştır. Diğer bir deyişle, bir kullanıcının herhangi bir bilgi kaynağına zarar vermesi, çalması veya yok etmesi, diğer kullanıcıların kaynağa erişimini zorlaştırmaktadır. Kitap hırsızlığının yanı sıra felaketler (yangın, sel

vb.), dikkatsiz kullanım ve kötü çevre koşullarından kaynaklanan hasarlar kütüphane koleksiyonlarının güvenliğini tehdit eden unsurlar arasında yer almaktadır (Akor, 2013, s.12; Yamson ve Cobblah, 2016, s.394). Kütüphanelerdeki güvenlik sisteminin amacı, kütüphane çalışanları, kütüphanenin ekipmanları ve kaynakları ve kütüphane kullanıcıları için güveni ve emniyeti sağlamak olmalıdır (Akor, 2013, s.5). Kütüphanelerde suç ve kütüphane hizmetleri ve operasyonları üzerindeki olumsuz etkileri azaltmak için şu önerilerin üniversite kütüphaneleri tarafından yürürlüğe girmesinin zorunlu olduğu belirtilmektedir (Abioye ve Rasaki, 2013, s. 12; Abor, 2013, s.40) :

1. İyi eğitimli kütüphane personelinin işe alınmasıyla yeterli ve etkili bir güvenlik sistemi kurulmalıdır.
2. Kullanıcıların ödünç verilmeyen materyallerden (referans materyalleri, diziler, özel yayınlar vb.) yararlanabilmelerini sağlamak için fotokopi hizmetleri verilmelidir.
3. Kütüphane kaynaklarının kullanımını daha uygun hale getirebilmek için fiyatı yüksek olan kaynakların kopyaları alınmalıdır.
4. Kütüphane personelleri ve kullanıcılarının kütüphane güvenlik konuları ve kütüphane hizmetlerinin nasıl kullanılacağına ilişkin düzenli olarak eğitim ve öğretim almaları gerekmektedir.
5. Kütüphane materyallerine zarar veren, materyalleri yasadışı olarak çıkaran, hırsızlık yapan, kullanıcı ve personellere ceza verilmelidir.
6. Suçluları tespit etmek ve tutuklamak için kütüphanelerde ceza tespit sistemi kurulmalıdır. Üniversite kütüphanesi, kullanıcıların bilgi ihtiyaçlarını karşılamak için yeterli kütüphane materyalleri sağlamalıdır.
7. Kütüphane, elektronik güvenlik ağını ve diğer bilgi teknolojileri elemanlarını korumak için istikrarlı ve kesintisiz güç kaynağı sunmalıdır.
8. Kütüphanede yoğun talep gören ve son sürüm metinler, elektronik ortama aktarılmalıdır.
9. Kütüphane güvenlik personeli, kullanıcıların kütüphane kurallarına ve yönetmeliklerine hassasiyet göstermeleri için kütüphanede stratejik bir konuma getirilmelidir.
10. Kütüphane giriş çıkışlarında gerektiğinde kapsamlı bir araştırma yapılmasını sağlamak için kadın ve erkek güvenlik personeli bulundurulmalıdır.

11. Üniversitenin merkezi kütüphanesindeki yoğunluğu azaltmak için, bölüm kütüphaneleri kurularak kullanıcılar için daha fazla kaynak sunulmalıdır.
12. Kitap hırsızlığı ve yıpranma, tehdidini en aza indirmek için kapalı devre televizyon sistemi (CCTV) arttırılmalıdır.

Koleksiyon güvenlik yönetimi, kütüphanede kullanabilecek materyallerin iyi durumda tutulmasını ve çalınmasını önlemek için gerekli önlemleri almak ve uygulamak ile ilgilidir. Bununla birlikte, koleksiyon güvenlik yönetimi, riski azaltmak ve koleksiyonlara erişimi sağlamak için koleksiyon güvenliği politikalarının, programlarının, prosedürlerinin veya önlemlerin uygulandığı genel bir biçimde kavramsallaştırılabilmektedir (Akor, 2013, s.10). Ajegbomogun (2004, s.386) kütüphane güvenlik yönetimini "kütüphane koleksiyonlarını yetkisiz kaldırma veya kaybolmaya karşı korumak için stratejik olarak tasarlanan işlem" olarak tanımlamaktadır. Bu aynı zamanda, kullanıcıların ve kitapların yangın salgınına, sellere, böceklere ve davetsiz misafirlere karşı korunmayı da içermektedir (Akor, 2013, s.10; Ajegbomogun, 2004, s.386). Buradan hareketle koleksiyon güvenliği yönetimi, kütüphanede bulunan koleksiyonların doğal ve doğal olmayan risk, hasar ve tehditlere karşı tedbir ve önlemlerin yönetim süreci olarak tanımlanabilir.



Şekil 5. Kütüphanelerde koleksiyon güvenliği yönetimi modeli
(Maidabino ve Zainab, 2012, s. 110)

Koleksiyon güvenliği yönetimi modeli, Maidabino ve Zainab tarafından 2012 yılında geliştirilmiştir (Şekil 5). Yapı olarak eve benzeyen model, üniversite kütüphanelerinde koleksiyonların korunması ve güvenliğinin sağlanabilmesi için temel bileşenleri ele almıştır. Evin üst katında yönetim, süreçler, insan sorunları ve fiziksel bileşenler yer alırken, alt katında güvenlik kültürü yer almaktadır. Her bileşeni ayrı olarak detaylandırılan modelin ilk katmanı yönetim bileşeni ile başlamaktadır. Buradaki süreç, üniversite kütüphanelerinde güvenlik bölümünden sorumlu bir üye veya bir personel tarafından koleksiyon güvenliğinin yönetilmesi ile başlamaktadır. Diğer bir deyişle, ilgili personelin koleksiyonların güvenliğine dair politika ve prosedürler hakkında bilinçli olması, risk yönetimi için talimat ve planların tasarlaması ve kütüphanede iyi bir koleksiyon güvenliğinin yönetilip yönetilmediğinden emin olması süreçlerini

kapsamaktadır. Modelin daha sonraki süreci ise, güvenlik yönetim ekibi tarafından kütüphanenin kataloglama, satın alma ve özel koleksiyonlar bölümü aracılığıyla formüle edilen güvenlik programlarını uygulamaya koyma süreçlerini içermektedir (Maidabino ve Zainab, 2012, s. 110). Modelin insan katmanı ise, insan ve insana dair yönleri içermektedir. Bu katman, kullanıcıların ve personellerin güvenlik sorunları ile ilgili olarak bilgilendirilmesi, eğitilmesini ve denetlenmesini içermektedir. Modelin dördüncü katmanı, güvenli bir koleksiyon ortamının uygulanmasında hem fiziksel hem de teknolojik uygulamaları kapsamaktadır. Bu bağlamda, koleksiyonların güvenliğini sağlamak için koleksiyonların tutulduğu binanın veya alanın fiziksel mimarisi gözden geçirilmeli ve bina girişleri ve çıkışları kontrol edilmelidir. Modelin alt seviyesi olan güvenlik kültürü ise, ev modelinin temelini oluşturmaktadır. Güvenlik kültürü, kullanıcıların ve personellerin kütüphanede korumanın önemine yönelik tutumlarını ve farkındalıklarını içermektedir (Maidabino ve Zainab, 2012, s. 112). Maidabino ve Zainab 2011 yılında gerçekleştirmiş oldukları bir çalışmada bu modelin ilk sürümüne (s.20) yer vermiştir. Bu model, bir sonraki modelden (2012) farklı olarak aracı bir bileşeni içerdiği dikkati çekmektedir. Bu bileşenin demografik değişkenler olduğu anlaşılmaktadır.

3.1.3. Personel ve Kullanıcı Güvenliği

Kurumun kendi personeli, sözleşmeli çalışanlar, danışmanlar, ortak çalışılan kurum ve kuruluşların çalışanları, alt yüklenicilerin personeli ve son kullanıcıya kadar tüm bireyler personel güvenliğine dahil edilmektedir. (Tuğ İlçin, Adak ve Çakır, 2014, s. 12). İnsan etkileşiminin olduğu her ortamda güvenliğin sağlanması gerekmektedir. Bununla birlikte, bir kurumda bilgi güvenliğinin bütünsel bir yaklaşımla ele alınarak gerek kurum personellerine gerekse kurumdaki mal varlıklarına gelebilecek hasar, zarar, saldırı ve tehditlere karşı her türlü önlemlerin alınması personel ve kullanıcı güvenliğinin sağlanması için önem taşımaktadır. Aynı zamanda, kurumda yer alan yöneticilerin bilgi güvenliğine karşı bilgi ve bilinç sahibi olmaları kurum personellerinin üzerinde oldukça etkili olacaktır. Bundan dolayı, üniversite kütüphaneleri yöneticilerinin kütüphane personellerini konu ile ilgili olarak bilinçlendirmesi ve konuya ilişkin olarak personellere eğitim vermesi gerekmektedir.

Bir kurumda bilgi güvenliği uygulanırken öncelikle güvenlik işlevinin nasıl konumlandırıldığı ve etiketleneceği ele alınmalıdır. İkinci olarak, kurumdaki ligili bilgi güvenliği ekibinin güvenlik işlevleri için personellerin görev ve görev planındaki düzenlemeler planlanmalıdır. Üçüncü olarak, kurumdaki ilgili Bilgi İletişim ekibi bilgi güvenliğinin normal Bilgi İletişim işlevi üzerindeki etkisini değerlendirmeli ve iş tanımlarını ve belgelenmiş uygulamaları buna göre ayarlamalıdır. Son olarak, kurumdaki genel yönetim ekibi bilgi güvenliği kavramlarını personel yönetimi uygulamalarına entegre etmek için bilgi güvenliği uzmanları ile çalışmalıdır (Whitman ve Mattord, 2017, s. 580). Personel güvenliği ISO/IEC 27002: 2005'in 8. Bölümü'nde şu şekilde tanımlanmıştır (ISO/IEC 27002: 2005, 2005, s.23-26):

- Görevler ve sorumluluklar: Personellerin, tedarikçiler ve üçüncü taraf kullanıcıların güvenlik görevleri ve sorumlulukları kuruluşun bilgi güvenliği politikasına uygun olarak tanımlanmalı ve belgelenmelidir.
- Araştırma: Tedarikçiler ve üçüncü taraf kullanıcıları için tüm adaylara ilişkin arka plan doğrulama kontrolleri, ilgili kanunlar, yönetmelikler ve etik kurallara uygun olarak ve iş gereklilikleri, erişilebilecek bilgilerin sınıflandırılması ve algılanan riskler ile orantılı olarak yapılmalıdır.
- Çalışma şartları: Sözleşme yükümlülüğünün bir parçası olarak, personeller, tedarikçiler ve üçüncü taraf kullanıcılar, iş sözleşmesinin şartlarını ve koşullarını kabul etmeli ve imzalamalıdır; bu da onların ve kuruluşun bilgi güvenliği için görevlerini belirtmelidir.
- Bilgi güvenliği bilinci ve eğitimi: Kuruluşun tüm çalışanları ve bağlantılı olduğu durumlarda tedarikçiler ve üçüncü taraf kullanıcılar, iş işlevleri ile bağlantılı olarak uygun prosedürler ve politikalar hakkında uygun bilinç ve farkındalık eğitimi ve düzenli güncellemeler almalıdır.
- Disiplin süreci: Güvenlik ihlali yapan çalışanlar için resmi bir disiplin süreci olmalıdır.

3.1.4. Yazılım ve Donanım Güvenliği

Genellikle program biçiminde olan yazılım, bir bilgi sisteminin fonksiyonlarını gerçekleştirebilmesi için ihtiyaç duyulan donanım dâhilinde çalışan özel komutlardır (Güngör, 2015, s.33). Yazılım güvenliği ise, "yazılımların tersine mühendislik yöntemleri ve araçları ile (debugger, disassamler, vb.) algoritmalarının ortaya çıkartılması veya değiştirilmesini engellemeyi amaçlayan yöntemler bütünü" olarak adlandırılmaktadır. Kötü niyetli yazılımlar (virüs, truva atı, uygulama yazılımlarındaki güvenlik açıkları vb.), en çok kullanıcı bilgisayarlarına zarar vererek ağlarda kolaylıkla yayılabilmektedir. Dolayısıyla bu tür saldırılara karşı tedbir ve önlemleri almak son derece önem taşımaktadır. Bu bağlamda, olası tehdit ve saldırılara karşı kullanıcıların makinasında bir anti virüs yazılımı bulundurulmalıdır. Aynı zamanda, saldırı tespit sisteminin (intrusion detection systems), saldırı engelleme sisteminin (intrusion preventions systems) ve güvenlik duvarı (firewall) yazılımları kullanılmalıdır.

Bilgi sistemini oluşturan fiziksel elemanlar donanım(hardware) olarak adlandırılmaktadır (Güngör, 2015, s.33). Donanım güvenliği, dijital çağda kütüphanelerin vazgeçilmez bulduğu bilgisayarlar, yazıcılar vb. gibi ekipmanların güvenliğidir (Anday ve Diğerleri, 2012, s.120). Donanımın maruz kaldığı saldırı türleri, zarar verme, izinsiz erişim ihmal, umursamazlık, farelerin kabloları kemirmesi ya da küçük böceklerin elektronik devrelere girerek kısa devreye yol açması, donanım parçalarının üzerinde gün geçtikçe toz birikmesi devrelerde ve güç kaynaklarında, özellikle soğutucu sistemlerde bulunan parçaların çalışmasını engelleyerek donanım güvenliğinin tehlikeye girmesine neden olabilmektedir (Çelebioğlu, 2005, s.7). Bu tür donanımları güvenli odalarda fiziksel kilit ve anahtar altında tutmaya ihtiyaç duyulmaktadır ve kolay takip edilmesi için bir envanter sistemi uygulanmalıdır (Anday ve diğerleri, 2012, s.120).

3.2. ÜNİVERSİTE KÜTÜPHANELERİNDE KİŞİSEL VERİLERİN YÖNETİMİ

Kişisel verilerin korunmasına yönelik uygulamaların önem taşıdığı kurumlardan biri üniversite kütüphaneleridir. Bu kurumlar genellikle teknolojik uygulamaları yoğunlukla kullanan bir kullanıcı grubuna hizmet sunmakla birlikte kullanıma açtıkları sistemlerle bireylerin bilgi ile olan etkileşimlerine (ödünç kaynak verileri, bilgi arama davranışlarına

yönelik veriler gibi) yönelik verilerin üretilmesine, işlenmesine, kullanılmasına ve depolanmasına imkân tanımaktadır. Bu noktada üniversite kütüphanelerinin kullanıcı etkileşimi sonucunda topladıkları ya da ürettikleri kişisel veriler boyutunda hem kullanıcılar hem de dermelerinde bulunan bilgi varlıklarının korunması bağlamında sorumlulukları bulunmaktadır.

Üniversite kütüphanelerinde veriyi işleyen, aktaran ve paylaşan görevli personeller kütüphanecilerdir. Bu veriler üniversitenin abone olduğu veri tabanları, satın aldığı bilgi kaynaklarının yanı sıra kullanıcı ve personellere ait kişisel bilgilerden de oluşmaktadır. Bu noktada üniversite kütüphanelerinde önemli olan bir husus ise, veri sahibinin rızası, kullanım amacının belirginliği, hukuksal dayanağının bulunması ve sadece amaca yönelik minimum seviyede kişisel bilgilerin elde edilmesi ve işlenmesidir (Henkoğlu ve Uçak, 2015, s.48). Üniversite kütüphanelerinde kişisel veriler tüm birimler arasında kullanılmaktadır. Ancak, kişisel veri akışının en yoğun olan yerleri, danışma hizmetleri ve ödünç verme hizmetlerinin olduğu iletişim alanlarıdır. Bu bağlamda, bu hizmet yerlerinin olduğu yerlerde kişisel verilerin özellikle korunması gerekmektedir. Bu birimlerde kullanılan kişisel verilere örnek verecek olursak, kullanıcının araştırma konusu, ödünç alınan kaynakların listesi, kullanıcının danışma hizmetleri kapsamında edindiği bilgiler, dolaşım kayıtları, arşiv belgeleri/kayıp kütüphane materyalleri, kütüphaneler arası kayıtlar (Inter Library Loan), fotokopi hizmetleri ile ilgili belgeler, kütüphane kaynaklarına ve veri tabanlarına bağlandığı IP adresi, web sayfasına yapılan ziyaretlere ilişkin kayıtlar, kullanıcının kimlik bilgilerinden (T.C. kimlik numarası, ad, soyad vd.) ve kullanıcının iletişim bilgileri (telefon, adres, vb.) oluşabilmektedir (Henkoğlu ve Uçak, 2015, s.47-64; Inoue, 2018, s.225). Bu veriler, kütüphanelerde -Genel Veri Koruma Tüzüğü'ne dayalı olarak- şu yasal dayanaklara bağlı olarak işlenebilmektedir (Axiell, 2018):

- Kullanıcının rızasına sahipseniz (veri konusu),
- Kullanıcılarınızla sözleşme yükümlülüğünüz varsa,
- Kullanıcı verilerinin işlenmesi yasal bir yükümlülüğe uymak için gerekliyse,
- Kullanıcı verilerinin işlenmesi bir veri konusunun veya başka bir kişinin hayati çıkarlarını korumak için gerekliyse,
- Kamu yararınaysa, veri işleme sorumluluğuna sahipseniz.

Veri koruma prensipleri ve yönetmeliğinden hareket ederek kütüphanecilerin kişisel verilerin korunmasında şu özelliklerin bilincinde olması gerektiği söylenebilir (Paraschiv, 2018; Korn ve Tullo, 2018, s.4 ve Brown, 2001, s. 69):

- İşleme için yasal gerekçeler daima belirlenmeli, yasal gerekçelere uyum sağlanmalı ve kişisel verilerin hangi amaçla tutulduğu saptanmalıdır.
- Bireylerin haklarına uygun olarak, kişisel veriler işlenmelidir.
- İlk yasal gerekçelerin ötesinde kişisel verileri paylaşmaya veya kullanmaya dikkat edilmelidir.
- Kişisel veri dosyalarının düzenli olması ve düzenli olarak güncellenmesi gerekmektedir.
- Kişisel verilere sağlam bir şekilde güvenli erişim ve güvenlik sağlanmalıdır.
- Yeterli miktarda kişisel veriler tutulmalı ve belli süre içerisinde muhafaza edilmelidir.
- Kişisel verilerin neden, nasıl, nerede ve ne kadar süreyle işlendiğinden bilgi sahibi olunmalıdır.
- Uygun teknik ve organizasyonel önlemlerin izinsiz olarak işlenmesi, kaza sonucu kayba uğraması vb. veya verilerin zarar görmesi durdurulmalıdır.
- Kurumunuzda kişisel verilerin işlenmesi için bir veri koruma görevlisi bulundurulmalıdır.

Kütüphaneler bağlamında, kullanıcıların mahremiyetinin sağlanması, uluslararası kurum ve kuruluşların mesleki ilkelerinde, bildirgelerinde, sözleşmelerinde yer almaktadır. Bu kurumlardan birisi olan ALA (Amerikan Library Association) etik kurallarında, kütüphane hakları bildirgesinde, politika ve kanunlarında kütüphanelerde kullanıcı mahremiyetinin gerekliliğini vurgulamaktadır (Connolly, 2018, s.14). Kullanıcı mahremiyetinin entellektüel özgürlük misyonunun ayrılmaz bir parçası olduğunu nitelendiren ALA, kütüphanelerde kullanıcı mahremiyeti konusunu şöyle nitelendirmiştir (ALA, 2014, 2016):

- Kullanıcı mahremiyeti, kütüphaneciliğin temel bir değeridir ve bir kütüphane kişisel olarak tanımlanabilir bilgilere sahip olduğunda ve bu bilgileri kendi adına gizli tuttuğunda mahremiyet oluşturmaktadır (2014).
- Kütüphanelerin bilgiye erişimi engellememesi için, kütüphaneciler, kullanıcıların mahremiyet ve sorgulama özgürlüğünü desteklemelidir (2014).
- Kütüphaneler, entegre yönetim sistemleri olarak adlandırılan kütüphane yönetim sistemlerinin kullanıcı mahremiyeti ile ilgili etik, politika ve yasal yükümlülükleri yansıttığından emin olmalıdır (2016).

Kütüphanelerde kullanıcı mahremiyeti entelektüel özgürlük ve etik kuralları kapsamında ele alan kurumlardan IFLA (International Federation of Library Associations) (1999) ve ALA (2008) tarafından hazırlanan bildirilerde, kullanıcıların kimliğinin ve kütüphaneden yararlandığı kaynakların üçüncü kişilere aktarılamayacağı ve kullanıcıların mahremiyetinin korunacağına değinilmiştir. Türkiye'de 1949 yılından günümüze faaliyet gösteren Türk Kütüphaneciler Derneği'nin düşünce özgürlüğü bildirgesi (2008) ve mesleki etik ilkelerinde (1996), kullanıcıların mahremiyetine saygı duyulacağından bahsedilerek kişisel verilerin üçüncü kişilere transfer edilemeyeceğine vurgu yapılmıştır. Bazı ülkelerin (Avusturalya, Kosta Rika, Estonya, İzlanda gibi) mesleki etik ilke ve kurallarında, kullanıcıların gizliliğinin sağlanması hususunda kütüphanecilere düşen görev ve sorumluluklara, kullanıcıların gizliliğine saygı duyulmasına, entellektüel özgürlük ve fikri mülkiyet haklarının korunmasına ilişkin bilgilere yer verilmiştir (Byrne, 2002, s.14; Sequeira, 2002, 76; Tamre, 2002, s.92; Friðgeirsdóttir, 2002, s.135; Inoue, 2002, s.150). Kütüphane kurumlarında kullanıcının kişisel verilerinin gizliliğinin sağlanması ve kullanıcı mahremiyetinin sağlanması kütüphane kaynaklarının başarılı kullanımı açısından hayati önem taşımaktadır (McMenemy, Poulter ve Burton, 2007). Bunun sağlanabilmesi için ise, kütüphanelerde kullanıcıların, yöneticileirn ve personelelrin mahremiyetinin sağlanabilmesi için gizlilik politikalarının oluşturulması gerekmektedir. Givens (2015, s.95-96), hazırlanan gizlilik politikalarıyla ilgili şu önerilerde bulunmaktadır:

1. İyi bir gizlilik politikası geliştirmek için gizlilikle ilgili kanunlar, yönetmelikler ve en iyi uygulamalar hakkında bilgi sahibi olunması gerekmektedir.
2. Gizlilik risklerinin değerlendirilmesi gerekmektedir.
3. Gizlilik politikaları hukuk ve kurumsal uygulamalarla uyumlu olmalı ve okuyucular için anlaşılabilir olmalıdır.
4. Gizlilik politikalarını oluşturan veya güncelleyen herkes, çevrelerindeki mevcut veri toplama uygulamalarını incelemelidir.
5. Hangi kişisel verilerin toplandığını ve nasıl kullanıldığını, paylaşıldığını, saklandığını, korunduğunu ve yok edildiğini anlamak önemlidir.
6. Her kütüphanenin kullanıcılarının veri toplama, kullanma, paylaşma ve güvenlik uygulamalarını bilmelerini sağlamak için bir kamu gizlilik politikasına sahip olması gerekmektedir.
7. Kütüphanede gizlilik eğitimi ve farkındalık konusunda eğitim verilmelidir.
8. Gizlilik politikaları ve uygulamaları hazırlanırken bir gizlilik danışmanından yardım alınmalıdır.

ACRL tarafından 2018 yılında "Yükseköğretimde Kütüphaneler İçin Standartlar (Standards for Libraries in Higher Education)" başlıklı eserini yayınlamıştır. Söz konusu

standartlar, ilkeler ve ilkeler ile ilgili performans göstergeleri etrafında şekillenmiştir. Kurumsal etkinlik (institutional effectiveness), mesleki değerler (profesyonel values), eğitim rolü (educational role), bulma (discovery), collections (koleksiyon), space (mekân), yönetim/yöneticilik/liderlik (management/administration/leadership), personnel (personel), dış ilişkiler (external relations) dokuz temel ilkeyi oluşturmaktadır. ACRL, 'mesleki değerler' ilkesinde kütüphanelerde kişisel verilerin korunmasına değinmiştir. Söz konusu ilke ve göstergeleri şu şekildedir (ACRL, 2018, s.10):

Mesleki değerler: Kütüphaneler fikri özgürlük, fikri mülkiyet hakları ve değerleri, kullanıcı mahremiyeti ve korunması, iş birliği ve kullanıcı merkezli hizmetin mesleki değerlerini geliştirir.

- Kütüphane, kütüphane kaynaklarının erişime sunulmasında tüm önlem ve tedbirleri alır.
- Kütüphane her kütüphane kullanıcısının gizlilik ve gizlilik haklarını korur.
- Kütüphane fikri mülkiyet haklarına saygı duyar ve bilgi kullanıcılarının çıkarları ile hak sahiplerinin çıkarları arasındaki dengeyi politika ve eğitim programlaması yoluyla savunur.
- Kütüphane, eğitim ve politika aracılığıyla intihali tespit eder ve akademik bütünlüğü destekler.
- Kütüphane kullanıcı merkezli bir yaklaşım benimser ve kullanıcıların fiziksel ve sanal ortamlarda hizmet tasarımı ve sunumunun tüm yönlerinde merkeziyetini gösterir.
- Kütüphane kampüs içinde ve kampüs dışında iş birliği yapar.

'Mahremiyet' veya 'kullanıcı mahremiyeti', kullanıcı kayıtlarının gizliliğinin sağlanmasıdır. Diğer bir deyişle, bilginin gizliliğinin korunmasıdır. Bu bağlamda kütüphanelerde mahremiyet, bir kütüphane kullanıcıları hakkında kişisel verilere sahip olduğunda ve bu verileri kendi adına gizli tuttuğunda oluşmaktadır. Mahremiyet kavramı içerisinde ise, kişisel olarak tanımlanabilir bilgi kavramı karşımıza çıkmaktadır. Bu kavram, bireyin adı, adresi telefon numarası vb. kişisel bilgilerden daha geniş bir yelpazeye sahiptir. Örneğin; kredi kartınızla satın aldığınız öge, kütüphane kartınızla yapılan işlemler, veri tabanı arama kayıtları, referans görüşmeleri, dolaşım kayıtları, ödünç materyal kayıtları, tarama oturumları, kütüphanenin wifi ağına bağlanılan kişisel bir telefona kadar kişileri tanımlayan bilgileri içermektedir (ALA, 2004; ALA, 2014; Connolly, 2018,15).

Ancak, bilgi ve belge merkezleri olan kütüphaneler tarafından elde edilen kişisel verilerin hangi amaçla kullanılacağına ilişkin eksiklikler ve belirsizlikler bulunmakla birlikte, kütüphane üyelerine bu konuda nadiren bilgi verilmekte ve kişisel verilerin nasıl muhafaza edileceğine dair sözleşmede bulunmamaktadır (Preisig, Rösch ve Stückelberger, 2014). Aynı zamanda üniversite kütüphanelerinde, kişisel verilerin işlenmesine ilişkin eksikliklerin bulunduğu, diğer üniversite birimleriyle sorumlulukların paylaşılmadığı, risk yönetiminin yapılmadığı, personele veri korumaya ilişkin bilinçlendirme eğitimi verilmediği ve bu konuda bir denetim mekanizmasının olmadığı görülmektedir (Henkoğlu ve Uçak, 2015, s. 70). Hem kütüphanelerin hem de kütüphanecilerin kullanıcıların bilgi edinme haklarının yanı sıra kullanıcıların kişisel veri korumasını gerçekleştirmelerine yardımcı olma sürecinde etkin ve proaktif bir role sahip olmaları gerekmektedir. Bu bağlamda, kütüphanelerde gizlilik, çalışan verisi ve kullanıcı verisi olarak karşımıza çıkmaktadır (Preisig ve diğerleri, 2014). Diğer bir deyişle, kütüphanecilerden beklenen sadece hizmet sunumu değil aynı zamanda kullanıcıların temel hak ve özgürlüklerinden biri olan kişisel verilerinin korunmasının da sağlanmasıdır.

4. BÖLÜM

ANKARA'DAKİ ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLERİN YÖNETİMİNE DÖNÜK KOŞULLARLA İLGİLİ BULGULAR

Çalışmanın bu bölümünde üniversite kütüphanelerinde kişisel verilerin korunması ve bilgi güvenliği uygulamalarına yönelik mevcut durumu belirlemek ve üniversitelerde karşılaşılan sorunları tespit etmek amacıyla geliştirilen ve ayrıntıları birinci bölümde sunulan araştırma araçlarıyla toplanan verilerden elde edilen bulgulara yer verilmiştir. Söz konusu bulgular Ankara'daki 15 üniversite kütüphanesinde hizmet sunma boyutunda karar verici durumundaki yöneticiler ve verilen kararların uygulanması aşamasında sorumlulukları bulunan kütüphanecilerin yaklaşımlarını yansıtmaktadır. Bu doğrultuda bulgular kütüphane yöneticileriyle gerçekleştirilen görüşmelerden elde edilen veriler ve kütüphanecilerle gerçekleştirilen anketlerden elde edilen veriler olmak üzere iki bölümde ele alınmıştır.

4.1. GÖRÜŞMELERDEN ELDE EDİLEN BULGULAR

Araştırmanın bu bölümünde üniversite kütüphaneleri yöneticileriyle gerçekleştirilen görüşmelere dayalı bulgulara yer verilmektedir. Bu kapsamda, yapılan görüşme içeriğine göre yöneticilerin kişisel verilerin korunması ve bilgi güvenliği ile ilgili uygulamalara yönelik görüşlerini gösteren bulgular bu bölüm altında ele alınmaktadır.

4.1.1. Kişisel Verilerin Yönetimine Yönelik Elde Edilen Bulgular

Bu bölümde, üniversite kütüphanelerinde kişisel verilerin yönetilmesine yönelik gerçekleştirilen uygulamalara ilişkin sorulara verilen yanıtlar sunulmaktadır. Bu kapsamda ilk olarak yöneticilere kütüphanelerinde personellere ve kullanıcılara ilişkin olarak hangi kişisel verilerin kayıt altına alındığı sorusu yöneltilmiştir. Söz konusu bulgular Tablo 2'de yer almaktadır.

Tablo 2. Kişisel veri tanımı kapsamında kütüphanelerde yer alan kişisel veriler

Kişisel veriler	Kullanıcı		Personel	
	S	*%*	*S*	*%*
T.C. Kimlik Numarası	13	86,7	11	73,3
Adı Soyadı	13	86,7	13	86,7
İletişim bilgileri	13	86,7	12	80,0
Adresi	12	80,0	11	73,3
Sicil Numarası	4	26,7	10	66,7
Unvanı	4	26,7	8	53,3
Nüfus bilgileri	4	26,7	5	33,3
Özgeçmiş	1	6,7	5	33,3
Kan grubu	1	6,7	1	6,7
Dili	1	6,7	1	6,7

Tablo 2'de 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamı altında 'kişisel veri' tanımı altında yer alabilecek T.C. kimlik numarası, adı soyadı, nüfus bilgileri, kan grubu, iletişim bilgileri, adresi, sicil numarası, unvanı, özgeçmişi ve dili olmak üzere on değişkene bağlı olarak kütüphanede tutulan verilere yönelik istatistiki bilgiler bulunmaktadır. Bu durumda Tablo 2 incelendiğinde, kütüphane yöneticileri kütüphanelerde kullanıcılara ve personele ait olarak kayıt altına alınan kişisel verilerin en çok T.C. kimlik numarası, adı soyadı, iletişim bilgileri, adresi olduğunu belirtmiştir. Bununla birlikte, nüfus bilgileri, kan grubu, özgeçmiş ve dili kütüphanelerde tutulan kişisel veriler arasında yer almaktadır. Diğer taraftan, Tablo 2'ye bakıldığında, personellerin özgeçmişi kurumların üçte birinde kayıt altına alınırken, kullanıcıların özgeçmişi yalnızca bir kütüphanede kayıt altına alınmaktadır. Burada, dikkat edilmesi

gereken nokta ise, kütüphane personellerinin de kendi kurum kütüphanelerinin kullanıcıları olmasıdır. Diğer bir deyişle, kullanıcılara ait özgeçmiş oranlarının içerisinde personellere ait kişisel verilerin de bulundurulması gerektiği düşünülmelidir. Aynı durum, kullanıcılara ait sicil numarası ve unvanında da ortaya çıkmaktadır. Yine Tablo 2'de kütüphanelerde personellere ait sicil numaralarının kullanıcılardan daha fazla tutulduğu görülmekte ve personellere ait unvanların da kullanıcılardan daha fazla tutulduğu ortaya çıkmaktadır. Tablo 2'ye ek olarak, kütüphane yöneticilerine kütüphanelerde günlük iş süreçlerinde kullanmak için kayıt altına aldıkları kişisel verilerin (kişi ile ilişkilendirilerek tutulan verilerin) neler olduğu da sorulmuştur (Bkz. Tablo 3).

Tablo 3. Kütüphane bünyesinde kullanılan kişisel veriler

Kişisel veriler	Kullanıcı		Personel	
	S	%	S	%
Bölümü/Fakültesi/Enstitüsü	14	93,3	5	33,3
Öğrenci Numarası	14	93,3	1	6,7
Kişisel/Kurumsal E-posta Hesabı	12	80,0	13	86,7
Ödünç işlemlerine yönelik bilgiler	12	80,0	10	66,7
Sınıfı	9	60,0	1	6,7
Üyelik kartları	6	40,0	1	6,7
Etkinliklere dair kayıtlar	6	40,0	6	40,0
Kullanıcı adı	5	33,3	4	26,7
Öğrenci kartları	5	33,3	1	6,7
Kütüphaneyi kullanma saatleri	4	26,7	4	26,7
Şifre	4	26,7	4	26,7
Tarama oturumları	4	26,7	3	20,0
Veri tabanı arama kayıtları	4	26,7	2	13,3
Web sayfasına yapılan ziyarete ilişkin kayıtlar	3	20,0	3	20,0
Personel kartları	2	13,3	9	60,0
Kişisel bilgisayara ait IP/MAC adresleri	1	6,7	4	26,7
Kullanıcının araştırma konuları	1	6,7	1	6,7

Tablo 3'e göre kütüphane yöneticileri, üniversitelerin çoğunluğunda kullanıcılara yönelik kişisel verilerin en çok bölümü/fakültesi/enstitüsü, öğrenci numarası, kişisel/kurumsal e-posta hesabı ve ödünç işlemlerine yönelik veriler olduğunu belirtmiştir. Personele yönelik kişisel verilerin ise en çok kişisel/kurumsal e-posta hesabı, ödünç işlemlerine yönelik bilgiler, etkinliklere dair kayıtlar ve bölümü/fakültesi/enstitüsünün olduğu ortaya çıkmaktadır. Kullanıcı ve personele yönelik olarak tutulan veriler arasında etkinliklere

dair kayıtlar, şifreler ve kütüphaneyi kullanma saatleri, kullanıcının araştırma konuları ve web sayfasına yapılan ziyaretler ise aynı oranda şekilde yerini almaktadır. Tablo 3'de dikkat çeken noktalar arasında ise, kütüphanelerde tutulan kişisel veriler arasında yer alan personel kartları, kişisel bilgisayarlara ait IP/MAC adresleri, kişisel/kurumsal e-posta hesaplarının kullanıcılardan çok personele yönelik olarak tutulması yer almaktadır. Yine, kullanıcılara ait kişisel verilerin personellere ait kişisel verilerden ayrıştığı noktalar ise, bölümü/fakültesi/enstitüsü, öğrenci numarası, ödünç işlemlerine yönelik bilgiler, sınıfı, üyelik kartları, öğrenci kartları ve veri tabanı arama kayıtlarıdır. Tablo 3'de yer alan yöneticilerin kişisel veri kapsamında korunmasına yönelik olarak *"tereddüt ettikleri bilgiler arasında ödünç alınan yayınların listesi, danışma hizmetleri kapsamında edinilen bilgilerin listesi ve IP adresleri yer alırken, yöneticilerin iletişim ve kimlik bilgilerinin korunması gerektiği konusunda da tereddütleri bulunmadığı*" konuyla ilgili bir yapılan bir araştırmada tespit edilmiştir (Henkoğlu ve Uçak, 2015, s.64). Tablo 2'ye bakıldığında, yöneticilerin çoğunluğu iletişim ve kimlik bilgilerinin üniversite kütüphanelerinde kullanılan kişisel veriler arasında yer alması, bu verilerin korunmasının bir nedeni olarak sayılabilmektedir.

Henkoğlu'nun yapmış olduğu (2015b, s.148) araştırmada üniversite kütüphaneleri yöneticileri, kullanıcılara yönelik kişisel veriler arasında en çok sayıda kullanıcıların kimlik bilgileri (Ad – Soyad, T.C. kimlik numarası vd.), kullanıcıların araştırma konuları ve iletişim bilgileri olduğunu belirtirken, en az sayıda ödünç alınan yayınların listesi olduğunu belirtmiştir. Araştırmada bu sorunun ardından kütüphane yöneticilerine kütüphanelerinde kişisel verilerin nasıl toplandığı sorusu yöneltilmiştir. Birden çok seçeneğin işaretlendiği bu soruya yönelik bulgular Tablo 4'de bulunmaktadır.

Tablo 4. Kütüphanede kişisel verilerin toplanma şekli (S=14)

Kişisel verilerin toplanma şekli	**S**	**%**
ÖİDB'den ilgili kütüphane sistemine aktarılarak	10	71,4
PDB aracılığıyla	9	64,2
BİDB'den ilgili kütüphane sistemine aktarılarak	8	57,1
Kullanıcı kitlesine sunulan kayıt formları aracılığıyla	7	50
Üçüncü parti kuruluşlardan ilgili kütüphane sistemine aktarılarak	1	7,1
Diğer	1	7,1

BİDB: Bilgi İşlem Daire Başkanlığı, ÖİDB: Öğrenci İşleri Daire Başkanlığı, PDB: Personel Daire Başkanlığı,

Üniversite kütüphanelerinin 10'u ÖİDB aracılığıyla kişisel verileri topladıklarını belirtirken, kütüphanelerin 9'u, PDB aracılığıyla kişisel verileri topladıklarını

belirtmiştir. Bu sayıyı takiben, kütüphanelerin 8'i BİDB'den ilgili kütüphane sistemine aktarılarak kişisel verileri topladıklarını ifade etmiştir. Kişisel verilerin kullanıcılara sunulan kayıt formları aracılığıyla toplandığını belirten kütüphanelerin sayısı ise 7'dir. Üçüncü parti[13] kuruluşlardan ilgili kütüphane sistemine aktarılarak kişisel veri topladığını belirten üniversite kütüphanelerinin sayısı ise 1'dir. Kütüphanede kişisel veri toplanmadığını belirten üniversite kütüphanelerinin sayısı da yine aynı şekilde 1'dir. Tablo 4'de yer alan kişisel verilerin toplanma şekline ek olarak, bu verilerin üniversite kütüphanelerinde ilk olarak ne zaman kayıt aldığına ilişkin bulgular birden fazla seçeneğin işaretlenebilmesi koşuluyla Tablo 5'de yer almaktadır.

Tablo 5. Kişisel veriler ilk olarak ne zaman kayıt altına alınmaktadır? (S=15)

	S	**%**
Kullanıcının üyelik formlarını doldurduğu bir zamanda	8	53,3
Her dönem başında üniversitenin ilgili sistemlerinden otomatik olarak alınmaktadır.	7	46,6
Kullanıcı bilgisi üniversitenin ilgili sistemine kaydedildiği anda kütüphane sistemine aktarılmaktadır.	6	40
Diğer	2	13,3

Tablo 5'e göre üniversite kütüphanelerinin en çok kişisel verileri kullanıcının üyelik formlarını doldurduğu bir zamanda aldıkları (8 kurum - %53,3) ortaya çıkmaktadır. Daha sonra ise, (7 kurum – %46,6) kütüphanelerde her dönem başında üniversitenin ilgili sistemlerinden kişisel verilerin otomatik olarak alındığı belirlenmiştir. Bununla birlikte, kişisel verileri kullanıcı bilgisinin üniversitenin ilgili sistemine kaydedildiği anda kütüphane sistemine aktarıldığı (6 kurum - %40) da kütüphane yöneticileri tarafından belirlenmiştir. Diğer seçeneğini işaretleyen kütüphane yöneticilerinden biri (%13,3), kişisel verilerin *'düzensiz aralıklarla'* kayıt altına alındığını belirtmiştir. Bir diğer yönetici(%13,3) ise, *"Üyelik formu var. Yönetmelik doğrultusunda alınıyor"* yanıtını vermiştir.

Yöneticilere üniversite kütüphanelerinde Kişisel Verilerin Korunması Kanunu kapsamında veri sorumlusunun olup olmadığına ilişkin bir soru yöneltilmiştir. Alınan yanıtlara göre, 8 kurum (%53,3) üniversite kütüphanesinde veri sorumlusunun

[13] Bir iş sözleşmesinde veya yasal bir durumda yer alan ana kişilerden biri olmayan ancak, bir konuda küçük bir rol oynayan kişidir (" Collins", 2020) .

bulunmadığı belirlenmiştir. Ayrıca bir kurum kütüphanede veri sorumlusunun bulundurulmamasını, personel kayıtlarının İnsan Kaynakları Müdürlüğü, öğrenci kayıtlarının ise Öğrenci İşleri Müdürlüğü tarafından toplanmasına bağlamıştır. Diğer yandan, geriye kalan 7 kurum (%46,7) kütüphane yöneticisi ise kütüphanelerinde kişisel verilerin yönetiminden sorumlu bir personelin bulunduğunu belirtmiştir. Henkoğlu ve Uçak (2015, s. 49) Anayasa'nın 20. Maddesinde geçen (T.C. Anayasası, 1982), kişinin açık rızası dâhilinde kişisel verilerin işlenmesini üniversitelerde elde edilen ve işlenen kişisel veriler konusunda veri sahiplerinin gerçek hak sahibi olduklarını ifade etmiştir. Yazarlar yüksek öğretim kurumlarında ve diğer kamu kurumlarında idari düzenlemelere bağlı olarak işlenen kişisel verilere ilişkin sorumluluğun, idare ve veriyi işleyen personelin tamamını içerdiğini belirtmiştir (Henkoğlu ve Uçak, 2015, s.49). Söz konusu düzenlemelere ilişkin olarak, üniversite kütüphanelerinde de kişisel verilere yönelik görev ve sorumluluk kişisel verileri işleyen personelin tamamını kapsamaktadır.

Kütüphane yöneticilerine sorulan bir diğer soru ise, kütüphanede tutulan kişisel verilerin sınıflanmasına yönelik bir düzenlemelerinin olup olmadığıdır. Elde edilen verilere göre, 9 kurum (%60) kişisel verilerin sınıflanmasına yönelik bir düzenlemelerinin olduğunu belirtirken, 6 kurum (%40) kişisel verilerin sınıflanmasına yönelik düzenlemelerinin olmadığını belirtmiştir. Kişisel verilerin sınıflanmasına yönelik düzenlemelerinin olduğunu belirten üniversite kütüphane yöneticilerine, bu düzenlemeleri nasıl gerçekleştirdikleri sorulmuştur. Birden çok yanıt seçeneğinin verildiği bu soruya, kurumların 8'i (%50) kullanıcı grubuna göre (akademisyen, öğrenci, mezun, vb.) kişisel verileri sınıfladıklarını belirtmiştir. Alınan yanıtlara göre kurumların kişisel verileri sadece kullanıcı grubuna göre değil aynı zamanda gizlilik derecelerine (tasnif dışı, özel, hizmete özel, gizli, çok gizli) (2 kurum - %12,5), işlem öncelik sıralarına (2 kurum - %12,5), güvenlik hassasiyet düzeylerine (1 kurum - %6,3), tür ve özelliklerine (1 kurum - %6,3) ve belge isimleri ve standart dosya planına (1 kurum - %6,3) göre sınıflandırdıkları tespit edilmiştir. Kullanıcı kayıtlarının gizlilik derecelerine göre üniversite kütüphanelerinde sınıflandırılıp sınıflandırılmadığını araştıran bir çalışmada (Henkoğlu ve Uçak, 2015, s. 56), *"katılımcıların büyük bölümünün kullanıcı kayıtlarının öğrenci ve personel bilgi sistemi üzerinden alındığı gerekçesiyle kendileri tarafından ayrıca sınıflandırma yapılmasına ihtiyaç duyulmadığını ve katılımcıların bu verilerin sahibine karşı sorumluluk hissetmedikleri"* belirlenmiştir. Bu durum ise, üniversite

kütüphanelerinde kullanıcılara yönelik hangi verilerin toplanması gerektiği ve hangi verilerin gizlilik düzeyine göre sınıflandırması ve güvenilirliğinin sağlanması gerektiği hakkında belirsizliklerin olması, üniversitelerde kişisel verilerin korunmasına yönelik bir politikanın bulunmamasına bağlanmıştır (Henkoğlu ve Uçak, 2015, s.56).

Üniversite kütüphanelerinde kişisel verilerin yoğun olarak işlendiği birimlerin, kullanıcıların kütüphane personelleriyle etkileşim içerisinde bulundukları ortamların olduğunu söyleyebilmek mümkündür. Ancak, kişisel verilerin işlendiği ortamları sadece kullanıcı-personel etkileşimi boyutunda düşünmek yanlış olacaktır. Diğer bir deyişle, kişisel veriler sadece insan-insan etkileşimine bağlı değil makine-insan etkileşimine bağlı olarak da işlenebilmektedir. Bu bağlamda, araştırma kapsamında üniversite kütüphanelerinde kişisel verilerin en çok işlendiği birimler birden çok seçeneğin işaretlenmesi koşuluyla belirlenmeye çalışılmıştır (Tablo 6).

Tablo 6. En çok kişisel veri işlenen birimler (S=15)

Birimler	**S**	**%**
Ödünç Verme Birimi	12	80
Elektronik Kaynaklar Birimi	6	40
Sağlama ve Kataloglama Birimi	5	33,3
Kurumsal İletişim Birimi	4	26,6
Basılı Süreli Yayınlar Birimi	4	26,6
Açık Erişim ve Kurumsal Arşiv Birimi	4	26,6
Enformasyon Teknolojileri Birimi	3	20
Danışma Birimi	3	20
Kalite Yönetim Birimi	1	6,6
Satın Alma ve Muhasebe Birimi	1	6,6
Diğer	1	6,6

Tablo 6'da görüldüğü üzere, üniversite kütüphanelerinde kişisel verilerin en çok işlendiği birim başta (12 kurum - %80) Ödünç Verme Birimi'dir. Daha sonra ise, Elektronik Kaynaklar Birimi (6 kurum - %40), Sağlama ve Kataloglama Birimi (5 kurum - %33,3) gelmektedir. Kullanıcıların veri tabanı abonelikleri, kampüs dışı erişim veya ücretli yayınlara erişimde kütüphanede yayınlara erişim sağlamaları veya veri tabanlarında yaptıkları arama kayıtları, yüksek lisans/doktora öğrencilerinin işlemleri vb. e-kaynaklar biriminde tutulan kişisel verilere örnek olarak gösterilebilir. Bununla birlikte, kütüphaneye sağlanan (derleme, bağış, satın alma vb.) yayınların ve eserlerin kütüphaneye kayıt edilmesi sırasında gerçekleştirilen işlemler Sağlama ve Kataloglama Birimi'nde kişisel verilerin işlenmesine gösterebilecek örnekler arasındadır. Kişisel verilerin işlendiği diğer birimler arasında ise, Kurumsal İletişim Birimi (4 kurum -

%26,6), Basılı Süreli Yayınlar Birimi (4 kurum - %26,6), Açık Arşiv ve Kurumsal Arşiv Birimi'nin (4 kurum - %26,6) yer aldığı görülmektedir. Tablo 3'e göre, üniversite kütüphanelerinde kişisel verilerin en az işlendiği birimler arasında ise, Kalite Yönetim Birimi (1 kurum - %6,6) ve Satın Alma ve Muhasebe Birimi (1 kurum - %6,6) yer almaktadır. Diğer seçeneğini işaretleyen bir kurum (%6,6) ise, üniversite kütüphanelerinin merkezi bir yapıya sahip olması nedeniyle, kullanıcılara yönelik kişisel verilerin birim kütüphaneleri tarafından işlendiğini belirtmiştir. Henkoğlu ve Uçak'ın (2018, s.55), yaptıkları bir araştırmada *"katılımcıların (%86,7) üniversite kütüphanelerinde danışma hizmetleri kapsamında tutulan bilgilerin kullanıcılarla ilişkilendirmediğini"* ortaya çıkarmışlardır. Yine yazarlar konuyla ilgili olarak elde edilen bu bulguların, üniversite kütüphanelerinde "*bilgi güvenliğine ilişkin önlemler kapsamında bilinçli olarak yapılan bir uygulamanın sonucu olduğunun söylenemeyeceğini"* dile getirmişlerdir. Ancak, araştırmamızda bulunan Tablo 2, Tablo 3 ve Tablo 4'e bakıldığında danışma birimleri olarak da nitelendirilen ödünç verme birimlerinde kullanıcı verilerinin işlendiği ortaya çıkmaktadır. Tablo 6'dan sonra gelen Tablo 7'de ise, üniversite kütüphanecileri yöneticilerine kütüphanelerinde tutulan kişisel verileri hangi amaçlarla kullandıkları sorulmuştur (Bkz. Tablo 7).

Tablo 7. Kütüphanenizde tutulan kişisel verileri hangi amaçlarla kullanıyorsunuz? (S=15)

	S	**%**
Hizmet sunumu	11	73,3
Raporlama/kullanım istatistiği alma (etki değerlendirme)	11	73,3
Kütüphane güvenliğini sağlama	9	60
Hizmet geliştirme	8	53,3
Koleksiyon güvenliğini sağlama	7	46,6

Tablo 7'ye göre araştırmamızdaki üniversite kütüphaneleri kişisel verileri çoğunlukla hizmet sunumu (11 kurum - %73,3) ve raporlama/kullanım istatistiği alma (11 kurum - %73,3) amacıyla kullanmaktadır. Bu amacı takiben sırasıyla kütüphane güvenliğini sağlama (9 kurum - %60), hizmet geliştirme (8 kurum - %53,3) gelmektedir. Diğer taraftan, kütüphanelerde kişisel verilerin en az koleksiyon güvenliğini sağlama amacıyla (7 kurum - %46,6) kullanıldığı görülmektedir (Tablo 7). Tablo 7'de ki bulgulara göre, kişisel verilerin farklı amaçlarla üniversite kütüphanelerinde kullanıldığı ortaya çıkmaktadır. Tablo 7'de görüldüğü üzere, yöneticiler kurumlarında kişisel verileri kütüphane güvenliğini sağlama ve koleksiyon güvenliğini sağlama amacıyla da kullanmaktadır. Üniversite kütüphaneleri, üniversitenin öğretim üyelerine, öğrencilerine, çalışan personellerine, mezunlara ve dış ziyaretçilere hizmet sunumu yapmaktadır. Bu

bağlamda, üniversite kütüphanelerinde güvenliğin oluşturulması ve kütüphanenin kaynaklarına zarar gelmemesi için kapı girişlerinde turnike sistemleri bulundurulmaktadır. Bununla birlikte, kütüphaneye iade edilmek koşuluyla ödünç alınan eserlerin, kütüphaneye iade edilmemesi, iade gününün geciktirilmesi veya esere zarar verilmesi durumlarında üniversite kütüphaneleri kullanıcılara karşı bazı güvenlik önlemleri ve kuralları ortaya koymuştur. Bu durumda, turnike sistemlerinde ve otomasyon sistemlerinde kişisel veriler kütüphanenin güvenliğini sağlamak amacıyla kullanılmaktadır. Aynı zamanda, kullanıcıların kullanıcı adı ve şifresini kullanarak erişim sağladıkları bilgisayarlarda, kullanıcıların verilerinin ve kayıtlarının sürekli olarak temizlenmesi kütüphane güvenliğinin sağlanmasına örnek olarak gösterilebilmektedir. Daha önceki sorularda üniversite kütüphanelerinde tutulan kişisel verilerin neler olduğunu, kişisel verilerin toplanmasını, kayıt altına alınmasını, üniversite kütüphanelerinde kişisel verilerin yönetiminden sorumlu bir personelin olup olmadığını, kişisel verilerin sınıflandırılmasına yönelik düzenlemeleri, kişisel verilerin en çok işlendiği birimleri ve kişisel verilerin tutulma amacına yönelik elde edilen bulgulara değinilmiştir. Bu sorulara ek olarak, Tablo 8'de üniversite kütüphanelerinde işlenen kişisel verilerin nerede saklandıklarına yönelik bulgulara yer verilmiştir.

Tablo 8. Kütüphanenizde kullanıcılara ve personele ait kişisel veriler nerede tutulmaktadır? (S=14)

	S	**%**
Kütüphanenin kendi sunucularında	11	78,6
Üniversitenin merkezi sunucularında	8	57,1
Hizmet aldığımız firmanın/şirketin sunucularında	5	35,7
Şifreli korumalı dolaplarda	4	28,6
Şifresiz/korumasız klasör ya da dolaplarda	1	7,1

Birden çok seçeneğin işaretlenebildiği Tablo 8 incelendiğinde, yöneticilerin neredeyse tamamı (11 kurum - %78,6) kütüphanenin kendi sunucularında kişisel veri tuttuklarını işaretlerken, yöneticilerin yarısından fazlası (8 kurum - %57,1) üniversitenin merkezi sunucularında kişisel veri tuttuklarını işaretlemiştir. Bununla birlikte, kütüphanelerde kişisel verilerin hizmet alınan firmanın/şirketin sunucularında (5 kurum), şifreli korumalı dolaplarda (4 kurum) ve şifresiz/korumasız klasör ya da dolaplarda (1 kurum) da tutulduğu ortaya çıkmıştır. Tablo 8'de yer alan bulgular doğrultusunda, üniversite kütüphanelerinde kullanıcılara ve personellere yönelik kişisel verilerin birden fazla ortamda tutulduğunu ifade etmek mümkündür. Bu soruya yanıt vermeyen 1 kurum ise, kişisel verilerin korunması ile ilgili politika eksikliğinin olması ve söz konusu politikanın

hazırlanmaması nedeniyle soruyu yanıtlamak istemediğini dile getirmiştir. Yöneticilere, kullanıcılara/personele ait kişisel verilerin hangi gerekçe ile kullanılmasına ve paylaşılmasına izin verildiği de birden fazla seçeneklerin işaretlenebildiği bir soru olarak yöneltilmiştir (Tablo 9).

Tablo 9. Kullanıcılara ait kişisel verilerin hangi gerekçe ile kullanılmasına ve paylaşılmasına izin verilmektedir? (S=14)

	S	%
Üniversite üst yönetimi ya da güvenlikten sorumlu birimler tarafından istenmesi halinde	10	71,4
Yasal çerçevede savcılık tarafından istenmesi halinde	9	64,3
İstatistik amaçlı olarak istenmesi halinde	7	50
Veri sahibinin kendisi hakkında tutulan bilgileri istemesi halinde	5	35,7
Bilgi Edinme Hakkı Kanunu çerçevesinde	4	28,6
Bilimsel araştırmalarda kullanmak şartıyla	3	21,4
Kamu menfaati görülmesi halinde (kişisel haklar gözetilmeksizin)	-	-
Kullanıcı/personel bilgileri hangi sebeple olursa olsun verilmez	1	7,1

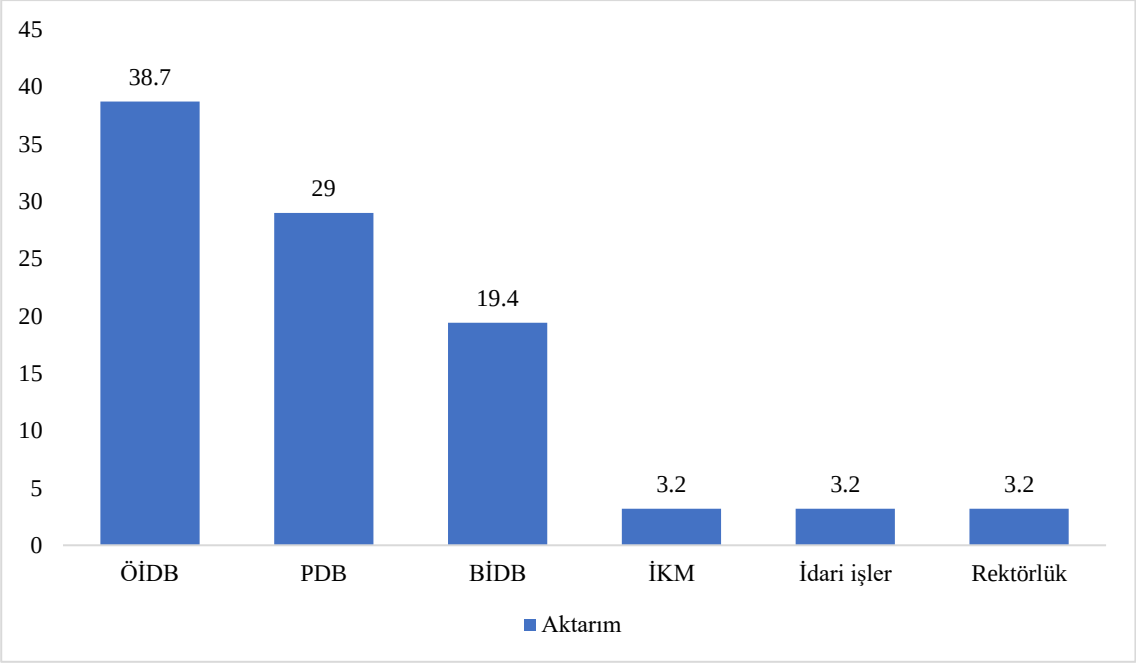
Tablo 9 incelendiğinde kullanıcılara ait 'kişisel verilerin birden fazla gerekçe ile kullanılmasına ve paylaşılmasına' izin verildiği anlaşılmaktadır. Söz konusu gerekçeler arasında ise özellikle, üniversite üst yönetimi ya da güvenlikten sorumlu birimler tarafından istenmesi halinde, yasal çerçevede savcılık tarafından istenmesi halinde, istatistik amaçlı istenmesi halinde kişisel verilerin paylaşılmasına izin verilmesi bulunmaktadır. Henkoğlu ve Uçak tarafından (2015) tarafından yapılan araştırmadan alınan bu soruda, araştırma bulgularımızla benzerlikler bulunmaktadır. Örneğin, Henkoğlu ve Uçak'ın araştırmalarında (2015) üniversite üst yönetimi ya da güvenlikten sorumlu birimler tarafından istenmesi halinde, yasal çerçevede savcılık tarafından istenmesi halinde araştırma bulgularımızla benzerlik taşımaktadır. Üniversite kütüphanelerinde kişisel verilerin kullanılmasına ve paylaşımına ilişkin elde edilen bulgulardan (Tablo 9) sonra, üniversite kütüphanelerinde diğer üniversite birimlerinden kişisel verileri nasıl aktardıklarına yönelik bulgular Tablo 10'da gösterilmektedir.

Tablo 10. Kütüphanenize üniversitenin diğer birimlerinden kişisel veriler nasıl aktarılıyor? (S=14)

	S	%
Yetkili kişilerin ya da bilgi işlem uzmanlarının çalışmalarıyla	5	35,7
Kullandığımız bütün sistemler birbirine entegre bir şekilde çalıştığından kişisel veriler otomatik olarak PDB, BİDB, ÖİDB gibi birimlerden aktarılmaktadır	4	28,6
Diğer	5	35,7

Tablo 10'da üniversite kütüphanelerinde diğer üniversite birimlerinden kişisel verilerin nasıl aktarıldığına yönelik veriler yer almaktadır. Kurumların 5'i (%35,7) yetkili kişilerin

ya da bilgi işlem uzmanlarının çalışmalarıyla kişisel verileri aktardığını belirtmiştir. Diğer seçeneğini işaretleyen yöneticilerden biri e-mail ile kişisel veri aktardıklarını belirtirken bir diğeri, kişisel veri aktarmadıklarını ifade etmiştir. Diğer seçeneğini işaretleyen başka bir yönetici ise bu soruya, *"Öğrenci İşleri ve Bilgi İşlem Müdürlüğü ile çalışmalar başlatıldı. 2 ay içerisinde, kütüphane üyelik işlemleri için gerekli kişisel ve iletişim bilgileri kütüphane otomasyon programına otomatik olarak aktarılacak"* yanıtını vermiştir. Görüşme yapılan kurumların 1'i (%6,7) ise bu soruya yanıt vermemiştir. Soruya yanıt vermeyen bu yönetici ise, üniversitenin diğer birimlerinden kişisel veri aktarmadıklarını belirtmiştir. Üniversite kütüphanelerinde, farklı yöntemlerle (Tablo 10) aktarılan kişisel verilerin üniversitenin hangi birimleriyle paylaşıldığı Şekil 6'da gösterilmektedir.



Şekil 6. Üniversite kütüphanesinde kişisel veri aktarımının gerçekleştiği birimler

Şekil 6 incelendiğinde, üniversite kütüphanelerinde en çok kişisel veri aktarımının gerçekleştirildiği üç birim ÖİDB (12 kurum - %38,7), PDB (9 kurum - %29) ve BİDB'dir (6 kurum - %19,4). Daha sonraki sıraları ise, İnsan Kaynakları Merkezi (İKM) (1 kurum - %3,2), İdari İşler Birimi (1 kurum - %3,2) ve Rektörlük (1 kurum - %3,2) almaktadır. Bu soruya yanıt veren bir yönetici ise, *"Personel programı yeniden yapılmaktadır. Program tamamlandıktan sonra, kütüphane otomasyonu vb. programların entegrasyonu planlanmaktadır"* yanıtını vermiştir.

Tablo 11. Üçüncü parti kuruluşlar kütüphanenizde tutulan hangi sistemlerdeki kişisel verilere ulaşabiliyor? (S=15)

	S	%
Kütüphane otomasyon sistemi	9	60
Kütüphanenin abone olduğu veri tabanı sistemleri	5	33,3
Üçüncü parti kuruluşlarla kişisel veri paylaşmıyoruz	4	26,7
Kütüphane kurumsal arşiv sistemi	3	20
Kapı (giriş-çıkış) turnike sistemleri	2	13,3

Tablo 11'de üniversite kütüphanelerinde üçüncü parti kuruluşların kütüphanede tutulan hangi sistemlerdeki kişisel verilere erişim sağlayabildikleri sorulmuştur. Kurumların 9'u (%60) üçüncü parti kuruluşların kütüphane otomasyon sistemindeki kişisel verilere erişim sağladıklarını belirtmiştir. Buna ek olarak, kurumların 5'i (%33,3) üçüncü parti kuruluşların kütüphanenin abone olduğu veri tabanı sistemlerinde tutulan kişisel verilere erişim sağladıklarını, 4 kurum ise (%26,7) üçüncü parti kuruluşlarla kişisel veri paylaşmadıklarını belirtmiştir. Kısaca, Tablo 11'e göre, üniversite kütüphanelerinde üçüncü parti kuruluşlar kütüphane otomasyon sistemi, kütüphanenin abone olduğu veri tabanı sistemleri, kütüphane kurumsal arşiv sistemi ve kapı (giriş-çıkış) sistemlerinde tutulan kişisel verilere erişim sağlayabilmektedir.

Yöneticilere sorulan bir diğer soru ise, kütüphanede tutulan kişisel verilerin kullanımına yönelik olarak kullanıcılardan onay alıp almadıkları olmuştur. Bu konuda 8 kurum (%53,3) kullanıcılardan bir onay almadığını belirtirken, 7 kurum (%46,7) ise kullanıcılardan onay alındığını belirtmiştir. Onay alınmadığını belirten bir kütüphanede yöneticisi ise *"kütüphanedeki kişisel verilerin hizmet sunumu dışında farklı amaçla kullanımının olmadığını"* ifade etmiştir. Bu soruyla ilgili bir soru da, *Bilgi Dünyası* dergisinde yayınlanan bir makalede (Henkoğlu ve Uçak, 2015, s.59) yöneticilere sorulmuştur. Söz konusu soru üniversite kütüphanelerinde *"elde edilen kişisel bilgilerin amaç dışı kullanılmayacağı, izinsiz olarak paylaşılmayacağı ve bu verilerin korunacağına ilişkin olarak veri sahibine yazılı taahhütte bulunup bulunmadıkları"* olmuştur. Sorulan bu soruya ilişkin alınan yanıtlara göre, yöneticilerin neredeyse tamamı olarak nitelendirebileceğimiz %93,3'lük bir oranla kişisel bilgilerin toplanması sürecinde veri sahibine herhangi bir sözleşme yapmadıkları tespit edilmiştir (Henkoğlu ve Uçak, 2015, s.59). Yöneticilere sorulan aydınlatma metnine yönelik alınan onaya ek olarak,

mevcut olan aydınlatma metninin içeriğinin neleri kapsadığı 20. soru olarak yöneltilmiştir (Tablo 12).

Tablo 12. Aydınlatma metninin içeriği aşağıdakilerden hangilerini kapsamaktadır? (S=7)

	S	%
Kişisel verilerin tutulma amacını kapsamaktadır	6	85,7
Kişisel verilerin saklanma süresini kapsamaktadır	1	14,3
Kişisel verilerin silinmesine yönelik bilgileri kapsamaktadır	1	14,3
Kişisel verilerin yeniden kullanımına yönelik bilgileri kapsamaktadır	1	14,3

Tablo 12 incelendiğinde, üniversite kütüphane yöneticilerinin, 6'sı (%85,7) aydınlatma metninin kişisel verilerin tutulma amacını kapsadığını belirtmiştir. Buna karşın, 7 üniversite kütüphanesi içerisinden yalnızca bir kütüphanede aydınlatma metninin içeriğinde kişisel verilerin saklanma süreleri, kişisel verilerin silinmesine yönelik bilgiler ve kişisel verilerin yeniden kullanımına yönelik bilgiler yer almaktadır. Yöneticiler arasında rıza onay metninin içeriğine yönelik bir bilgilendirme yapılmadığını ifade edenlerin oranı ise, (1 kurum) %14,3'dür. Söz konusu bulgular, aydınlatma metinlerinin kişisel verilerin yönetilmesine yönelik temel unsurları içermesi açısından eksik olduğunu yansıtmaktadır. Çünkü, kişisel verilerin yönetilmesi de belge yönetim süreçlerinde olduğu gibi belli bir döngüye (düzenleme, silme, paylaşma vb.) dayanmaktadır ve bu döngünün yazılı bir düzenlemeye temel oluşturması gerekmektedir. Kullanıcılardan onay almadıklarını belirten bir yönetici, söz konusu metni planladıklarını belirterek, planlanan metnin içerisinde kişisel verilerin tutulma amacı, hangi kişisel verilerin farklı amaçlarla kullanılabileceği bilgisi, kişisel verilerin saklanma süreleri ve kişisel verilerin yeniden kullanımına yönelik bilgileri içereceğini dile getirmiştir.

Görüşme formunda üçüncü parti[14] kuruluşlarla ilgili olarak yöneticilere sorulan bir diğer soru ise, üniversite kütüphanelerinin üçüncü parti kuruluşlarla yaptığı anlaşmalarda kişisel verilerin korunmasına yönelik gizlilik sözleşmesi yapıp yapmadıkları olmuştur. Kurumların 6'sı (%40,0) kişisel verilerin korunmasına yönelik gizlilik sözleşmesi yaptıklarını belirtirken, 5'i (%33,3) gizlilik sözleşmesi yapmadıklarını belirtmiştir. Geriye kalan 4 kurum (%26,7) ise kısmen gizlilik sözleşmesi yaptıklarını ifade etmiştir.

[14]Üniversite kütüphaneleri tarafından satın alınan kütüphane otomasyon sistemleri birer üçüncü parti kuruluş olarak sayılabilmekte ve bu kuruluşların sözleşmelerinde kişisel verilerin korunmasına yönelik bildirim anlaşmaları yapılabilmektedir.

Bu durum bazı anlaşmalarda kişisel verilere yönelik bir gizlilik sözleşmesi olmadan anlaşmanın yapıldığını ya da yöneticilerin konu ile ilgili bilgi eksikliklerinin olduğunu göstermektedir.

Kişisel verilerin yönetilmesi aşamasında, kişisel verilerin kaldırılması (silme/yok etme/ anonimleştirme) işlemleri yer almaktadır. Kişisel Verileri Koruma Kurumu (2018, s.6-16), kişisel verilerin ilgili 'kullanıcılar' için hiçbir şekilde erişilemez ve tekrar kullanılmaz hale getirilmesi işlemine kişisel verilerin silinmesi, kişisel verilerin 'hiç kimse' tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemine kişisel verilerin yok edilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ise anonimleştirme işlemi olarak tanımlamaktadır. Üniversite kütüphanelerinde kişisel verilerin kaldırılmasına yönelik uygulanan işlemlere ait bulgular ise, Tablo 13'de sunulmuştur.

Tablo 13. Kişisel verilerin kaldırılması (silme/yok etme/anonimleştirme) aşamasında hangi işlemler yapılmaktadır (S=15)

	S	**%**
Silme/Yok etme/Anonimleştirme	9	60
Hiçbiri	1	6,7
Diğer	5	33,3

Tablo 13'e göre, 9 kurum (%60) otomasyon sistemlerindeki kişisel verileri silme/yok etme/anonimleştirme işlemlerini gerçekleştirerek kaldırdıklarını belirtmiştir. Diğer seçeneğini işaretleyen bir kurum kütüphanelerde kişisel verilerin kaldırılmasına ilişkin olarak bu soruya, *'kullanıcı işlemleri birim kütüphaneleri tarafından yürütülmektedir'* yanıtını verirken iki kurum, kişisel verilere yönelik pasifleştirme ve yedekleme işlemi yaptığını belirtmiştir.

Kütüphanede tutulan kişisel verilerin saklanmasına yönelik bir uygulamanın olup olmadığı yöneticilere sorulmuş ve alınan yanıtlar neticesinde üniversite kütüphanelerinin çoğunda kişisel verilerin saklanmasına yönelik bir uygulamanın olmadığı (8 kurum-%53,3) tespit edilmiştir. Bununla birlikte, kişisel verilerin saklanmasına yönelik uygulamaların geliştirilme aşamasında olduğunu belirten kurumların sayısı 5'iken (%33,3), kişisel verilerin saklanmasına yönelik uygulamaların bulunduğunu belirten kurumların sayısı ise 2'dir (%13,3). Diğer taraftan, yöneticilerin biri otomasyon sistemlerinde yer alan kişisel verilerin sonsuza kadar silinmeyeceğini dile getirmiştir.

Araştırmamızda elde edilen bu sonuçlar, Henkoğlu (2015b, s.125) tarafından yapılan araştırma sonuçlarıyla da örtüşmektedir.

Kişisel verilerin yönetilmessi sürecinde, dikkat edilmesi gereken unsurlardan birisi belge yönetim süreçlerinde olduğu gibi verilerin sistematik ve hiyerarşik olarak düzenlenmesi ve kategorilendirilmesidir. Bu durum ise, kişisel veri koleksiyonlarının oluşturulmasıyla mümkün olabilmektedir. Kişisel veri koleksiyonu, kişisel verilerin sınıflanmasına yönelik olabilmektedir. Örneğin, kütüphane otomasyon sistemlerine kullanıcıların (akademisyen, öğrenci, mezun vb.) bir liste veya veri tabanlarında tutulması kişisel veri koleksiyonlarına örnek olarak gösterilebilmektedir. Bununla birlikte, kütüphane bünyesinde yapılan etkinlik ve faaliyetlere ilişkin kayıtlarda da kişisel veri koleksiyonları oluşturulabilmektedir. Diğer taraftan, bu koleksiyonlar, haftalık, aylık veya yıllık tutulabilmektedir. Bu bağlamda, yöneticilere sorulan diğer bir soru ise, kütüphanede kişisel veri koleksiyonunun bulunup bulunmadığı olmuştur. Bu soruya ek olarak, kütüphanecilere otomasyon sistemlerinde tutulan kişisel veriler ile ilgili bir soru yöneltilmiştir.

Tablo 14'ün ilk sorusunda yöneticilerin neredeyse tamamı (14 kurum - %93,3) kütüphanelerinde kişisel veri koleksiyonunun olmadığını belirtmiştir. Bir (%6,7) yönetici ise kütüphanede akademisyen, öğrenci, personel gibi kullanıcı gruplarına yönelik kişisel veri koleksiyonu bulundurduğunu dile getirmiştir. Tablo 14'ün ikinci sorusu olan *"Şu anda aktif olmayan ancak sistemlerinizce tutulan kişisel verilere tekrar ihtiyacınız olacağını düşünüyor musunuz?"* sorusuna hayır yanıtını verenlerin sayısı 8 kurum (%61,5), tekrar ihtiyaç olacağını düşünenlerin sayısı ise 5 kurumdur (%38,5). Bir kurum, sistemlerde *'kişisel verinin tutulmadığını'* belirterek bu soruyu boş bırakmıştır.

Tablo 14. Kişisel verilere yönelik sorular

	Evet		**Hayır**		**Toplam**	
	S	**%**	**S**	**%**	**S**	**%**
Kütüphanenizde kişisel veri koleksiyonunuz var mı?	1	6,7	14	93,3	15	100
Şu anda aktif olmayan ancak sistemlerinizde tutulan kişisel verilere tekrar ihtiyacınız olacağını düşünüyor musunuz?	5	38,5	8	61,5	13	100
Kütüphanenizde hassas verilerin yönetilmesini içeren sizin ya da üst yönetimin imzaladığı, belirli zaman aralıklarında güncellenen bir politikanız var mı?	4	26,7	11	73,3	15	100

Sistemlerde tutulan kişisel verilere tekrar ihtiyaç olacağını dile getiren bir diğer yönetici ise bu soruya, *"Evet, mezun bir kullanıcı, lisansüstü eğitime başlayabilir. Bu durumda, tekrar kullanıcı kaydı oluşturmak gerekecektir."* yanıtını vermiştir. Evet yanıtını veren başka bir yönetici ise, *"Geriye dönük herhangi bir güvenlik sorgulamaları için"* cevabını vererek sistemlerdeki kişisel verilere tekrar ihtiyaç duyacaklarını ifade etmiştir. Alınan bu yanıtta ise, kütüphanelerde kişisel verilerin 'güvenlik' ve 'gizlilik' boyutları ön plana çıkmaktadır. Bu soruya evet yanıtını veren üçüncü bir yönetici ise, *"hizmet geliştirme, geçmiş istatistik değerlendirme"* için kişisel verilere ihtiyaç duyulacağını belirtmiştir. Alınan yanıtlardan hareket edilerek, Tablo 7'de elde edilen bulgularda olduğu gibi, üniversite kütüphanelerinde kişisel veriler farklı amaçlarla (hizmet sunumu, güvenlik, kullanıcı kayıtlarının oluşturulması vb.) kullanılabilmektedir.

Yöneticilere sorulan diğer bir soru ise, "Kütüphanenizde kişisel verilerin yönetilmesini içeren sizin ya da üst yönetimin imzaladığı, belirli zaman aralıklarında güncellenen politikanız var mı?" sorusu olmuştur. Bu soruya, hayır seçeneğini işaretleyen kurumların sayısı 11 (% 73,3) iken, evet seçeneğini işaretleyen kurumların sayısı 4'tür (%26,7). Bu soruya evet yanıtını veren bir yönetici, *"üst yönetim tarafından bağlı oldukları bir politikanın bulunduğunu"* ifade etmiştir. Kişisel verilere ilişkin sorulan diğer bir soru ise, üniversite kütüphanelerinde kişisel verilerin yönetilmesine yönelik olarak imzalanan kişisel verilerin korunması politikasına duyulan gereksinimin düzeyleri olmuştur (Bkz. Tablo 15).

Tablo 15. Kütüphanenizde kişisel verilerin yönetilmesini içeren sizin (kütüphane yöneticisi) ya da üst yönetimin imzaladığı politikaya ne düzeyde ihtiyaç duyuyorsunuz?

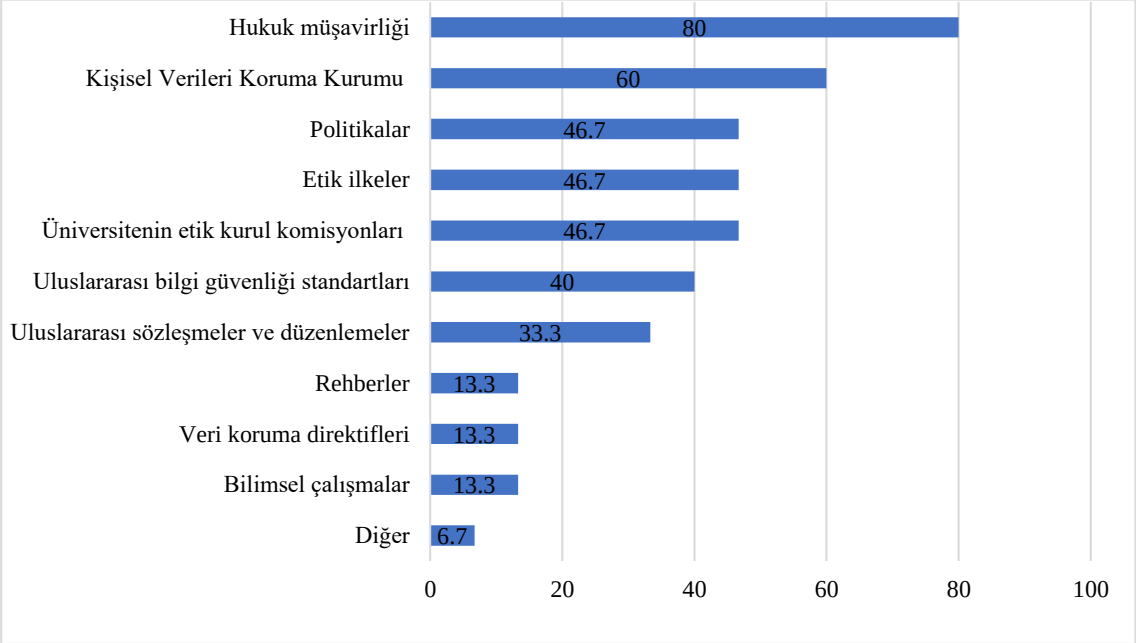
	S	**%**
İhtiyaç duyuyoruz	6	46,2
Fikrim yok	4	30,8
İhtiyaç duymuyoruz	3	23,1
Toplam	13	100

($\bar{x}$=2,76, σ=1,36)

Kütüphane kurumlarının 6'sı (%46,2) kişisel verilerin yönetilmesini içeren politikaya ihtiyaç duyduklarını, 4 kurum (%30,8) fikrinin olmadığını, 3 kurum (%15,4) ise söz konusu politikaya ihtiyaç duymadıklarını belirtmiştir (Tablo 15). İki kurum ise bu soruya yanıt vermemiştir. Bir kurum ise, hassas verilerin yönetilmesini içeren politikaya 'kütüphane bazında ihtiyaç duymadıklarını ancak kurumsal politika bazında' ihtiyaç

duyduklarını belirtmiştir. Araştırma kapsamında, ele alınan başka bir soru ise, yöneticilerin kütüphanelerde bir sorunla karşı karşıya kaldıklarında başvurulan kaynakların neler olacağıdır (Şekil 7).

Şekil 7. Kütüphanede herhangi bir sorunla karşılaşsaydınız başvuracağınız kaynak hangisi olurdu? (S=15)



Yöneticilerden alınan yanıtlara göre, kütüphanede herhangi bir sorunla karşılaşıldığında başvurulan kaynaklar arasında en çok hukuk müşavirliği, Kişisel Verileri Koruma Kurumu ve daha sonra ise politikalar, etik ilkeler ve etik kurul komisyonları yer almıştır. Diğer seçeneğini işaretleyen bir yönetici ise kişisel verilerin yönetilmesine yönelik uygulamalara yönelik olarak, *"6698 sayılı Kişisel Verilerin Korunması Kanunu gereği yapılmak zorunda ve yapılıyor"* yanıtını vermiştir.

Görüşme formuna katılan yöneticilere sorulan son soru ise, '6698 sayılı Kişisel Verileri Koruma Kanunu kapsamında kütüphaneye yönelik gerçekleştirilen bir uygulamanın olup olmadığı' olmuştur. 12 yönetici kanun kapsamında herhangi bir uygulamanın gerçekleştirilmediğini belirtirken, geriye kalan üç yöneticiden alınan yanıtlar ise şu şekildedir:

1. *"Kişisel Verileri Koruma Kurumundan bir uzmanın seminer vermesi sağlandı. Üniversitemizin Kişisel Verileri Koruma Komisyonu'nda kütüphanemizden bir personel görevlendirildi."*

2. *"Üniversiteye kayıt olurken öğrencilerimize, Kişisel Verileri Koruma Kanunu'na uygun olarak ve başka bir amaçla kullanmayacağımızı taahhüt ederek, kütüphaneye üye olması için kullanacağımızı beyan ederek; rıza belgesi imzalatıyoruz."*
3. *"İdari birim olarak faaliyet yürütüyoruz."*

4.1.2. Bilgi Güvenliği Uygulamalarına Yönelik Bulgular

Görüşme formunun bu bölümünde üniversite kütüphanelerinde bilgi güvenliği uygulamalarına (kurumsal, bina, koleksiyon, kullanıcı, yazılım ve donanım) ilişkin bulgular sunulacaktır.

Tablo 16. Kurumsal Güvenlik Uygulamalar

Güvenlik Ölçümleri	Evet		Hayır		Geliştirilme Aşamasında		Toplam	
	S	%	S	%	S	%	S	%
Üst yönetim tarafından onaylanmış bilgi güvenliği politika belgesi var mı?	4	26,7	9	60	2	13,3	15	100
Kütüphanenizde ISO standartlarına uygun olarak kalite yönetim sistemi ve/veya bilgi güvenliği yönetim sistemi bulunmakta mıdır?	6	40	8	53,3	1	6,7	15	100
Kütüphanenizdeki bilgi güvenliği politikasında kişisel verilerin korunması ile bilgi güvenliği birlikte ele alınıyor mu?	3	20	8	53,3	4	26,7	15	100
Bilgi güvenliği denetlemeleri kütüphane içerisinden bir personel tarafından mı yapılmaktadır?	5	33,3	9	60	1	6,7	15	100
Kütüphaneye yeni bir sistem alınırken güvenliği denetleniyor mu?	13	86,7	2	13,3	-	-	15	100
Kütüphanenizde bilgi güvenliği risk analizi yapılmakta mıdır?	4	26,7	7	46,7	4	26,7	15	100
Kütüphanenizde özel hayatın gizliliğine yer veren etik ilkeler var mı?	10	66,7	4	26,7	1	6,7	15	100

Tablo 16'da üniversite kütüphanelerinde uygulanan kurumsal güvenlik uygulamalarını belirlemek amacıyla oluşturulan sorulara yönelik yanıtlar yer almaktadır. İlgili sorulara bakıldığında genel olarak kütüphanelerde bilgi güvenliği politika belgesi, kalite yönetim sistemi/bilgi güvenliği yönetim sistemi bulunup bulunmadığı, politikaların içeriği, bilgi güvenliği denetlemeleri, sistemlerin güvenliği, bilgi güvenliği risk analizi ve özel hayatın gizliliğine yönelik olmak üzere yedi soru yer almaktadır.

Ankara'daki üniversite kütüphanelerinde gerçekleştirilen kurumsal güvenlik uygulamalarına yönelik verilen yanıtların dağılımları incelendiğinde: 9 kurumda (%60) üst yönetim tarafından onaylanmış bilgi güvenliği politika belgesi olmadığı; 8 kurumda (%53,3) ISO standartlarına uygun olarak kalite yönetim sistemi ve/veya bilgi güvenliği

yönetim sisteminin yer almadığı; 8 kurumda (%53,3) bilgi güvenliği politikalarında kişisel verilerin korunması ile bilgi güvenliği politikalarına birlikte yer verilmediği; 9 kurumda (%60) bilgi güvenliği denetlemelerinin kütüphane içerisinden bir personel tarafından yapılmadığı; 13 kurumda (%86,7) yeni bir sistem alınırken güvenilirliğinin denetlendiği; 7 kurumda (%46,7) bilgi güvenliği risk analizinin gerçekleştirilmediği; 10 kurumda (%66,7) ise özel hayatın gizliliğine yer veren etik ilkelerin bulunduğu görülmüştür (Tablo 16). Görüşme formuna katılan yöneticilere yöneltilen bilgi güvenliği uygulamalarına ilişin olarak sorulan bir diğer soru ise, bina güvenliği uygulamaları olmuştur (Bkz. Tablo 17).

Tablo 17. Bina Güvenliği

Güvenlik Ölçümleri	Evet		Hayır		Geliştirme Aşamasında		Toplam	
	S	%	S	%	S	%	S	%
Kütüphanenizde bina güvenliğine yönelik bir politikanız var mı?	6	40	6	40	3	20	15	100
Kütüphanenizin binası kütüphane binası olarak mı tasarlandı?	7	46,7	8	53,3	-	-	15	100
Kütüphanenizde iç hava kalitesi ölçümleri yapılıyor mu?	8	53,3	7	46,7	-	-	15	100
Kütüphanenizde nem ölçümleri yapılıyor mu?	6	40	9	60	-	-	15	100
Kütüphanenizde gürültü ölçümleri yapılıyor mu?	5	33,3	10	66,7	-	-	15	100
Kütüphane binasında ışıklandırma yeterli mi?	13	86,7	1	6,7	1	6,7	15	100
Deprem, sel vb. afetler için erken uyarı sistemleriniz var mı?	7	46,7	6	40	2	13,3	15	100

Bu kapsamda, yöneticilere bina güvenliğine yönelik politika, kütüphane binası, kütüphane iç hava kalitesi ölçümleri, nem ölçümleri, gürültü ölçümleri, binanın ışıklandırması ve deprem, sel vb. afetler için erken uyarı sistemlerinin bulunup bulunmadığı sorulmuştur.

Ankara'daki üniversite kütüphanelerinde gerçekleştirilen bina güvenliği uygulamalarına yönelik yöneticilerin yanıtları analiz edildiğinde: 6 kurumda (%40) bina güvenliğine yönelik politika bulunurken, 6 kurumda (%40) bina güvenliğine yönelik politika bulunmamakta; 15 kurum arasından 8 kurum (%53,3) binasının kütüphane binası olarak tasarlanmadığı; 8 kurumda (%53,3) iç hava kalitesi ölçümlerinin yapıldığı; 9 kurumda (%60) nem ölçümlerinin yapılmadığı; 5 kurumda (%33,3) gürültü ölçümleri yapılırken 10 kurumda (%66,7) gürültü ölçümlerinin yapılmadığı; 13 kurum (%86,7) binasında ışıklandırmanın yeterli düzeyde olduğu; 7 kurumda (%46,7) deprem, sel vb. afetler için erken uyarı sistemlerinin bulunduğu tespit edilmiştir.

Tablo 17'ye ek olarak bina güvenliğine yönelik uygulamaları ölçmek amacıyla yedi farklı soru (Tablo 18) daha katılımcılara yöneltilmiştir. Tablo 18 incelendiğinde bu soruların temel olarak, üniversite kütüphanelerinde doğal afetlere, acil durumlara karşı alınan önlem ve tedbirler, kütüphane binalarının denetlenmesi, kütüphane binalarında bina otomasyon sisteminin bulunup bulunmaması gibi sorulardan oluştuğu anlaşılmaktadır.

Tablo 18. Bina Güvenliğine Yönelik Diğer Bulgular

Güvenlik Ölçümleri	Evet		Hayır		Geliştirme Aşamasında		Toplam	
	S	%	S	%	S	%	S	%
Doğal afetlere karşı önlem ve tedbirlerinizi aldınız mı?	7	46,7	5	33,3	3	20	15	100
Kütüphanemizin tüm birimlerinde (Süreli Yayınlar, Arşiv vb.) insan ve koleksiyon güvenliğini sağlamak amacıyla tedbirler alındı mı?	9	60	4	26,7	2	13,3	15	100
Acil durumlara karşı levhalar ve tabelalar, yönlendirmeler var mı?	13	86,7	1	6,7	1	6,7	15	100
Bilgi güvenliği politikası içerisinde bina güvenliğine yer verildi mi?	6	40	5	33,3	4	26,7	15	100
Kütüphanenizin binası (iç-dış) bir denetleyici tarafından denetleniyor mu?	12	80	2	13,3	1	6,7	15	100
Kütüphanenizde bina otomasyon sistemleri (ısıtma- soğutma ve havalandırma, aydınlatma, yangın algılama ve alarm sistemleri) var mı?	13	86,7	2	13,3	-	-	15	100
Gerektiğinde emniyet, itfaiye vb. kuruluşlarla kimin ne zaman iletişim kuracağının ve olayın nasıl rapor edileceğini tarif eden bir prosedür mevcut mu?	7	46,7	7	46,7	1	6,7	15	100

Ankara'daki üniversite kütüphanelerinde bina güvenliğine yönelik olarak elde edilen diğer bulgular arasında ise: doğal afetler ve önlemlere karşı tedbirleri aldıklarını belirten 7 kurum (%46,7); kütüphanenin tüm birimlerinde insan ve koleksiyon güvenliğini sağlamak amacıyla tedbirler aldıklarını belirten 9 kurum (%60); acil durumlara karşı levhalar ve tabelalar, yönlendirmeler bulunduğunu belirten 13 kurum (86,7); bilgi güvenliği politikası içerisinde bina güvenliğine yer veren 6 kurum (%40); kütüphane binasının (iç-dış) bir denetleyici tarafından denetlendiğini belirten 12 kurum (%80); kütüphanelerin bina otomasyon sistemlerinin bulunduğunu ifade eden 13 kurum (%86,7); gerektiğinde emniyet, itfaiye vb. kurumlarla kimin ne zaman iletişim kuracağının ve olayın nasıl rapor edileceğini tarif eden bir prosedür bulunduran 7 kurum (%46,7) ve söz konusu prosedürü bulundurmayan 7 kurum (%46,7) bulunmaktadır (Tablo 18).

Tablo 19'da üniversite kütüphanelerinde koleksiyon güvenliği uygulamalarına yönelik kütüphane yöneticilerinin vermiş olduğu yanıtlara göre oranlar ve cevaplar yer almaktadır. Tablo 19'daki koleksiyon güvenliğine yönelik olarak sorulan sorular ise genel olarak, koleksiyonların güvenliğini ve korunmasını içeren ve koleksiyonların güvenliğine dair politikaların olup olmadığına yönelik sorulardan oluşmaktadır.

Tablo 19. Koleksiyon güvenliği uygulamaları

Güvenlik Ölçümleri	Evet		Hayır		Geliştirme Aşamasında		Toplam	
	S	%	S	%	S	%	S	%
Kütüphanenizde kütüphane koleksiyon güvenliğine yönelik yazılı bir politikanız var mı?	7	46,7	5	33,3	3	20	15	100
Koleksiyon güvenliği politikaları ve prosedürleri düzenli olarak gözden geçirilip güncelleniyor mu?	9	60	5	33,3	1	6,7	15	100
Kütüphanedeki çeşitli koleksiyonlara yönelik riskler (küflenme, yıpranma, hasar görme vb.) tanımlanıyor mu?	11	73,3	3	20	1	6,7	15	100
Acil durumlar ve güvenlik ihlali için uygun ve test edilmiş prosedürler bulunmakta mıdır?	7	46,7	5	33,3	3	20	15	100
Kayıp, hasar görmüş, yıpranmış koleksiyonlar için yedekleme politikanız var mı?	11	73,3	3	20	1	6,7	15	100

Kütüphane yöneticilerinin koleksiyon güvenliği uygulamalarına yönelik sorulara verdikleri yanıtlar incelendiğinde: kurumların 7'sinde (%46,7) kütüphane koleksiyon güvenliğine yönelik yazılı bir politika bulunduğu; kurumların 9'unda (%60) koleksiyon güvenliği politikaları ve prosedürleri düzenli olarak gözden geçirilip güncellendiği; 11 kurumda (%73,3) çeşitli koleksiyonlara yönelik risklerin tanımlandığı; 7 kurumda (%46,7) acil durumlar ve güvenlik ihlali için uygun ve test edilmiş prosedürlerin bulunduğu; kurumların 11'inde (%73,3) kayıp, hasar görmüş, yıpranmış koleksiyonlar için yedekleme politikasının olduğu belirlenmiştir.

Tablo 20'ye bakıldığında üniversite kütüphanelerinde koleksiyon güvenliğine yönelik diğer uygulamalar ele alınmıştır. Tablo 20'de yer alan güvenlik ölçümleri koleksiyonların güvenliğine yönelik olarak materyallerin kayıt altına alınması, materyallerin işaretlenmesi, güvenlik sistemlerinin yerleştirilmesi, giriş ve çıkışlara yönelik denetim uygulamaları, koleksiyonlara yönelik alınan güvenlik önlemleri, kütüphane materyallerinin yerleşimi ile ilgili sorulardan oluşmaktadır.

Tablo 20. Koleksiyon güvenliğine yönelik diğer uygulamalar

Güvenlik Ölçümleri	Evet		Hayır		Geliştirme Aşamasında		Toplam	
	S	%	S	%	S	%	S	%
Kütüphane tarafından edinilen tüm materyaller kayıt altına alınıyor ve numaralandırılıyor mu?	15	100	-	-	-	-	15	100
Tüm koleksiyonlar manyetik şeritlerle işaretlendi mi?	14	93,3	1	6,7	-	-	15	100
Güvenlik sistemleri izinsiz ve yetkisiz girişleri engellemek için kütüphanenin giriş, çıkış ve depo alanlarına yerleştirildi mi ? (elektronik anti hırsızlık sistemi, görsel kameralar, duman algılama sistemi, CCTV, manyetik algılama sistemi)	13	86,7	2	13,3	-	-	15	100
Genel ve özel koleksiyon alanlarına girişlere yönelik bir denetim uygulamanız var mı?	11	73,3	4	26,7	-	-	15	100
Koleksiyonları korumak için kütüphanelerde önleyici tedbirler alınıyor mu?	12	80	2	13,3	1	6,7	15	100
Rafların düzeni ve boyutları, oturma ve okuma alanlarının düzeni, yangın önleme ekipmanlarının yerleştirilmesi gibi işlemler TSE(Türk Standartları Enstitüsü) standartlarına uygun olarak yapıldı mı?	12	80	2	13,3	1	6,7	15	100

Görüşme formuna katılan yöneticilerden koleksiyon güvenliği uygulamalarına yönelik olarak elde edilen bulgular ise: 15 kurum (%100) kütüphane tarafından edinilen tüm materyallerin kayıt altına alındığını ve numaralandırıldığını; 14 kurum (%93,3) koleksiyonların manyetik şeritlerle işaretlendiğini; 13 kurum (%86,7) güvenlik sistemlerinin izinsiz ve yetkisiz girişimleri engellemek için kütüphanenin giriş, çıkış ve depo alanlarına yerleştirildiğini; 11 kurum (%73,3) kütüphanede genel ve özel koleksiyon alanlarına girişlere yönelik denetim uyguladıklarını; 12 kurum (%80) koleksiyonları korumak için kütüphanede önleyici tedbirler aldıklarını; 12 kurum (%80) rafların düzeni ve boyutları, oturma ve okuma alanlarının düzeni, yangın önleme ekipmanlarının yerleştirilmesi gibi işlemlerin TSE standartların uygun olarak yerleştirildiğini belirtmiştir. Tablo 21'de kütüphanelerde bilgi güvenliği unsurlarından birisi olan personel ve kullanıcı güvenliği ele alınmıştır. Tablo 21'deki güvenlik ölçümlerine bakıldığında sorular, personel ve kullanıcının güvenliğini sağlamaya yönelik politika, güvenlik soruşturması, iş ve işlemler için hassas görevler listesi, tedbirler ve önlemler, kişisel eşyalar için dolaplar/alanlar, bilgilendirme levhaları, kullanıcı şifreleri ve kullanıcıların görev listelerine yönelik sorulardan oluşmaktadır.

Tablo 21. Personel ve Kullanıcı Güvenliği

Güvenlik Ölçümleri	Evet		Hayır		Geliştirme Aşamasında		Toplam	
	S	%	S	%	S	%	S	%
Kütüphanenizde personel ve kullanıcı güvenliğine yönelik yazılı bir politikanız var mı?	4	26,7	7	46,7	4	26,7	15	100
Kütüphanenize personel alımı yapılmadan önce güvenlik soruşturması yapılıyor mu?	15	100	-	-	-	-	15	100
Kütüphanenizde yapılacak iş ve işlemler için hassas görevler listesi yapıldı mı?	6	40	6	40	3	20	15	100
Kütüphanenizde personelin güvenliğini sağlamak için tedbirler alındı mı?	12	80	2	13,3	1	6,7	15	100
Kütüphanenizdeki personelin kişisel eşyaları için kişisel dolaplar/alanlar var mı?	14	93,3	-	-	1	6,7	15	100
Kullanıcılar kütüphanenin ortak kullanım alanlarında kişisel eşyalarının güvenliği ile ilgili olarak işaret ve levhalarla bilgilendiriliyor mu?	14	93,3	1	6,7	-	-	15	100
Kullanıcı şifrelerinin belirlenmesi ve kullanılması ile ilgili güvenlik tedbirleri uygulanıyor mu?	14	93,3	-	-	1	6,7	15	100
Kütüphanenizde her bir personelin görev listesinde (tanımlarında) kullanıcı verilerinin güvenliği ve korunması konularına yer verildi mi?	6	40	5	33,3	4	26,7	15	100

Tablo 21'deki bulgulara göre: 7 kurumda (%46,7) personel ve kullanıcı güvenliğine yönelik yazılı bir politikanın bulunmadığı; 15 kurumda (%100) personel alımı yapılmadan önce güvenlik soruşturması yapıldığı; 6 kurumda (%40) yapılacak iş ve işlemler için hassas görevler listesinin[15] yapıldığı anlaşılmaktadır. Yine 6 kurumda (%40) hassas görevler listesinin yapılmadığını; 12 kurumda (%80) personelin güvenliğini sağlamak için güvenlik tedbirlerinin alındığı; 14 kurumda (%93,3) personellerin kişisel eşyaları için dolaplar/alanlar olduğu; 14 kurumda (%93,3) kişisel eşyaların güvenliği ile ilgili bilgilendirilme yapıldığı; 14 kurum (%93,3) kullanıcı şifrelerinin belirlenmesi ve kullanıcı kullanılması ile ilgili tedbirleri aldıklarını; 6 kurum (%40) kütüphanedeki her bir personelin görev listesinde kullanıcı verilerinin güvenliği ve korunması konularına yer verdiklerini belirtmiştir.

Tablo 22'de üniversite kütüphanelerinde yazılım ve donanım güvenliği uygulamalarına yönelik görüşme formuna yanıt veren yöneticilerden elde edilen bulgular yer almaktadır.

[15] Örneğin: http://sgdb.ankara.edu.tr/files/2012/12/hassas-g%C3%B6revler_bilgi-notu.docx (Kayrancıoğlu).

Tablo 22 incelendiğinde, üniversite kütüphanelerinde yazılım ve donanım güvenliği konusunda politika, ortak kullanım alanlarında bulunan teknolojik varlıkların güvenliği, kullanıcı ve personele ait doğrulama araçları[16], yazılım ve donanım güvenliği konusunda prosedür ve politikalar, internet erişimi için kullanılan kullanıcı adı ve parolalar ile ilgili sorular yer almaktadır.

Tablo 22. Yazılım ve Donanım Güvenliği

Güvenlik Ölçümleri	Evet		Hayır		Geliştirme Aşamasında		Toplam	
	S	%	S	%	S	%	S	%
Kütüphanenizde yazılım ve donanım güvenliği konusunda politika var mı?	7	46,7	5	33,3	3	20	15	100
Kütüphanenizde ortak kullanım alanlarında bulunan teknoloji varlıklarının (masa üstü bilgisayar, taşınabilir bilgisayar, tablet, sunucular, projeksiyon, fotokopi, tarayıcı gibi) güvenliği tam olarak sağlanabiliyor mu?	13	86,7	2	13,3	-	-	15	100
Kullanıcı ve personele ait hassas verilerin doğruluğunun ve güvenilirliğinin sağlanması için doğrulama araçları kullanılıyor mu?	7	46,7	5	33,3	3	20	15	100
Sistem açma/kapama, yedekleme, teknolojik varlıkların bakımı ve bilgisayar odasının kullanılması gibi sistem faaliyetleri için bir prosedürünüz var mı?	8	53,3	4	26,7	3	20	15	100
Kütüphanenizdeki bilgisayarların yazılım ve donanım güvenliği sağlanıyor mu?	15	100	-	-	-	-	15	100
Kullanıcıların kütüphane içerisinden internet erişiminde kullanıcı adı ve şifre isteniyor mu?	11	73,3	4	26,7	-	-	15	100

Ankara'daki 15 üniversite kütüphane kurumunun katıldığı görüşmede yazılım ve donanım güvenliği ile ilgili ilk olarak, "Kütüphanenizde yazılım ve donanım güvenliği konusunda bir politika var mı?" sorusu sorulmuştur. Alınan yanıtlara göre, 15 kurum arasından 7 kurum (%46,7) kütüphanede yazılım ve donanım güvenliği konusunda politikalarının olduğunu belirtmiştir.

Kütüphanenin ortak kullanım alanlarında bulunan teknoloji varlıklarının (masa üstü bilgisayar, taşınabilir bilgisayar, tablet, sunucular, projeksiyon, fotokopi, tarayıcı gibi) güvenliğinin tam olarak sağlanıp sağlanmadığına ilişkin olarak sorulan bir soruya ise 13

[16] Doğrulama araçları, veri ve bilgilerin doğruluğunu, gizliliğini sağlamak amacıyla kullanılan araçlardır. Bu soruda ise, kimlik doğrulama(authentication) anlamında kullanılmıştır. Kimlik doğrulama ise, bir programın veya kullanıcının bir sisteme erişirken kim olduğunu belirleme işlemidir.

kurum (%86,7) ‘evet’ seçeneğini işaretleyerek, teknolojik varlıkların güvenliğinin tam olarak sağlandığını ifade etmiştir.

Yazılım ve donanım güvenliğinde yöneticilere sorulan diğer bir soru ise, “Kullanıcı ve personele ait hassas verilerin doğruluğunun ve güvenilirliğinin sağlanması için doğrulama araçları kullanılıyor mu?” şeklindedir. Kullanıcı ve personellere ait hassas verilerin doğruluğunun ve güvenilirliğinin sağlanması için doğrulama araçlarının kullanıldığını belirten kurumların sayısı ise 7’dir (%46,7).

Yazılım ve donanım güvenliği ile ilgili yöneticilere sorulan başka bir soru ise, kütüphanede sistem açma/kapama, yedekleme, teknolojik varlıkların onarımı, bakımı ve bilgisayar odasının kullanılması gibi sistem faaliyetleri için bir prosedürün olup olmadığı olmuştur. Alınan yanıtlara göre, 8 kurum (%53,3) ‘evet’ seçeneğini işaretleyerek prosedürlerinin olduğunu belirtmiştir.

Tablo 22’deki bulgulara göre, 15 kurum (%100), kütüphanedeki bilgisayarların yazılım ve donanım güvenliğinin sağlandığını belirtmiştir. Yine, 11 kurum (%73,3) kullanıcıların kütüphane içerisinden internet erişiminde kullanıcı adı ve şifre istendiğini ifade etmiştir. Yöneticilere Tablo 22’de yer alan sorulara ek olarak yazılım ve donanım güvenliği ile ilgili, kütüphanede bulunan bilgisayarlara yazılım yüklemeleri, kullanıcı faaliyetleri, temiz ekran ve temiz masa politikası[17], güvenlik duvarı kısıtlamaları, satın alınan ürünler için denetleme uygulamaları ve siber saldırılara yönelik önlemler olmak üzere toplamda altı soru yöneltilmiştir (Tablo 23).

[17]Temiz ekran ve temiz masa politikası, kurum ve kuruluşlarda fiziksel ve elektronik ortamda bilgi güvenliği risklerini azaltmak amacıyla hazırlanan politika belgesidir. Örneğin, Türkiye’de Sağlık Bakanlığı’nın bu konuda politika belgesi bulunmaktadır. : https://bilgiguvenligi.saglik.gov.tr/files/BGYS_Dokuman_Ornekleri/BG.PO...%20TEMİZ%20MASA%20TEMİZ%20EKRAN%20POLİTİKASI.pdf

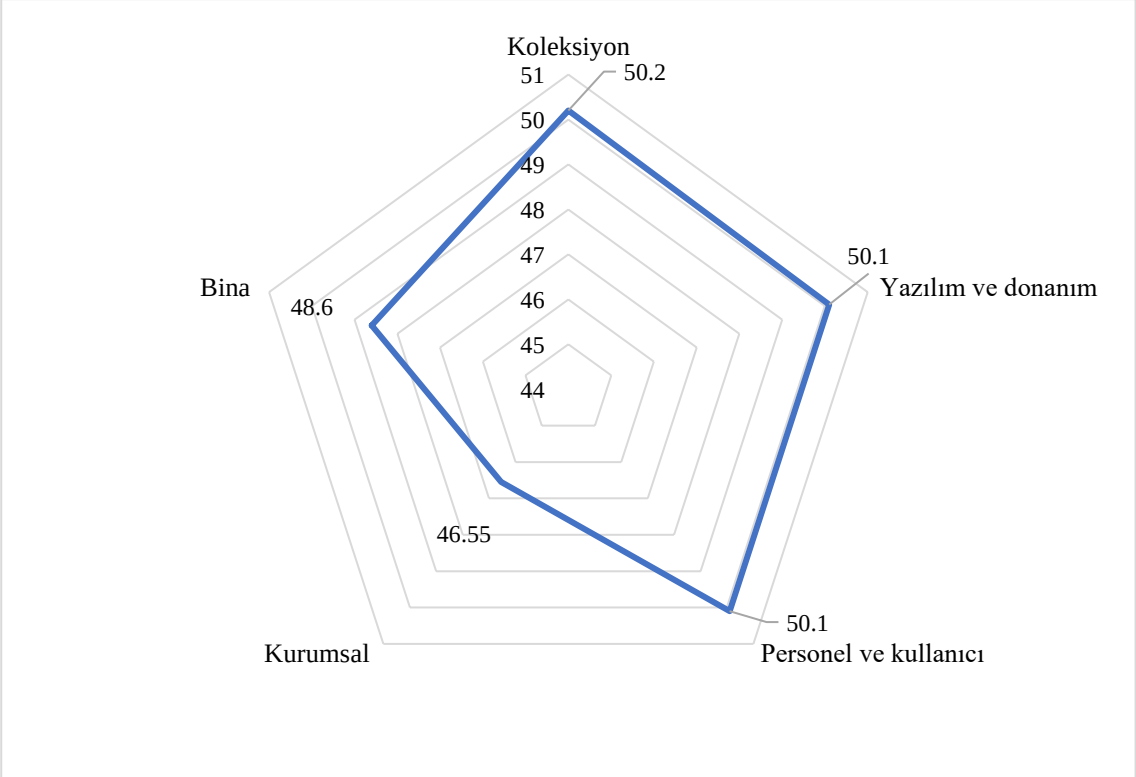
Tablo 23. Yazılım ve Donanım Güvenliği İle İlgili Diğer Bulgular

Güvenlik Ölçümleri	Evet		Hayır		Geliştirme Aşamasında		Toplam	
	S	%	S	%	S	%	S	%
Kullanıcıların ortak kullanım alanlarındaki bilgisayarlara yazılım yüklemelerine yönelik bir güvenlik uygulamanız var mı?	12	80	1	6,7	2	13,3	15	100
Ortak kullanım alanlarındaki bilgisayarlardaki kullanıcı faaliyetleri merkezi bir noktadan izleniyor mu?	8	53,3	7	46,7	-	-	15	100
Kütüphaneniz bilgi veya bilgi işlem araçları ile ilgili olarak temiz ekran ve temiz masa politikası uyguluyor mu?	6	40	7	46,7	2	13,3	15	100
Kullanıcıların ve personelin güvenliğini sağlamak amacıyla kötü amaçlar için kullanılan sitelere güvenlik duvarı kısıtlamaları getirildi mi?	15	100	-	-	-	-	15	100
Satın alınan ürünler (elektronik araç ve gereç, bilgi sistemi, vb.) için herhangi bir denetleme yapılıyor mu?	14	93,3	-	-	1	6,7	15	100
Kütüphanenizde siber saldırılara yönelik (anti-virüs, şifreleme, yedekleme) önlemler alındı mı?	14	93,3	-	-	1	6,7	15	100

Görüşme formunun 34. sorusunda yer alan yazılım ve donanım güvenliği ile ilgili bulgular incelendiğinde: kullanıcıların ortak kullanım alanlarındaki bilgisayarlara yazılım yüklemelerine yönelik bir güvenlik uygulamalarının olduğunu ifade eden 12 kurum (%80); ortak kullanım alanlarındaki bilgisayarlardaki kullanıcı faaliyetlerinin merkezi bir noktadan izlendiğini belirten 8 kurum (%53,3); kütüphanede bilgi veya bilgi işlem araçları ile ilgili olarak temiz ekran ve temiz masa politikasının olduğunu işaretleyen 7 kurum (%46,7); kullanıcıların ve personelin güvenliğini sağlamak amacıyla kötü amaçlar için kullanılan sitelere güvenlik duvarı kısıtlamaları getirildiğini belirten 15 kurum (%100); satın alınan ürünler (elektronik araç ve gereç, bilgi sistemi, vb.) için herhangi bir denetlemenin yapıldığı 14 kurum (%93,3); kütüphanede siber saldırılara yönelik (anti-virüs), şifreleme, yedekleme) önlemlerin alındığını belirten 14 kurum (%93,3) bulunmaktadır.

Daha önceki bölümlerde verilen üniversite kütüphanelerinde bilgi güvenliği uygulamalarına (Tablo 16-23) ek olarak, Ankara'daki üniversite kütüphanelerinin bilgi güvenliği uygulamalarına olan genel eğilimleri Şekil 8'de tespit edilmeye çalışılmıştır. Şekil 8'de verilen uygulamalara yönelik oranlar, üniversite kütüphanelerinde yöneticilerin kurumsal güvenlik, bina güvenliği, koleksiyon güvenliği, personel ve kullanıcı güvenliği ve yazılım ve donanım güvenliği [Tablo 16-Tablo 23] sorularına

verdikleri yanıtların ortalamaları alınarak oluşturulmuştur. Örneğin, Tablo 16'da yer alan kurumsal güvenlik uygulamalarının ortalamaları alınmıştır.



Şekil 8. Bilgi güvenliği uygulamalarında genel durum

Şekil 8'deki bulgulara göre, üniversite kütüphanelerinde koleksiyon güvenliğine (%50,2), diğer bilgi güvenliği unsurlarından daha fazla eğilim bulunmaktadır. Şekil 8'e göre katılımcıların en az (%46,55) eğilim gösterdiği bilgi güvenliği uygulaması ise, kurumsal güvenlik uygulamalarıdır.

Yöneticilerden, kütüphaneye ilişkin bilgi güvenliği uygulamalarını değerlendirmeleri istenmiştir. Söz konusu uygulamalara ilişkin değerlendirmeler Tablo 24 başlığı altında ele alınmıştır. Üniversite kütüphanelerinde mevcut uygulamaları değerlendiren yöneticilerin yanıt oranları incelendiğinde tüm uygulamalar (genel, bina, koleksiyon vb.) için çoğunlukla 'yeterli' düzeyde yanıt verdikleri dikkatleri çekmektedir.

Tablo 24. Mevcut uygulamalara yönelik değerlendirmeler

Mevcut uygulamalar	Çok yetersiz		Yetersiz		Kısmen		Yeterli		Çok yeterli		Toplam			
	S	%	S	%	S	%	S	%	S	%	S	%	x̄	σ
Genel kurumsal güvenlik	-	-	4	28,6	3	21,4	5	35,7	2	14,3	14	100	3,36	1,08
Bina güvenliği	1	7,1	3	21,4	3	21,4	5	35,7	2	14,3	14	100	3,29	1,20
Koleksiyon güvenliği	1	7,1	2	14,3	2	14,3	7	50	2	14,3	14	100	3,50	1,16
Personel ve kullanıcı güvenliği	-	-	2	14,3	4	28,6	5	35,7	3	21,4	14	100	3,64	1,00
Yazılım ve donanım	-	-	2	14,3	3	21,4	6	42,9	3	21,4	14	100	3,71	0,99
Kişisel verilerin k	-	-	3	21,4	2	14,3	7	50	2	14,3	14	100	3,57	1,01

Diğer taraftan, katılımcıların kütüphanedeki bilgi güvenliği uygulamalarının mevcut durumu, sırasıyla donanım ve yazılım güvenliği (x̄=3,71), personel ve kullanıcı güvenliği (x̄=3,64), kişisel verilerin güvenliği (x̄=3,57), koleksiyon güvenliği (x̄=3,50), genel kurumsal güvenlik (x̄=3,36) ve bina güvenliği uygulamalarıdır (x̄=3,29). Tablo 22'daki bulgulara bakıldığında, yöneticilerin tamamı (15 kurum - %100), kütüphanedeki bilgisayarların yazılım ve donanım güvenliğinin sağlandığını belirtmiştir. Bununla birlikte, Tablo 24'de yazılım ve donanım güvenliğine yönelik uygulamalar yeterli düzeyde (6 kurum - %42,9) tespit edilmiştir. Sonuç olarak, Tablo 22 ve Tablo 24'de yer alan yazılım ve donanım güvenliği ile ilgili uygulamalara yönelik bulgular birbiriyle örtüşmektedir.

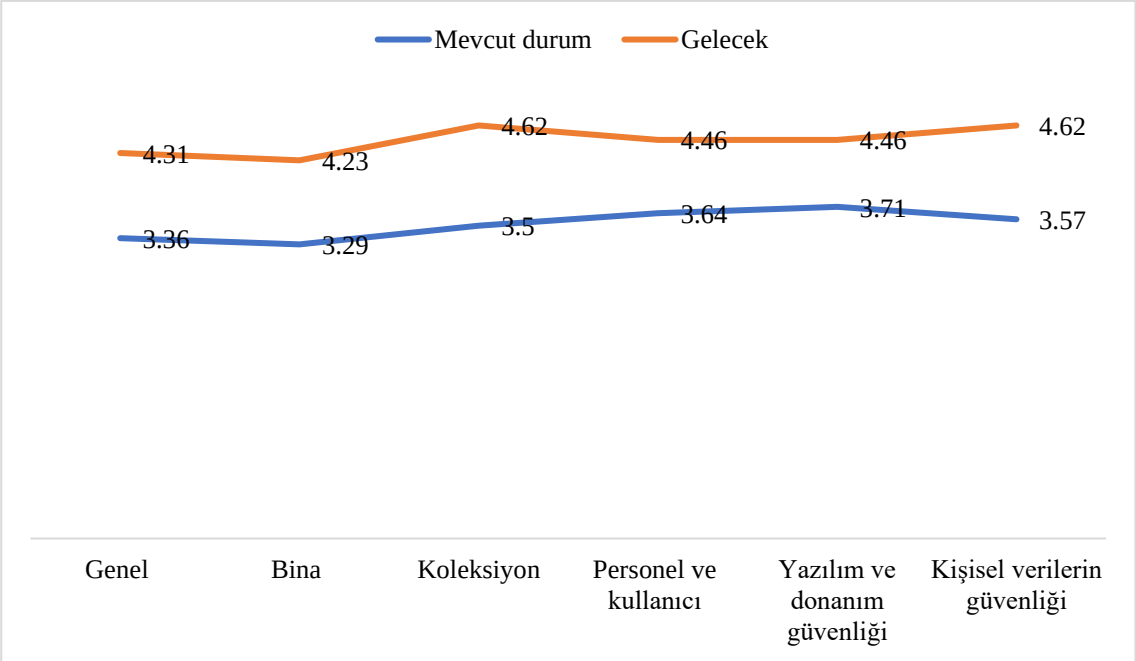
Yöneticilerin mevcut uygulamalarını değerlendirmelerine ek olarak, gelecek beş yıla yönelik güvenlik uygulamalarını değerlendirmeleri (Tablo 25) istenmiştir. İki soru arasından hareket edilerek katılımcıların beş yıl içerisinde yöneticilerin kütüphanelerinde gerçekleştirecekleri güvenlik uygulamalarına dair iyileştirmeleri ve geliştirmeleri ortaya çıkarılacaktır.

Tablo 25. Gelecek beş yıla yönelik değerlendirmeler

Mevcut uygulamalar	Çok yetersiz		Yetersiz		Kısmen		Yeterli		Çok yeterli		Toplam			
	S	%	S	%	S	%	S	%	S	%	S	%	x̄	σ
Kurumsal güvenlik	-	-	-	-	2	15,4	5	38,5	6	46,2	13	100	4,31	0,75
Bina güvenliği	-	-	-	-	2	15,4	6	46,2	5	38,5	13	100	4,23	0,72
Koleksiyon güvenliği	-	-	-	-	1	7,7	3	23,1	9	69,2	13	100	4,62	0,65
Personel ve kullanıcı güvenliği	-	-	-	-	1	7,7	5	38,5	7	53,8	13	100	4,46	0,66
Donanım ve yazılım	-	-	-	-	1	7,7	5	38,5	7	53,8	13	100	4,46	0,66
Kişisel verilerin güvenliği	-	-	-	-	-	-	5	38,5	8	61,5	13	100	4,62	0,50

Tablo 25'de yöneticilerden üniversite kütüphanelerinin gelecek beş yıla yönelik iyileştirmeleri ve geliştirmeleri ile ilgili hedeflerine yönelik değerlendirmeleri yer almaktadır. Tablo 25'e göre mevcut uygulamaların beş yıl içerisinde 'çok yeterli' düzeye geleceği görülmektedir. Bilgi güvenliği uygulamalarındaki yaklaşımın ise en çok, kişisel verilerin güvenliği($\bar{x}$=4,62) ve koleksiyon güvenliği($\bar{x}$=4,62) uygulamalarında olduğu anlaşılmaktadır (Tablo 25). Bir yönetici, kütüphane bünyesinde uygulanan bilgi güvenliği uygulamalarının 'kurumsal' uygulamalara bağlı kalınması dolayısıyla soruyu yanıtlamamıştır. Bu soruya yanıt vermeyen başka bir yönetici ise, gelecek beş yıl içerisinde emeklilik durumunun olacağı için soruyu boş bırakmıştır.

Yöneticilerin mevcut ve gelecekteki uygulamaları Tablo 24 ve Tablo 25'de ayrıntılı bir şekilde ele alınmıştır. Söz konusu iki tabloda yer alan, mevcut ve gelecek beş yıl içerisindeki ortalamalarına ilişkin karşılaştırmalar Şekil 9'da yer almaktadır.



Şekil 9. Yöneticilerin mevcut ve gelecekteki bilgi güvenliği uygulamalarına yönelik karşılaştırmaları

Şekil 9'a göre, gelecek beş yıl içerisinde yöneticilerin bilgi güvenliği uygulamalarını iyileştirecekleri ve geliştirecekleri anlaşılmaktadır. Yöneticilerin gelecek beş yıl içerisinde en çok iyileştirmeyi düşündüğü uygulamalar ise, koleksiyon ve kişisel verilerin güvenliği olmuştur.

4.2. ANKETLERDEN ELDE EDİLEN BULGULAR

Araştırmanın bu bölümünde üniversite kütüphanelerinde görev almakta olan kütüphanecilere uygulanan değerlendirme aracına dayalı bulgulara yer verilmektedir. Bu kapsamda, yapılan görüşme içeriğine göre yöneticilerin kişisel verilerin korunması ve bilgi güvenliği ile ilgili uygulamalara yönelik görüşlerini gösteren bulgular bu bölüm altında ele alınmaktadır.

4.2.1. Bilgi Güvenliği Farkındalığına Yönelik Bulgular

Tablo 26'da kütüphanecilerin kişisel verilerin korunması hakkında bilgi düzeyi gösterilmektedir. Toplam 94 kütüphaneci arasından 33 kütüphaneci (%35,1) kavram hakkında bilgi sahibi olduklarını belirtmiştir.

Tablo 26. Kişisel verilerin korunması hakkındaki bilgi düzeyiniz?

	S	%
Kavram hakkında bilgi sahibiyim	33	35,1
Kavram hakkında kısmen bilgi sahibiyim ve çalıştığım kurumda nasıl uygulanacağına yönelik bilgi sahibiyim	33	35,1
Kavram hakkında kısmen bilgi sahibiyim	25	26,6
Kavram hakkında bilgim yok	3	3,2
Toplam	94	100

Aynı zamanda, geriye kalan 61 kütüphaneci arasından 33 kütüphaneci ise (%35,1), kavram hakkında kısmen bilgi sahibi olduklarını ve çalıştıkları kurumda nasıl uygulanacağına yönelik bilgi sahibi olduklarını işaretlemişlerdir. 28 kütüphanecinin içerisinde yer alan 25 kütüphaneci (%26,6), kavram hakkında kısmen bilgi sahibi olduklarını ifade ederken, 3 kütüphaneci (%3,2) ise, kavram hakkında bilgilerinin olmadığını ifade etmişlerdir. 1 kütüphaneci ise kişisel verilerin korunması hakkındaki farkındalıkla ilgili olan bu soruya yanıt vermemiştir.

Tablo 27. Kütüphanenizde kişisel verilerin korunmasına yönelik gerçekleştirilen uygulamaları değerlendiriniz? (S=93)

	S	%
Çok yetersiz	9	9,7
Yetersiz	12	12,9
Orta seviye	29	31,2
Yeterli	36	38,7
Çok yeterli	7	7,5

($\bar{x}$=3,21, σ=1,08)

Kütüphanecilere sorulan başka bir soru ise kurumlarında gerçekleştirilen kişisel verilerin korunmasına yönelik uygulamaları değerlendirmeleri olmuştur. Tablo 27'ye bakıldığında kütüphanecilerin %38,7'si (36 kütüphaneci) uygulamaları yeterli seviyede bulurken %31,2'si (29 kütüphaneci) orta seviyede yeterli bulmuştur. 93 kütüphaneci arasında kişisel verilerin korunmasına yönelik uygulamaları yetersiz bulan kütüphanecilerin oranı ise (12 kütüphaneci) %12,9'dur. Soruya yanıt vermeyen 2 kütüphaneciden biri, kütüphane bünyesine yeni alınan personel olması dolayısıyla uygulamaları değerlendirmemiş, diğeri ise konu hakkında bilgisinin olmadığını belirtmiştir. Kütüphanecilerin kişisel verilerin korunmasına yönelik verdikleri gerçekleştirilen uygulamaların ortalaması ise 3,21'dir.

Kütüphanedeki iş süreçlerinin kişisel verilerden yararlanmayı ya da kütüphanede tutulan bu verileri içeren sistemlere erişmeyi gerektiğine yönelik sorulan bir soruda kütüphanecilerin %52,1'sı (49 kütüphaneci) zaman zaman erişim gerektirdiğini, %37,2'si

(35 kütüphaneci) erişim gerektirdiğini, %10,6'sı (10 kütüphaneci) erişim gerektirmediğini belirtmiştir. Bu soruya yanıt vermeyen kütüphanecilerin oranı ise, %1,1 oranla bir kütüphaneciye aittir. Üniversite kütüphanesi personellerine 'Kütüphaneye ait sistemlerdeki personele ya da kullanıcılara ait (Örneğin OPAC üzerinde bir bilgi kaynağını kimin ödünç aldığını görme, kütüphaneye kimlerin giriş-çıkış yaptığını görme gibi) erişim yetkiniz var mı?' diye bir soru yöneltilmiştir (bkz. Tablo 28).

Tablo 28. Kütüphaneye ait sistemlerdeki personele ya da kullanıcılara ait kişisel verilere erişim yetkiniz var mı?

Erişim yetkisi	**S**	**%**
Tüm sistemlere değil ancak yetkim dahilinde bulunan sistemlerdeki kişisel verilere erişebilirim	34	36,6
Evet, kütüphanemizde tüm sistemlerdeki – personel ve kullanıcı dahil-kişisel verilere erişebilirim	30	32,3
Hayır, çalıştığım pozisyon doğrultusunda herhangi bir kişisel veriye erişimim bulunmamaktadır	18	19,4
Evet, kütüphanemizde yalnızca kullanıcılarla ilgili tüm sistemlerdeki kişisel verilere erişebilirim	8	8,6
Evet, kütüphanemizde yalnızca personelle ilgili tüm sistemlerdeki kişisel verilere erişebilirim	2	2,2
Diğer	1	1,1
Toplam	**93**	**100**

Kütüphanecilerin 34'ü "Tüm sistemlere değil ancak yetkim dahilimde bulunan sistemlerdeki kişisel verilere erişebilirim" seçeneğini, 30'u ise, "Evet, kütüphanemizde tüm sistemlerdeki – personel ve kullanıcı dahil-kişisel verilere erişebilirim" seçeneğini işaretlemiştir. Tablo 28'de dikkat çeken nokta ise, kütüphanecilerin 2'sinin kütüphanede yalnızca personelle ilgili tüm sistemlerdeki kişisel verilere erişebilmesi olmuştur. Diğer taraftan kütüphanecilerin 18'i "çalıştığı pozisyon doğrultusunda herhangi bir kişisel veriye erişiminin olmadığını" belirtmiştir. İki kütüphaneci ise bu soruya yanıt vermemiştir.

Tablo 29'da kütüphanecilerin kütüphanedeki unsurlara yönelik güvenlik düzeylerinin değerlendirmeleri yer almaktadır. Bu kapsamda, kütüphanedeki kullanım alanları ve unsurları, kütüphane binası, kütüphane koleksiyonu, kullanıcı erişimine sunulan donanımlar, kullanıcı erişimine sunulan yazılımlar ve son olarak kişisel verilerin korunması güvenlik ölçütleri arasında yer almıştır.

Tablo 29. Kütüphanedeki unsurlara yönelik güvenlik düzeyleri

Güvenlik düzeyi	Yetersiz		Kısmen		Yeterli		Toplam	
	S	%	S	%	S	%	S	%
Kullanım alanları ve unsurlar	14	15,1	31	33,3	48	51,6	93	100
Bina	26	27,6	33	35,1	35	37,3	94	100
Koleksiyon	13	14	40	43	40	43	93	100
Donanımlar	17	18,4	32	34,8	43	46,5	92	100
Kişisel verilerin korunması	18	19,6	34	37,0	40	43,5	92	100

Tablo 29'daki bulgular incelendiğinde kütüphaneciler, yoğunlukla kullanım alanları ve unsurlarını bina güvenliğini, donanımları ve kişisel verilerin korunmasını yeterli düzeyde bulmuştur. Tablo 26'ya bakıldığında 3 kütüphaneci kişisel veri kavramı hakkında bilgi sahibi olmadığını belirtirken, 33 kütüphaneci kavram hakkında bilgi sahibi olduğunu belirtmiştir. Aynı zamanda Tablo 27 incelendiğinde, 36 kütüphaneci kişisel verilerin korunmasına yönelik gerçekleştirilen uygulamaları yeterli düzeyde bulmuştur. Tablo 26 ve Tablo 27'de yer alan bulgular Tablo 29'de yer alan bulgularla örtüşmektedir. Tablo 30'da üniversite kütüphanelerinde kişisel verilerin korunmasına ve bilgi güvenliği politikalarına yönelik politikaların yeterlilik düzeyine ilişkin veriler yer almaktadır.

Tablo 30. Kütüphanenizde kişisel verilerin korunması ve bilgi güvenliği politika belgelerine yönelik yeterlilik düzeyi

		Yetersiz	Kısmen	Yeterli	Toplam
Kişisel verilerin korunması (S=91)	S	9	22	27	58
	%	9,9	24,2	29,7	63,8
Bilgi güvenliği (S=92)	S	11	25	25	61
	%	12,0	27,2	27,2	66,4

Kütüphaneciler, kurumlarına yönelik olan kişisel verilerin korunması ve bilgi güvenliği politika belgelerini yeterli düzeyde bulmuşlardır. Kişisel verilerin korunmasına yönelik olan soruya toplam 91 katılımcının 33'ü (%36,2) ise, kişisel verilerin korunması ile ilgili politika belgelerinin olmadığını ifade etmiştir. 4 kütüphaneci ise bu soruya yanıt vermemiştir.

Tablo 30'da yer alan bilgi güvenliği sorusuna, katılımcılar kütüphanedeki uygulamaların en çok kısmen olduğunu belirtmiştir. Bilgi güvenliği ile ilgili politika belgesinin olmadığını belirten kütüphaneci sayısı ise 31'dir (%33,6). 95 kütüphaneci arasından 3 kütüphaneci ise bu soruya yanıt vermemiştir.

Görüşme formunda üniversite kütüphaneleri yöneticilerine sorulan güvenlik uygulamalarının gelecek beş yılın sonundaki yeterlilik durumuna ilişkin değerlendirmeleri kütüphanecilere de sorulmuştur. Söz konusu kütüphanecilere ilişkin değerlendirmeler Tablo 31'de yer almaktadır.

Tablo 31. Güvenlik uygulamalarının gelecek beş yılın sonundaki yeterlilik durumu

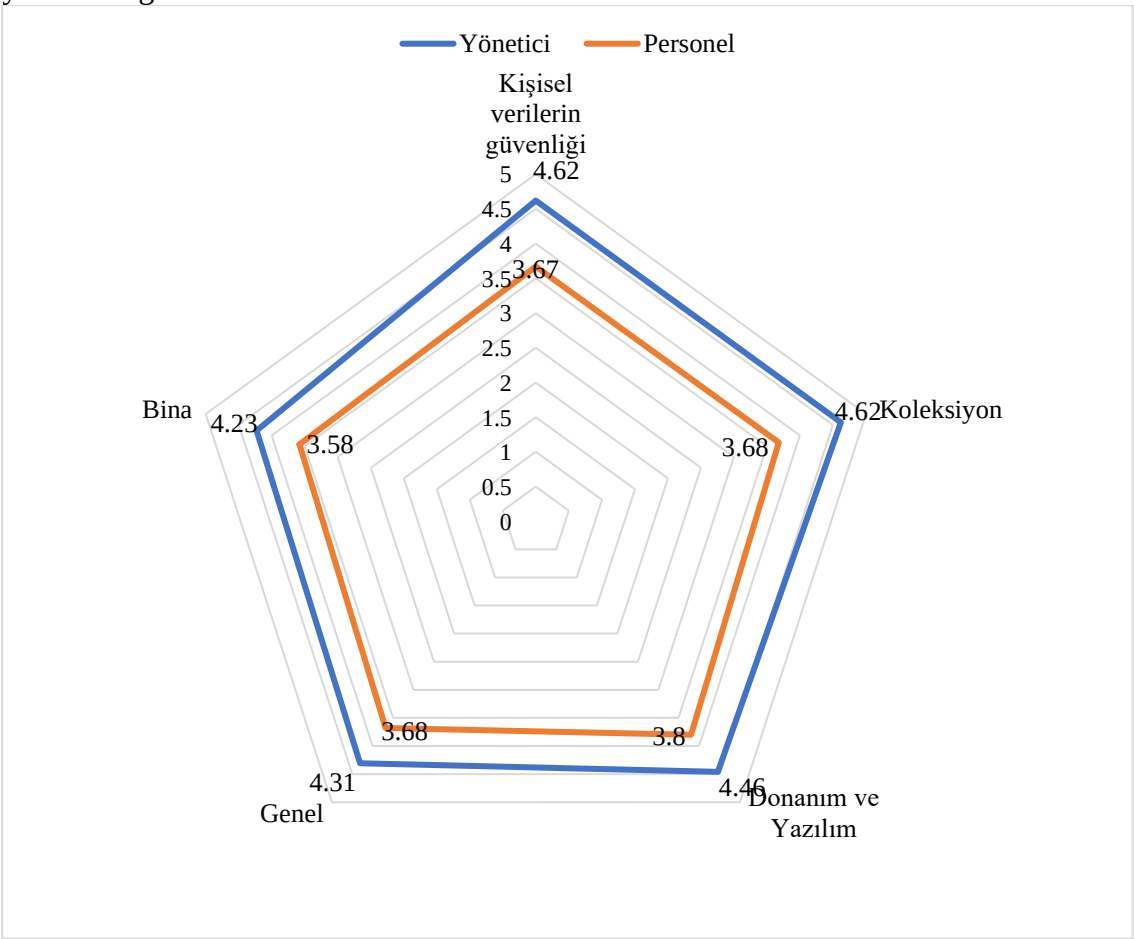
Gelecek beş yıla yönelik değerlendirme	**Çok yetersiz**		**Yetersiz**		**Kısmen**		**Yeterli**		**Çok yeterli**		**Toplam**			
	S	**%**	**S**	**%**	**S**	**%**	**S**	**%**	**S**	**%**	**S**	**%**	**x̄**	**σ**
Kurumsal güvenlik	2	2,2	5	5,5	29	31,9	39	42,9	16	17,6	91	100	3,68	0,9
Bina güvenliği	4	4,3	9	9,8	24	26,1	39	42,4	16	17,4	92	100	3,58	1,02
Koleksiyon güvenliği	3	3,3	8	8,7	19	20,7	47	51,1	15	16,3	92	100	3,68	0,95
Kullanıcı güvenliği	3	3,3	6	6,6	24	26,4	39	42,9	19	20,9	91	100	3,71	0,98
Donanım ve yazılım güvenliği	3	3,3	4	4,3	22	23,9	42	45,7	21	22,8	92	100	3,80	0,95
Kişisel verilerin güvenliğine yönelik uygulamalar	3	3,3	6	6,5	24	26,1	44	47,8	15	16,3	92	100	3,67	0,93
Kişisel verilerin korunmasına yönelik politikalar	4	4,4	10	11	19	20,9	39	42,9	19	20,9	91	100	3,64	1,06
Bilgi güvenliğine yönelik politikalar	4	4,3	8	8,7	23	25	39	42,4	18	19,6	92	100	3,64	1,03

Kütüphanecilerin gelecek beş yılda, bilgi güvenliği uygulamalarından özellikle donanım ve yazılım güvenliği(x̄=3,80), kullanıcı güvenliği(x=3,71), koleksiyon güvenliğine yönelik uygulamaların (x̄=3,68), kurumsal güvenliğe yönelik uygulamaların yeterli düzeyde olacağı belirlenmiştir. Kütüphanecilerin gelecek beş yılda en az yeterli düzeyde gördüğü bilgi güvenliği uygulaması ise (x̄=3,58) bina güvenliği uygulamasıdır. Burada bina güvenliğine ayrılan yeterlilik durumu bazı üniversite kütüphanelerinin üniversitenin kendisinden bağımsız bir binasının olmaması dolayısıyla üst yönetime bağlı olmasıyla ilişkilendirilebilir. Şekil 10'da görüşme formu ve değerlendirme aracında yönetici ve

personellere sorulan üniversite kütüphanelerinin gelecek beş yıla yönelik bilgi güvenliği uygulamalarının yeterlilik düzeylerinin değerlendirmeleri yer almaktadır.

Şekil 10'a göre, üniversite kütüphanelerinde karar verici konumunda olan yöneticiler, gelecek beş yılda bilgi güvenliği uygulamalarının kütüphanecilere kıyasla daha fazla 'yeterli' düzeyde olacağını belirtmişlerdir. Bununla birlikte, yöneticilerin gelecek beş yılda kişisel verilerin güvenliğine ve koleksiyon güvenliğine olan yaklaşımları daha fazla iken, kütüphanecilerin genel kurumsal güvenlik uygulamalarına ve kişisel verilerin güvenliğine olan yaklaşımları daha fazladır.

Şekil 10. Aritmetik ortalama değerlerine göre personel ve yöneticinin gelecek beş yıla yönelik öngörüleri



Diğer taraftan Şekil 10'da, yönetici ve kütüphaneciler bina güvenliğine yönelik uygulamaların gelecek beş yılda yeterlilik düzeyinin diğer unsurlara göre daha az artış göstereceğini belirtmişlerdir.

5.BÖLÜM

SONUÇ VE ÖNERİLER

Kurum ve kuruluşların mihenk taşı bünyesinde barındırdığı veri-bilgi-belge döngüsüdür. Bu döngü kurumsal fonksiyonlara dayanmakla birlikte, bilgi yönetimi, bilgi sistemleri, arşiv yönetimi, elektronik belge yönetimi, kişisel verilerin yönetimi olmak üzere çeşitli yönetim süreçlerinden meydana gelmektedir. Bunun yanı sıra, kurumlarda oluşturulan iş ve işlemlerin temelinde birey ve bireylerin ürettikleri bilgi varlıkları olarak isimlendirebileceğimiz ürün/ürünler yer almaktadır. Bu ürün/ürünler içerisinde ise, bireysel veriler ve kurumsal veriler yer almaktadır. Diğer taraftan, kurumlardaki bilgi ve belgelerin oluşturulması, düzenlenmesi, paylaşılması, aktarılması, transfer edilmesi, silinmesi, yok edilmesi ve anonim hale getirilmesi kurumsal altyapının tamamlanması açısından önem arz etmektedir. Çünkü, bireysel olarak da adlandırılagelen kişisel verilerin değiştirilmesi, yok edilmesi, ifşa edilmesi, yetkisizce erişilmesi ve farklı amaçlarla kullanılması kurumları her türlü risk, tehdit ve saldırıya maruz bırakacaktır. Bu bağlamda, etkin bir şekilde kurumsal bilgi yönetiminin ve bilgi güvenilirliğinin sağlanması bireysel güvenlik, mahremiyet ve kurumsal güvenliğin oluşturulmasına zemin hazırlayacaktır.

Kurumlarda oluşturulacak bilgi güvenliğinin ve bilgi güvenliği sistemlerinin kurumlardaki insan, bilgi, belge, mekân bağlamında ele alınması gerekmektedir. Bilgi güvenliğinin fiziksel güvenlikten, insan güvenliğine, insan güvenliğinden kurumsal güvenliğe kadar geniş bir yelpazede ele alınması konunun bütün olarak incelenmesine neden olmuştur. Aynı zamanda, bilgi güvenliğinin disiplinlerarası bir konumda olması farklı disiplinleri birbirine bağlamıştır. Bu çalışmada da birer kurum olarak nitelendirilen üniversite kütüphanelerinde bilgi güvenliği ve bilgi güvenliği uygulamaları farklı boyutlarla araştırılmaya çalışılmıştır. Birinci aşamada çalışmanın kuramsal bölümü tamamlanmış; bilgi güvenliği, bilgi güvenliğinin kapsamı, gelişim evreleri, bilgi güvenliğinin bileşenleri, bilgi güvenliği standartları ve bilgi güvenliğine yönelik kanunlar ve düzenlemeler, kişisel veri, kişisel verilerin yönetimi, kişisel verilere yönelik kanunlar ve düzenlemeler literatür çalışmalarına dayanılarak analiz edilmiştir. İkinci aşamada ise,

üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin yönetimi okuyuculara sunulmuştur.

Son olarak, araştırmanın birinci ve ikinci aşamalarından hareket edilerek Ankara'daki üniversite kütüphaneleri yöneticileri ve kütüphanecilerinin kurumsal bilgi güvenliği ve kişisel verilerin yönetimi ve korunması konusunda görüşme formu ve değerlendirme aracı geliştirilmiştir. Geliştirilen görüşme formu üniversite kütüphanelerinde kişisel verilerin neler olduğu, kişisel verilerin elde edilmesi, aktarılması, saklanması gibi kişisel verilerin yönetimiyle birlikte, bina güvenliği, koleksiyon güvenliği gibi bilgi güvenliği uygulamalarını içermektedir. Değerlendirme aracı ise, üniversite kütüphanelerinde kişisel verilerin yönetimi ve bilgi güvenliği uygulamalarına ilişkin kütüphanecilerin farkındalığını ve bilincini ölçmek amacıyla tasarlanmıştır. Bu bağlamda, geliştirilen araştırma araçlarının araştırmanın amaçlarına yönelik olarak geliştirildiği görülmektedir.

Üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin korunmasına yönelik yapılan çalışmada ulusal ve uluslararası kaynaklar araştırılmış, üniversite kütüphaneleri yöneticileriyle gerçekleştirilen yüz yüze görüşmeler sonucunda elde edilen bulgular ve kütüphanecilerle yapılan anket aracından elde edilen bulgular değerlendirilmiş ve aşağıdaki sonuçlara ulaşılmıştır.

Ankara'daki üniversite kütüphaneleri yöneticileri ile yapılan görüşmeler sonucunda, üniversite kütüphanelerinde uygulanan bilgi güvenliği uygulamalarının tam olarak sağlanamadığı ortaya çıkmıştır. Söz konusu durumun nedenleri arasında ise, bazı üniversite kütüphanelerinin onarım aşamasında olması, bazı üniversite kütüphanelerinin taşınma aşamasında olması ve bazı üniversitelerin merkezi bir noktadan yürütülmesi gibi sebepler gösterilmektedir. Bununla birlikte, bazı üniversite kütüphanelerinin merkezi yapıya sahip dağınık yerleşkelere sahip olması dolayısıyla araştırma kapsamına sadece merkez kütüphaneleri dâhil edilmiştir.

Değerlendirme aracına katılım gösteren gönüllü kütüphaneciler ile yapılan görüşmelerde ise, kütüphanecilerin bazıları konu hakkında bilgi sahibi olmadıklarını belirterek değerlendirme aracında bazı soruları yanıtlamamıştır. Bu durumun sebepleri ise bazı üniversitelerin kurulumunun henüz tamamlanmamış olması, üniversite kütüphanelerinde kütüphane kayıtları dışında daha özel kişisel verilerin kayıt altına alınmadığının ve bu

nedenle konuyla ilgili personele ihtiyaç olmadığının düşünülmesi ve kullanıcı üyelik işlemlerinin alt kütüphanelerce yapılması olarak gösterilmiştir.

Üniversite kütüphane yöneticileri ile yapılan görüşmelerde, yöneticiler kurumlarında kişisel verilerin en çok T.C. kimlik numarası, adı, soyadı, iletişim bilgileri ve adreslerin kullanıcılara yönelik tutulduğunu belirtirken personele yönelik tutulan veriler arasında ise bu verilerle birlikte sicil numarasının yer aldığını belirtilmiştir. Diğer taraftan, kullanıcılara ve personele ait tutulan kişisel veriler arasında kan grubu, adresi, nüfus bilgileri, kullanıcı adı, şifre, sınıfı, bölümü gibi verilerin kütüphanelerde tutulduğu tespit edilmiştir. Kulllanıcılara yönelik tutulan verilerin minumum düzeyde olması veri güvenliği açısından önem taşımaktadır. Bu bağlamda, gereksiz verilerin kütüphane bünyesinde tutulmaması gerekmektedir.

Kütüphane bünyesinde kullanıcılara yönelik kişisel verilerin arasında en çok Bölümü/Fakültesi/Enstitüsü, öğrenci numarası, kişisel/kurumsal e-posta hesabı ve ödünç işlemlerine yönelik veriler yer almaktadır. Personele yönelik veriler arasında ise kişisel/kurumsal e-posta hesabı, ödünç işlemlerine yönelik bilgiler ve personel kartları bulunmaktadır.

Araştırmada elde edilen bulgulara göre, üniversite kütüphanelerinde kişisel veriler farklı yollarla toplanmaktadır. Yöneticilerin birden fazla seçeneği işaretleyebildiği bu soruya göre, kişisel veriler üniversite kütüphanelerinde ÖİDB'den ilgili kütüphane sistemine aktarılarak, PDB aracılığıyla ve BİDB'dan ilgili kütüphane sistemine aktarılarak elde edilmektedir.

Kişisel verilerin üniversite kütüphanelerinde ilk olarak, kullanıcının kütüphanede üyelik formlarını doldurduğu anda kayıt altına alındığı belirlenmiştir. Aynı zamanda, üniversite kütüphanelerinde kişisel veriler, her dönem başında üniversitenin ilgili sistemlerinden otomatik olarak ve kullanıcı bilgisi üniversitenin ilgili sistemine kaydedildiği anda kütüphane sistemine aktarılarak kayıt altına alındığı araştırma bulgularından elde edilmiştir.

Kişisel Verilerin Korunması Kanunu kapsamında 8 kurumda veri sorumlusunun bulunmadığı belirlenmiştir. Veri sorumlusunun amacı, kişisel verilerin işlenme

amaçlarını ve vasıtalarını belirlemektir. Bu bağlamda, üniversite kütüphanelerinin bazılarında kişisel verilerin işlenme amaçlarının belirlenmediği ön plana çıkmaktadır.

Kişisel verilerin sınıflandırılması, kategorize edilmesi ve düzenlenmesi kişisel verilerin bütünlüğü ve erişilebilirliği açısından önem taşımaktadır. Üniversite kütüphanelerinde yöneticilerin çoğunluğu kişisel verileri kullanıcı grubuna göre, gizlilik derecelerine göre, işlem öncelik sıralarına göre, güvenlik hassasiyet düzeylerine, tür ve özelliklerine, belge isimleri ve standart dosya planına göre sınıflandırma yaptıklarını işaretlemiştir.

Üniversite kütüphanelerinde kişisel verilerin yoğun olarak işlendiği yerler kullanıcı-personel etkileşiminin olduğu alanlardır. Araştırma bulgularına göre, ödünç verme, elektronik kaynaklar, sağlama ve kataloglama birimi üniversite kütüphanelerinde kişisel verilerin en çok işlendiği birimlerdir. Bununla birlikte, kütüphanenin farklı birimlerinde de kişisel verilerin işlendiği (kurumsal iletişim birimi, açık erişim ve kurumsal arşiv birimi, satın alma ve muhasebe birimi) görülmüştür. Buradan hareketle, üniversite kütüphanelerinde kişisel verilerin farklı birimlerde işlendiği ortaya çıkmaktadır. Daha önceki bulgularda, üniversite kütüphanelerinin bazısında veri sorumlusunun olmadığı tespit edilmişti. Ancak, bu soruda ise kişisel verilerin kütüphanenin farklı birimlerinde işlendiği ortaya çıkmıştır. Bu birimlerde kişisel verilerin işlenmesi ile ilgili görev tanımlarının personellere yapılıp yapılmadığı konusunda belirsizlikler bulunmaktadır. Aynı zamanda, üniversite kütüphanelerinin farklı birimlerinde kişisel verilerin işlenmesine ihtiyaç olup olmadığı tartışılmalıdır.

Üniversite kütüphanelerinde kişisel verilerin kullanım amacının belirlenmesi, kullanıcılara yönelik kişisel verilerinin ne amaçla işlendiğine dair kullanıcılara bilgi verilmesi noktasına önem arz etmektedir. Hizmet sunumu ve raporlama/kullanım istatistiği alma kütüphanelerde kişisel verilerin en çok kullanılma amaçları arasında bulunmaktadır. Bu bulguların yanı sıra, yöneticiler kişisel verileri kütüphane güvenliğini sağlama, hizmet geliştirme ve koleksiyon güvenliğini sağlamak olmak üzere farklı amaçlarla kullanmaktadır.

Kişisel verilerin tutulduğu ortamların güvenilir olması kişisel verilerin mahremiyetinin ve güvenilirliğinin oluşturulmasına olanak tanıyacaktır. Araştırma verilerine göre, kişisel

veriler en çok kütüphanenin kendi sunucularında ve üniversitenin merkezi sunucularında tutulmaktadır.

Üniversite kütüphane yöneticileri kullanıcılara yönelik kişisel verilerin birden fazla gerekçe ile kullanılmasına ve paylaşılmasına izin verildiğini belirtmiştir. Söz konusu gerekçeler arasında ise, üniversite üst yönetimi ya da güvenlikten sorumlu birimler tarafından istenmesi halinde, yasal çerçevede savcılık tarafından istenmesi halinde ve Bilgi Edinme Hakkı Kanunu çerçevesinde kişisel verilerin paylaşılması yer almaktadır. Burada, üniversite kütüphanelerinde kişisel verilerin hangi şartlar altında kullanılacağı ve paylaşılacağına yönelik belirsizliklerin olduğu görülmektedir. Çünkü, yöneticilerin bu soruya yönelik dağılımları seçeneklere göre farklılıklar göstermektedir (Tablo 9).

Yetkili kişilerin ya da bilgi işlem uzmanlarının çalışmalarıyla ve sistemler arası etkileşim olması dolayısıyla PDB, BİDB ve ÖİDB birimlerinden kişisel verilerin üniversitenin diğer birimlerinden otomatik olarak aktarıldığı belirlenmiştir. Üniversite kütüphanelerinde kişisel verilerin en çok aktarıldığı birimler ise sırasıyla ÖİDB, PDB ve BİDB'dir. Kısaca, üniversite kütüphanelerinde kişisel verilerin üniversitenin farklı başkanlıklarına aktarıldığı ortaya çıkmıştır.

Kütüphane otomasyon sistemi, kütüphanenin abone olduğu veri tabanı sistemleri, kütüphane kurumsal arşiv sistemi ve kapı turnike sistemleri üçüncü parti kuruluşların kişisel verilere erişim sağlayabildikleri sistemler arasında yer almaktadır.

Üniversite kütüphanelerinin sekizinde kullanıcıların kişisel verilerinin işlenmesine ve korunmasına yönelik rızaları alınmamaktadır. Diğer taraftan, kullanıcı rızasını aldıklarını belirten yedi kurum kişisel verilerin korunmasına yönelik aydınlatma metinlerinde en çok kişisel verilerin tutulma amacını içerdiğini belirtmiştir. Söz konusu aydınlatma metinlerinde, kişisel verilerin saklanma sürelerine, silinmesine ve yeniden kullanımına yönelik bilgilerin az sayıda olması ise dikkat çekicidir. Buradan hareketle, "Ankara'daki üniversite kütüphanelerinde kişisel verilerin korunması ile ilgili aydınlatma metinlerinde eksiklikler bulunmaktadır" şeklinde olan hipotezimiz doğrulanmıştır.

Kişisel verilerin kütüphanelerde izinsiz bir şekilde paylaşılması, aktarılması ve yetkisizce kullanımının önüne geçebilmek amacıyla gizlilik sözleşmeleri imzalamaları

gerekmektedir. Ankara'da bulunan üniversite kütüphanelerinin 5'inde gizlilik sözleşmelerinin olmadığı belirlenmiştir. 4 kütüphanede ise kısmen gizlilik sözleşmesi imzaladıklarını belirtmiştir.

Üniversite kütüphanelerinde kişisel verilerin korunmasına yönelik önemli bir diğer konu ise, kişisel verilerin kullanma sürelerinin belirlenmesi ve verilerin silinmesine yönelik adımların atılmasıdır. Üniversite kütüphaneleri yöneticileri, otomasyon sistemlerinden kişisel verileri silme/yok etme/anonimleştirme yöntemlerini kullanarak kaldırdığını belirtmiştir.

Araştırmada üniversite kütüphanelerinde kişisel verilerin saklanmasına yönelik uygulamalarında eksiklikler tespit etmiştir. 8 kurumda verilerin saklanmasına yönelik bir uygulama bulunmamaktadır. Üniversite kütüphanelerinde kişisel verilerin saklanmasına yönelik olarak 'kişisel verilern saklanmasına gerek var mıdır?', 'kişisel verilerin kullanım süreleri nelerdir?', 'kişisel veriler hangi koşullarda muhafaza edilmelidir?' vb. sorulara yanıt verilmesi gerekmektedir.

Çoğu kurumda kişisel verilerin yönetilmesini içeren bir politikanın bulunmadığı tespit edilmiştir. Kurumların bazısının ise, söz konusu politikaya ihtiyaç duydukları ön plana çıkmıştır.

Araştırmada yöneticiler kütüphanede herhangi bir sorunla karşılaştıklarında en çok hukuk müşavirliği ve Kişisel Verileri Koruma Kurumu'na başvuracağını belirtmiştir. Bununla birlikte, politikalar, etik ilkeler, üniversitenin etik kurul komisyonları başvurulan kaynaklar arasında yer almaktadır.

Üniversite kütüphaneleri yöneticileri ile kurumsal uygulamaları üzerine yapılan görüşmelerde göze çarpan noktalar ise şu şekildedir: üniversite kütüphanelerinin çoğunluğunda bilgi güvenliği politika belgesinin bulunmadığı; ISO standartlarına uygun olarak bilgi güvenliği yönetim sistemi ve/veya kalite yönetim sisteminin olmadığı; bilgi güvenliği politikalarında kişisel verilerin korunması ve bilgi güvenliğinin birlikte alınmadığı; kütüphanelerde bilgi güvenliği risk analizlerinin yapılmadığı belirlenmiştir. Üniversite kütüphanelerinin kurumsal uygulamalarına dayalı bu veriler ise, "Ankara'daki

üniversite kütüphanelerinin temel bileşenlerine yönelik bilgi güvenliği uygulamaları yetersizdir" şeklinde olan hipotezimizi doğrulamıştır.

Üniversite kütüphanelerinde bina güvenliğine yönelik bulgulara bakıldığında ise: 6 kurumda bina güvenliğine yönelik politika bulunmamakta; kütüphanelerinin çoğunluğunun binasının kütüphane binası olarak tasarlanmadığı ve kütüphanelerin çoğunluğunda nem ve gürültü ölçümlerinin yapılmadığı belirlenmiştir.

Üniversite kütüphanelerinde bilgi güvenliği unsurlarından birisi olan personel ve kullanıcı güvenliğine yönelik önlem ve tedbirlerin alınması önem taşımaktadır. Yöneticilerin kurumlarında personel ve kullanıcı güvenliği bilinç ve farkındalığını oluşturması, konu ile ilgili politikaların oluşturulması gerekmektedir. Araştırma bulgularında şaşırtıcı bir bulgu ise, kütüphanelerin çoğunluğunda personel ve kullanıcı güvenliğine yönelik yazılı bir politika bulunmamaktadır.

Üniversite kütüphaneleri yöneticilerinin bilgi güvenliği uygulamalarına yönelik eğilimleri ise en çoktan aza doğru: koleksiyon güvenliği, personel ve kullanıcı güvenliği, yazılım ve donanım güvenliği, bina güvenliği ve kurumsal güvenlik uygulamaları şeklindedir.

Yöneticilerin mevcut bilgi güvenliği uygulamalarına yönelik olarak en çok donanım ve yazılım güvenliği yer alırken en az yeterli düzeyde yer alan uygulama bina güvenliği olmuştur. Yöneticilerin gelecek beş yıla yönelik değerlendirmelerinde en üst seviyede koleksiyon ve kişisel verilerin güvenliği yer alırken en alt seviyede bina güvenliği yer almaktadır.

Kütüphanecilerin kişisel veri kavramına yönelik farkındalıklarına ilişkin bulgulara göre, kütüphanecilerin çoğu kavram hakkında bilgi sahibidir. Bununla birlikte, kütüphanecilerin çoğu kütüphanelerinde gerçekleştirilen kişisel verilerin korunmasına yönelik uygulamaları yeterli düzeyde bulmuştur.

Kütüphanecilerin çoğunun kütüphanedeki tüm sistemlere değil ancak yetkisi dahilinde bulunan sistemlerdeki kişisel verilere erişim sağlayabildikleri belirlenmiştir. Diğer

taraftan, 18 kütüphaneci görevi doğrultusunda herhangi bir kişisel veriye erişiminin bulunmadığını belirtmiştir.

Kütüphanedeki unsurlara (kullanım alanları, bina, koleksiyon vb.) yönelik güvenlik eğilimlerini ise yeterli düzeyde bulmuşlardır. 33 kütüphaneci kişisel verilerin korunmasına yönelik politikanın olmadığını belirtirken, 31 kütüphaneci bilgi güvenliğine yönelik politika belgelerinin olmadığını belirtmiştir. Bu doğrultuda araştırmamızın "Üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin yönetimine dönük karar verme ve uygulama düzeyindeki eksiklikler (politika, konuyla ilgili bilinç ve farkındalık, risk değerlendirmesi gibi konularda) bulunmaktadır" şeklinde olan hipotezi doğrulanmıştır.

Kütüphanecilerin gelecek beş yıla yönelik öngörülerine göre ise, ilk üç sırada donanım ve yazılım, kurumsal ve koleksiyon güvenliği bulunurken son üç sırada kişisel verilerin korunmasına yönelik politikalar, bilgi güvenliği, kişisel verilerin korunmasına yönelik uygulamalar ve bina güvenliğine yönelik uygulamalar bulunmaktadır.

Üniversite kütüphanelerinde karar verici konumunda yöneticiler, kurumlarındaki bilgi güvenliği uygulamalarını personele göre daha fazla yeterli düzeyde bulmuştur.

Üniversite kütüphanelerinde bilgi güvenliği mevcut bilgi güvenliği düzenlemelerine ve uygulamalarına yönelik koşulları ve sorunları ortaya koyan bulgulara dayanarak aşağıdaki önerilere ulaşılmıştır.

1. Türkiye'de 2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu'na uygun olarak, tüm üniversite kütüphaneleri de kurum olarak kişisel verilerin yönetilmesini içeren yapılandırılmış düzenleme ve politikalarını oluşturmalıdır.
2. Üniversite kütüphaneleri kişisel verilerin elde edilmesi, toplanması, işlenmesi, aktarılması, paylaşılması ve saklanmasını içeren kurallar, standartlar ve sözleşmeler hazırlamalıdır.
3. Üniversite kütüphaneleri kişisel hakların korunması amacıyla veri gizliliğinin ve güvenliğini ayrıntılı bir şekilde ele alan aydınlatma metni ve onay formu oluşturulmalıdır.
4. Kişisel verilerin korunması ve yönetilmesine yönelik yönetici ve personellere eğitim ve farkındalık çalışmaları yapılmalıdır.

5. Kullanıcı mahremiyetinin ve bilgi güvenliğinin sağlanması noktasında, kullanıcılara yönelik etkinlikler düzenlenmelidir.
6. Üniversite kütüphanelerinde bilgi güvenliğini sağlamak amacıyla hukuki, teknik ve idari tedbirler alınmalıdır.
7. Üniversite kütüphaneleri yöneticileri kişisel verilerin yönetilmesi ve korunması hususunda Kişisel Verileri Korunması Kurumu ile koordinasyon ve uyum çalışmaları gerçekleştirilmelidir.
8. Üniversite kütüphaneleri bilgi güvenliği uygulamalarına yönelik SWOT Analizi, Bilgi Güvenliği Risk Analizi ve Denetim Çalışmaları gerçekleştirmelidir.
9. Üniversite kütüphanelerinde bilgi güvenliğinin sağlanması amacıyla Bilgi Güvenliği Yönetim Sistemi Standartları oluşturulmalıdır.
10. Üniversite kütüphanelerinde bilgi güvenliği uygulamalarının ayrı ve ayrıntılı olarak (bina güvenliği politikası, kullanıcı güvenliği politikası vb.) yapılandırıldığı yazılı politikalar hazırlanmalıdır.

Bu araştırmada bilgi güvenliği ve kişisel verilerin korunması yönetici ve kütüphaneci bağlamında ele alınmıştır. Konu ile ilgili olarak eksikliklerin giderilmesi, yönetici ve kütüphanecilerde bilinç ve farkındalıkların oluşturulması amacıyla Bilgi Bilimi ve Kütüphanecilik alanında daha fazla çalışma yapılmalıdır. Bununla beraber, yapılacak olan çalışmalara, akademisyen, öğrenci, personel vb. olmak üzere kullanıcı boyutunda da bakılması gerekmektedir.

KAYNAKÇA

108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (2016, 17 Mart). *T.C. Resmî Gazete.* (Sayı: 29656). http://www.resmigazete.gov.tr/default.aspx# adresinden erişildi.

6698 Numaralı Kişisel Verilerin Korunması Kanunu (2016, 7 Nisan). *Resmî Gazete* (Sayı: 29677). 8 Ekim 2018 tarihinde http://. mevzuat.gov.tr/MevzuatMetin/ 1.5.6698.pdf adresinden erişildi.

Abioye, A. A., ve Rasaki, O. E. (2013). Survey of Security Challenges in University Libraries in Southwest Nigeria. *Library & Archival Security, 26*(1-2), 1-13. Doi: https://doi.org/10.1080/01960075.2013.869078

ACRL. (2018). *Standards for libraries in higher education.* Chicago, Illinos.

Afyonluoğlu, M. (16-18 Kasım 2018). Üniversitelerde Kişisel Veriler. (Üniversiteler Teknoloji Zirvesi 2018 Huawei&InfoTürk). Antalya, Türkiye. 7 Mayıs 2019 tarihinde http://afyonluoglu.org/PublicWebFiles/presentations/20181116%C3%9Cniversiteler%20Tekn%20Zirvesi-MustafA-V2-PRINTABLE. Pdf adresinden erişildi.

Afyonluoğlu, M. (28 Ocak, 2019). E-devlette kişisel verilerin korunması. KVKK 28 Ocak Veri Koruma Günü Konferansı. Ankara, Türkiye. 7 Mayıs 2019 tarihinde http://afyonluoglu.org/PublicWebFiles/presentations/20190128-KVKK-MustafaA-V1-PRINTABLE.pdf adresinden erişildi.

Ağıralan, E. (2015). *Bilgi güvenliği, kişisel verilerin korunması ve mahremiyet etki Değerlendirmesi.* (Yüksek lisans tezi). Polis Akademisi, Ankara.

Ajegbomogun, F. O. (2004). Users' assessment of library security: A Nigerian University case study. *Library Management, 25*(8/9), 386-390. Doi: https://doi.org/10.1108/01435120410562880

Akalın, M. (2018). *Örnek açıklamalarıyla sosyal bilimlerde araştırma tekniği anket.* Ankara: Seçkin yayıncılık.

Akdağ, H. (2013). *Türk Ceza Kanunu kapsamında kişisel verilerin korunması* (Birinci baskı). Ankara.

Akıncı, A. N.. (2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün getirdiği yenilikler ve Türk hukuku bakımından değerlendirilmesi: Çalışma raporu-6*. Kalkınma Bakanlığı, Ankara.

Akıncı, A. N. (2019). *Büyük veri uygulamalarında kişisel veri mahremiyeti*. (Uzmanlık tezi). T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Sektörler ve Kamu Yatırımları Genel Müdürlüğü.

Akor, P. U. (2013). Security management for prevention of book thefts in university libraries: A case study of benue state university library, Nigeria. *Library Phisophy and Practice*, 995. 17 Nisan 2019 tarihinde https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=2403&context=libphilprac adresinden erişildi.

Aksoy, N. (2012). *Kişisel verilerin korunması ve işlenmesi* (Yüksek Lisans Tezi). Marmara Üniversitesi, İstanbul.

ALA. (2016, Temmuz 28). Library Privacy Guidelines for Library Management Systems [Text]. http://www.ala.org/advocacy/privacy/guidelines/library-management-systems adresinden erişildi.

ALA. (2014). Privacy and Confidentiality: Library CoreValues [Text]. http://www.ala.org/advocacy/privacy/toolkit/corevalues adresinden erişildi.

ALA. (2007, Mayıs 29). Privacy and confidentiality.http://www.ala.org/advıcacy/int freedom/privacyconfidentialityqa adresinden erişildi.

ALA. (2004). Policy concerning confidentiality of personally ıdentifiable ınformation about library users [Text]. http://www.ala.org/advocacy/ intfreedom/statementspols/otherpolicies/policyconcerning adresinden erişildi.

Anday, A., Francese, E., Huurdeman, H. C., Yılmaz, M., ve Zengenene, D. (2012). Dijital kütüphane ortamında bilgi güvenliği sorunları: literatür değerlendirmesi. *Bilgi Dünyası, 13*(1), 117-137.

Anayasal bir hak olarak kişisel verilerin korunması hakkı. (t.y.). KVKK. Ankara. https://kvkk.gov.tr/yayinlar/ANAYASAL%20B%C4%B0R%20HAK%20OLARAK%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%

C4%B0N%20KORUNMASINI%20%C4%B0STEME%20HAKKI.pdfadresinden erişildi.

Arıtürk, M. (2015). *Bilgi farkındalığı ve bilgi güvenliğinin karşılaştırılması*. Program adı: XVII. Akademik Bilişim Konferansı, Eskişehir. https://ab.org.tr/ab15/bildiri/74.docx

Arnason, S. T., ve Willett, K. D. (2007). *How to Achieve 27001 Certification: An Example of Applied Compliance Management*. Doi: https://doi.org/10.1201/9781420013139

Avcı, Y. (2019). *Kişisel verilerin korunması*. (Yüksek Lisans Tezi). Selçuk Üniversitesi, Konya.

Avrupa Komisyonu. (2018). AB genişleme politikasına ilişkin 2018 bilgilendirmesi. 27 Ekim 2018 tarihinde https://www.ab.gov.tr/siteimages/pub/komisyon_ulke_Raporlari/2018_turkiye_raporu_tr.pdf adresinden erişildi.

Avrupa Konseyi. (2016). Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 12 Ekim 2018 tarihinde https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 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. 12 Ekim tarihinde https://eurlex.europa.eu./LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF adresinden erişildi.

Avrupa Konseyi. (1981). Kişisel verilerin otomatik işleme tabi tutulması karşısında Bireylerin korunması sözleşmesi. http://www.resmigazete.gov.tr/eskiler/2016/03/20160317-2.pdf adresinden erişildi.

Avrupa Konseyi (1950). Avrupa İnsan Hakları Sözleşmesi. 7 Mayıs 2019 tarihinde

http://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf adresinden erişildi.

Aydın, S. E. (2014). *AİHM içtihatları bağlamında kişisel verilerin kaydedilmesi suçu* (Yüksek Lisans Tezi). İstanbul Üniversitesi, İstanbul.

Aydoğmuş, E. (2010). *Assessment of information security maturity levels and ISO/IEC 27001:2005 compliance of organizations in Turkey* (Master Thesis). İstanbul Teknik Üniversitesi, İstanbul.

Baker, W., ve Wallace, L. (2007). Is Information Security Under Control?:Investigating Quality in Information Security Management. *IEEE Security and Privacy Magazine*, *5*(1), 36-44. Doi: https://doi.org/10.1109/MSP.2007.11

Balcı, A. (2013). *Sosyal Bilimlerde Araştırma: Yöntem, Teknikler ve İlkeler.* Ankara, Pegem Akademi.

Baş, T. (2003). *Anket: anket nasıl hazırlanır, anket nasıl uygulanır, anket nasıl değerlendirilir.* (4. Baskı). Ankara: Seçkin.

Baş, T. (2001). *Anket: anket nasıl hazırlanır, anket nasıl uygulanır, anket nasıl değerlendirilir.* (4. Baskı). Ankara: Seçkin.

Başak, C. D. (2018). Güvenlik ağ'da başlar! *CyberMag.* 13 Aralık 2018 tarihinde *https://www.cybermagonline.com/guvenlik-agda-baslar* adresinden erişildi.

Başalp, N. (2003). *Kişilik hakkının korunması sorunu çerçevesinde kişisel verilerin korunması ve saklanması* (Yüksek Lisans Tezi). İstanbul Üniversitesi, İstanbul.

Başdinkçi, N. (2017). *Sağlık kurumlarında bilgi güvenliği risk değerlendirmesi ve kullanıcıların bilgi güvenliği farkındalık düzeyinin ölçülmesi.* (Yüksek Lisans Tezi). Çukurova Üniversitesi, Adana.

Bilgi ve İletişim Güvenliği Tedbirleri. (2019, 6 Temmuz). *Resmî Gazete*. (30823). http://www.resmigazete.gov.tr/eskiler/2019/07/20190706-10.pdfadresinden erişildi.

Bina İşletimi | Cem ÖZEL (2018, 05 Eylül) Bilgi ve Belge Yönetimi (BBY) Haber

Portalı. (t.y.). https://www.bbyhaber.com/bby/2018/10/05/bina-isletimi adresinden erişildi.

Borazan, M. (2015, Aralık). *Gizlilik, bireysel haklar ve kişisel verilerin korunması*. Program adı: XX.Türkiye'de İnternet Konferansı, İstanbul. http://inet-tr.org.tr/inetconf20/kitap/inet15-MBorazan.pdf

Boyd, J. K. (2002). *A comparison of cronbach's coefficient alpha and latent variable model estimates of composite reliability for congeneric measures* (Order No. 3045120). Available from ProQuest Dissertations&Theses Global. (305521953). Erişim adresi: https://search.proquest.com/docview/305521953?accountid=11248

Botez, A. M., ve Repanovici, A. (2017). The importance of security for people and collections in libraries. *Romanian Journal of Library and Information Science*, *13*(1), 11-20.Doi: https://doi.org/10.26660/rrbsi.2017.13.1.11

Bowers, S.L. (2006). Privacy and library records. *The journal of academic librarianship, 32*(4), s.377-383. Doi:https://doi.org/10.1016/j.acalib.2006.03.005

Boz, A. (2014). *Kişisel verilerin korunması: Türkiye, ABD ve AB örnekleri.* (Yüksek Lisans Tezi). Polis akademisi, güvenlik stratejileri ve yönetimi anabilim dalı, Ankara.

Brown, S. (2001). Privacy in and information technology or what a give away!. *Libraries and librarians: Making a difference in the knowledge age.* IFLA council and general conference: conference programme and proceedings (67th, Boston, MA, August 16-25, 2001) (p. 66-72) in. 8 Kasım 2018 tarihinde https://files.eric.ed.gov/fulltext/ED459705.pdfadresinden erişildi.

BS 7799-3:2017. (2017). Information security management systems. Guidelines for information security risk management. British Standards Institute.

BSI-Standard 100-2 IT-Grundschutz Methodology. (2008). Bundesamt für Sicherheit in der Informations technik. (Version 2.0). 26 Aralık 2018 tarihinde https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSI Standards/standard_1002_e_pdf.pdf?__blob=publicationFile&v=1 adresinden erişildi.

BSI-Standard 100-3 Risk analysis based on IT-Grundschutz. (2008). Bundesamt für

Sicherheit in der Informations technik. (Version 2.5). 26 Aralık 2018 tarihinde https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile&v=1adresinden erişildi.

BSI-Standard 100-4 Business Continuity Management. (2008). Federal Office for Information Security. (Version 1.0). 26 Aralık 2018 tarihinde https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Standards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1 adresinden erişildi.

Bük, A. (2015). *Elektronik ortamda saklanan kişisel verilerin elde edilmesi /değiştirilmesi suretiyle işlenen suçların ceza hukuku açısından değerlendirilmesi* (Doktora Tezi). Polis Akademisi, Ankara.

Büyüköztürk, Ş. (2018). *Veri analizi el kitabı.* (24. Baskı). Ankara: Pegem Akademi.

Byrne,, A. (2002). Information ethics for a new millenium. A. Vaagan ve diğerleri (Ed.). *The ethics of librarianship: An international survey* (s.8-18) içinde. Saur, München: IFLA.

Caballero, A. (2014). Chapter1 - Information Security Essentials for IT Managers: ProtectingMission-Critical Systems. Içinde J. R. Vacca (Ed.), *Managing Information Security (Second Edition)* (ss. 1-45). Doi: https://doi.org/10.1016/B978-0-12-416688-2.00001-5

Çakmak, T. (2011). Kurumsal içerik yönetimi kapsamında elektronik bilgi ve sistemlerinin bir kurum örneğinde değerlendirilmesi. (Yayımlanmamış yüksek lisans tezi). Hacettepe Üniversitesi, Ankara.

Can, A. (2014). *SPSS ile bilimsel araştırma sürecinde nicel veri analizi.* Ankara: Pegem akademi.

Chaudhry, A. S., ve Al-Mahmud, S. (2015). Information literacy at work. *The Electronic Library*, *33*(4), 760-772. Doi: https://doi.org/10.1108/EL-04-2014-0063

Cherdantseva, Y., ve Hilton, J. (2013b). A Reference Model of Information Assurance Security. *2013 International Conference on Availability, Reliability and Security*, 546-555. Doi: https://doi.org/10.1109/ARES.2013.72

Cherdantseva, Y., ve Hilton, J. (2013a). Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals,". Içinde *F. Almeida, and I. Portela (eds.), Organizational, Legal, and Technological Dimensions of IS Administrator*. Doi: https://doi.org/10.4018/978-1-4666-4526-4.ch010

Connoly, M. (2018). *User privacy: A practical guide for librarians*. Rowman & Littlefield.

Cooke, L. (2018). Privacy, libraries and the era of big data. *IFLA Journal*, *44*(3), 167 169.

Council of Europe. (1950). European convention on human rights. 14 Mayıs 2019 tarihinde https://www.echr.coe.int/Documents/Convention_ENG.pdf adresinden erişildi.

Cox, K. L. (2018). The general data protection regulation: What does it mean for Libraries Worldwide?. *Association of Research Libraries.* 6 Ekim 2018 tarihinde https://www.arl.org/storage/documents/IssueBrief_GDPR_May 2018.pdf adresinden erişildi.

Çalıkuşu, F., Karamehmet, B., ve Denizci, Ö. M. (t.y.). *Bilgi güvenliği yönetim sistemi kapsamında risk yönetimi modeli*.

Çam, H., Aslay, F. ve Özen, Ü. (2019). Yükseköğretim kurumlarında bilgi güvenliği farkındalık düzeylerinin ölçümlenmesi. *Yönetim Bilişim Sistemleri Dergisi, 5*(2), 1-11. 3 Ocak 2020 tarihinde https://dergipark.org.tr/tr/download/article-file/909714 adresinden erişildi.

Çek, E. (2017). *Kurumsal bilgi güvenliği yönetişimi ve bilgi güvenliği için insan faktörünün önemi.* (Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi, İstanbul.

Çelebioğlu, D. (2005). *Türkiyede bilgi ve iletişim teknolojilerinde bilgi güvenliği*

(Telekomünikasyon Kurumu). http://afyonluoglu.org/PublicWebFiles/Reports-TR/Uzmanlik_Tez/BTK/siber/2005%20%C5%9Eubat%20T%C3%BCrkiyede%20B%C4%B0T%20Bilgi%20G%C3%BCvenli%C4%9Fi.PDF adresinden erişildi.

Çelik, A., ve Uçak, N. (1993). Üniversite kütüphaneleri üzerine. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi, 10*(2), 115-121.

Çokmutlu, M. (2014). *Türk ceza hukukunda kişisel verilerin korunması* (Doktora tezi). Kocaeli üniversitesi, Kocaeli.

Collins. (2020). Definition of third party. Erişim adresi: https://www.collinsdictionary.com/dictionary/english/third-party

Coombs, K. A. (2004). Walking a tightrope: Academic libraries and privacy. *The Journal of Academic Librarianship, 30*(6), 493-498. Doi:https://doi.org/10.1016/j.acalib.2004.08.003

Çukadar, S., Gürdal, G., Çelik, S. ve Kahvecioğlu, K. (2011, 27-29 Mayıs). Türkiye'de üniversite kütüphaneleri: Mevcut durum ve gelecek. (ed. Durmuş Günay ve ErcanÖztemel). Uluslararası Yükseköğretim Kongresi: Yeni Yönelişler ve Sorunlar Bildiri Kitabı içinde, 3. Cilt, Bölüm 16, 2426-2439.

DPA 2018. (2018) Chapter 12. http://www.legislation.gov.uk/ukpga/2018/12/introduction/enacte adresinden erişildi.

Değer, M.K. ve Öztürk, N.G. (2017). 21.yüzyıl kütüphaneleri: Karma(hybrid) kütüphaneler. II.Uluslararası Sosyal Bilimler Sempozyumu içinde (s. 2577-2581). 18-19-20 Mayıs 2017, Alanya.

Demirok, E. (2016). *Kurumsal bilgi güvenliği yönetim sistemi uygulaması; Vakıf Üniversitesi örneği* (Yüksek Lisans Tezi). Okan Üniversitesi, İstanbul.

Dinkçi, F. (2014). *Kişisel verilerin korunmasında uluslararası düzenlemeler ve Türkiye örneği* (Yüksek Lisans Tezi). Ondokuz Mayıs Üniversitesi, Samsun.

Doğantimur, F. (2009). *ISO 27001 standardı çerçevesinde kurumsal bilgi güvenliği* (Mesleki Yeterlilik Tezi). Strateji Geliştirme Başkanlığı, Maliye Bakanlığı.

Düşünce özgürlüğü bildirgesi. (2008, Şubat 22). *Türk Kütüphaneciler Derneği.* 19 Kasım 2018 tarihinde http://37.230.106.98/~kutuphaneciorg/wp-content/uploads/Dusunce_Ozgurlugu_Bildirgesi-724x1024.jpg adresinden erişildi.

Easttom, C., ve Butler, W. (2019). A modified McCumber cube as a basis for a taxonomy of cyberattacks. *2019 IEEE 9th Annual Computing andCommunication Workshop and Conference (CCWC)*, 0943-0949. Doi: https://doi.org/10.1109/CCWC.2019.8666559

Ekiz, D. (2015). *Bilimsel araştırma yöntemleri: Yaklaşım, yöntem ve teknikler.* (4. Baskı). Ankara: Anı yayıncılık.

Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği. (2014, 13 Temmuz). *Resmî Gazete.* (30808).http://www.resmigazete.gov.tr/eskiler/2019/20190621-3.htm adresinden erişildi.

Elektronik Haberleşme Kanunu (2008, 10 Kasım). *Resmî Gazete. (27050).* 25 Haziran 2019 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf adresinden erişildi.

Elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğin korunması hakkında yönetmelik. (2012, 24 Temmuz). *TC Resmî Gazete. (28363).* 4 Ekim2018 tarihinde http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.16405&MevzuatIliski=0&sourceXmlSearch=ki%C5%9Fisel%20 verilerin adresinden erişildi.

Emiral, F. (2014). Bilgi güvenliği bilincinin genele yayılması. 5 Aralık 2018 tarihinde *http://www.denetimnet.net/UserFiles/Documents/50_45_1.pdf* adresinden erişildi.

Erdinç, G. H. (2017). *Bilgi güvenliği, kişisel verilerin korunması ve biyometrik verilerin işlenmesine ilişkin öneriler* (Yüksek Lisans Tezi). İstanbul Teknik Üniversitesi, İstanbul.

Eric, D. J. (1997). Managing information about people: Data protection issues for academic library managers. *Library Management*, *18*(1), 42-52. Doi: https://doi.org/10.1108/01435129710157734

Eroğlu, Ş. (2018). Dijital Yaşamda Mahremiyet (Gizlilik) Kavramı ve Kişisel Veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğrencilerinin Mahremiyet ve Kişisel Veri Algılarının Analizi. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, *35*(2), 130-153. Doi: https://doi.org/10.32600/huefd.439007

Ersoy, U. (2009). *Bir insan hakları kavramı olarak "kişisel verilerin korunması"*. (Yüksek Lisans Tezi). Gazi Üniversitesi, Ankara.

Ersöz, F. ve Ersöz, T. (2019). *SPSS ile istatiksel veri analizi.* Ankara: Seçkin Yayıncılık.

European Commission. (2019). Rules on international data transfers [Text]. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en adresinden erişildi.

European Commission, &Directorate-General for Justice and Consumers. (2016). *Guide to the EU-U.S. privacy shield.* Luxembourg: Publications Office.

European Data Protection Supervisor. (2018). *Guidelines on the protection of personal data in IT governance and IT management of EU institutions*. https://edps.europa.eu/sites/edp/files/publication/it_governance_ management_en.pdf adresinden erişildi.

European Commission. (2018). National Data Protection Authorities. Erişim adresi:http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=50061

European Commission. (2019). Commission implementing decision of 23.01.2019 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of The council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information. Brussels. 19 Nisan 2019 https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf adresinden erişildi.

European Commission. (2016). Guide totheEu-U.S. PrivacyShield. Belgium. 12 Ekim 2018 tarihinde https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf adresinden erişildi.

Federal Act on Data Protection. (19 June, 1992). 20 Nisan 2019 tarihinde https://www.admin.ch/opc/en/classifiedcompilation/19920153/201903010000/235.1.pdf adresinden erişildi.

FERPA. (1974). Family educational and privacy rights. 18 Ağustos 2019 tarihinde https://www.govinfo.gov/content/pkg/USCODE-2011-title20/pdf/USCODE-2011-title20-chap31-subchapIII-part4-sec1232g.pdf adresinden erişildi.

FFIEC. (2016). Information Security. 18 Ağustos 2019 tarihinde https://ithandbook.ffiec.gov/media/274793/ffec_itbooklet_informationsecurity.pdf adresinden erişildi.

Firarek, A. (2002). Technology and privacy in the academic library. *Online Information Review*, *26*(6), 366-374. Doi: https://doi.org/10.1108/14684520210452691

Friðgeirsdóttir, S. (2002). Librarians and information specialist ethical issues: an Icelandic perspective. A. Vaagan ve diğerleri (Ed.), *The ethics of librarianship: An international survey*(s.123-141) içinde. Saur, München: IFLA.

FTC. (2015, Şubat 27). Information for EU Residents Regarding the U.S. – EU Safe Harbor Program. https://www.ftc.gov/tips-advice/business-center/guidance/information-eu-residents-regarding-us-eu-safe-harbor-program adresinden erişildi.

GDPR Archives. (2019). GDPR.eu. https://gdpr.eu/tag/gdpr/ adresinden erişildi.

Genç, C. (2019). Kişisel verilerin korunması kapsamında bilgi güvenliği farkındalığı analizi ve e-devlet yapısının incelenmesi. (Yüksek Lisans Tezi). İstanbul Okan Üniversitesi, İstanbul.

Givens, C. (2015). *Information privacy fundamentals for librarians and information proffessionals.* London: Rowman&Littlefield.

Grama, L. J. (2011). *Legal issues in informationsecurity*. London: Jones&Bartlett Learning.

Gramm-LeachBlileyAct (GLBA). (1999).PublicLaw 106-102-NOV.12. 21 Ağustos 2019

tarihinde https://www.govinfo.gov/content/pkg/STATUTE-113/pdf/STATUE-113-Pg1338.pdf adresinden erişildi.

Great Britain. (1998). *Data Protection Act 1998: Elizabeth II. 1998. Chapter 29.* London: Stationery Office.

Gültekin, N. M. (2012). *Kişisel verilerin ceza hukuku yönünden korunması*. Galatasaray Üniversitesi, İstanbul.

Güneş, G., Bozkurt, E., Sönmez, S., ve Çakır, N. (2015). Kütüphanelerde iç hava kalitesinin incelenmesi: Marmara Üniversitesi Merkez Kütüphanesi. *Bilgi Dünyası*, *16*(2), 222-241.Doi: https://doi.org/10.15612/BD.2015.486

Güngör, M. (2015). *Ulusal bilgi güvenliği: Strateji ve kurumsal yapılanma* (Uzmanlık Tezi). Bilgi Toplumu Dairesi Başkanlığı, Kalkınma Bakanlığı. http://www.bilgitoplumu.gov.tr/wpcontent/uploads/2015/11/Ulusal_Bilgi_ Guvenligi _Strateji_ve_Kurumsal_Yapilanma.pdf

Güneş, G. (2009). *Bilgi ve belge merkezleri çalışanlarının iş ortamından kaynaklanan sağlık şikayetleri ve risk faktörleri.* (Doktora Tezi). Marmara Üniversitesi, İstanbul.

Güriş, A. ve Astar, M. (2014). *Bilimsel araştırmalarda istatistik.* İstanbul: Der yayınları.

Gürsel, E., ve Düğmeci, F. (2018). Yapısal anlamda Türkiye Kişisel Verileri Koruma Kurumu'na ilişkin bir değerlendirme. *Research Studies Anatolia Journal*, *1*(2), 318-329. Doi: https://doi.org/10.33723/rs.430753

Gürsel, İ. (2016). Protection of personal data in international law and the general aspects of the Turkish data protection law. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, *18*(1), 33-61.

Haklı, T. (2012). *Bilgi güvenliği standartları ve kamu kurumları bilgi güvenliği için bir model önerisi* (Yüksek Lisans Tezi). Süleyman Demirel Üniversitesi, Isparta.

Harris, J. L., veDiMarco, S. R. (2010). Locking down a university library: how to keep people safe in a crisis: A Mansfield University of Pennsylvania

Perspective. *Library &Archival Security*, *23*(1), 27-36. Doi : https://doi.org/10.1080/01960071003591523

Henkoğlu, T. (2015a). *Bilgi güvenliği ve kişisel verileri korunması*. Ankara: Yetkin Yayınları.

Henkoğlu, T. (2015b). *Hassas bilgi varlıklarının ve kişisel verilerin hukuksal düzenlemeler ile korunması ve bu kapsamda üniversiteler için bilgi güvenliği politikasının geliştirilmesi* (Doktora Tezi). Hacettepe Üniversitesi, Ankara.

Henkoğlu, T. ve Uçak, N.Ö. (2012). Elektronik bilgi güvenliğinin sağlaması ile ilgili hukuki ve etik sorumluluklar. *Bilgi Dünyası, 13*(2), 377-396.

Henkoğlu, T. ve Yılmaz, B. (2013). Avrupa Birliği bilgi güvenliği politikaları. *Türk Kütüphaneciliği, 27*(3), 451-471.

Henkoğlu, T., ve Uçak, N. Ö. (2015). Üniversite kütüphanelerinde kişisel verilerin korunması. *Bilgi Dünyası, 16*(1), 45-74. Doi: https://doi.org/10.15612/BD.2015.472

HIPPA. (1996).PublicLaw 104-191 § 21 Ağustos 2019 tarihinde https://www.govinfo.gov/content/pkg/ PLAW-104publ191/pdf/PLAW-104publ191.pdf adresinden erişildi.

NicholsHess, A., LaPorte-Fiori, R., ve Engwall, K. (2015). Preserving patron privacy in the 21st century academic library. *The Journal of Academic Librarianship, 41*(1), 105-114. Doi:https://doi.org/10.1016/j.acalib.2014.10.010

Höne, K. ve Eloff, J. H. P. (2002). Information security policy—What do international information security standards say? *Computers& Security*, *21*(5), 402-409. Doi:https://doi.org/10.1016/S0167-4048(02)00504-7

IFLA. (2018). *Briefing: Impact of the General data protection regulation 2018*. 6 Ekim 2018 tarihinde https://www.ifla.org/files/assets/clm/publications/briefing_ *general_data_protection_regulation_2018.pdf* adresinden erişildi.

IFLA. (1999). Kütüphaneler ve düşünce özgürlüğü konulu IFLA bildirisi. (K. Gezgin, Çev.). *IFLA Committe on Freedom of Access to Information and Freedom of*

*Expression.*19 Kasım 2018 tarihinde https://www.ifla.org/files/assets/faife/statements/iflastat_tr.pdf adresinden erişildi.

Information Commissioner's Office. (2018). *Guide to the General Data Protection Regulation (GDPR)*. https://ico.org.uk/for-organizations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-ispersonal-data adresinden erişildi.

Inoue, Y. (2018). Privacy and libraries in the case of Japan. *IFLA Journal*, *44*(3), 223-228. Doi: https://doi.org/10.1177/0340035218785391

Inoue, Y. (2002). The code of ethics of the Japan Library Association. A. Vaagan ve diğerleri (Ed.), *The ethics of librarianship: An international survey* (s.142-162) içinde. Saur, München: IFLA.

Is your library ready for GDPR? (2018). Axiell. 6 Ekim 2018 tarihinde https://www.axiell.co.uk/is-your-library-ready-for-gdpr-4-month-klaxon/ adresinden erişildi.

ISO/IEC. (2009). *ISO/IEC 27000:2009 Information technology- Security techniques-Information security management systems-Overview and vocabulary.* https://www.iso.org/standard/41933.html adresinden erişildi.

ISO/IEC. (2018). ISO/IEC 27000:2018 *Information technology – Security techniques – Information security management systems-Overview and vocabulary.* 18 Aralık 2018 tarihindehttps://standards.iso.org./ittf/PubliclyAvailable Standards/c0739006_ISO_IEC_2700_2018_E.zip adresinden erişildi.

ISO/IEC. (2018). ISO/IEC 27005:2018 *Information technology – Security techniques – Information security risk management.* 23 Aralık 2018 tarihinde https://www.iso.org/obp/ui/#iso:std:isoiec:27005:ed-3:v1:en adresinden erişildi.

ISO/IEC. (2017). ISO/IEC 27007:2017 *Information technology – Security techniques – Guidelines for Information Security Management Systems Auditing*. 23 Aralık 2018 tarihinde https://www.iso.org/obp/ui/#iso:std:iso-iec:27007:ed-2:vl:en adresinden erişildi.

ISO/IEC. (2017). ISO/IEC 27003: 2017. *Information technology – Security techniques –*

Information security management system -- Guidance. 23 Aralık 2018 tarihinde https://www.iso.org/standard/63417.html adresinden erişildi.

ISO/IEC. (2016). ISO/IEC 27004:2016. *Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation.* 23 Aralık 2018 tarihinde https://www.iso.org/obp/ui/#iso:std:iso-iec:27004:ed-2:vl:en adresinden erişildi.

ISO/IEC. (2015). ISO/IEC 27006:2015. *Informatontechnology – Security techniques – Requirements for bodies providing audit and certification of information security management systems.* 23 Aralık 2018 tarihinde https://www.iso.org/obp/ui/#iso:std:iso-iec:27006:ed-3:vl:en adresinden erişildi.

ISO/IEC. (2013). ISO/IEC 27002:2013. *Information technology – Security techniques – Code of practice for information security controls.* 23 Aralık 2018tarihinde https://www.iso.org/standard/54533.html adresinden erişildi.

ISO/IEC. (2013). ISO/IEC 27001:2013. *Information technology – Security techniques – Information security management systems – Requirements.* 18 Aralık 2018 tarihinde https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en adresinden erişildi.

ISO/IEC. (2010). ISO/IEC 27003: 2010. *Information technology – Security techniques – Information security management system implementation guidance.* 23 Aralık 2018 tarihinde https://www.iso.org/standard/42105.htmladresinden erişildi.

ISO/IEC. (2009). ISO/IEC 27004:2009. *Information technology – Security techniques – Information security management – Measurment.* 23 Aralık 2018 tarihinde https://www.iso.org/standard/42106.html adresinden erişildi.

ISO/IEC. (2008). ISO/IEC 27005:2008 *Information technology – Security techniques – Information security risk management.* 23 Aralık 2018 tarihinde https://www.iso.org/standard/42107.html adresinden erişildi.

ISO/IEC. (2005). ISO/IEC 27002:2005. *Information technology – Security techniques –*

Code of practice for information security management. 23 Aralık 2018 tarihindehttps://www.iso.org/standard/50297.html adresinden erişildi.

ISO/IEC. (2005). ISO/IEC 17799: 2005 *Information security – Security techniques – Code of practice for information security management.* 23 Aralık 2018 tarihinde https://www.iso.org/standard/39612.htmladresinden erişildi.

Kanyengo, C. W. (2009). Preservation and conservation of information resources in the University of Zambia Library. *Journal of Archival Organization, 7*(3), 116-128. Doi :https://doi.org/10.1080/15332740903126736

Kaptan, S. (1989). *Bilimsel araştırma ve gözlem teknikleri.* Ankara: Tekışık Matbaası.

Kartal, M. T. (2018). Kişisel verilerin korunması: Türk bankacılık sektörü üzerine kavramsal bir değerlendirme. *Uluslararası Ekonomi ve Yenilik Dergisi*, *4*(1), 1-18. Doi: https://doi.org/10.20979/ueyd.347548

Kaya, C. (2011). Avrupa Birliği veri koruma direktifi ekseninde hassas (kişisel) veriler ve işlenmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 69*(1-2), 317-334.

Khoo, B., Harris, P., ve Hartman, S. (2010). Information security governance of enterprise information systems: an approach to legislative compliant. *International Journal of Management & Information Systems (IJMIS), 14*(3), 49-56. Doi: https://doi.org/10.19030/ijmis.v14i3.840

Kılınç, D. (2012). Anayasal bir hak olarak kişisel verilerin korunması. *Ankara Üniversitesi Hukuk Fakültesi Dergisi, 61*(3), 1089-1169.

Killmeyer, J. (2000). Information security architecture. İçinde *Information Security Architecture : An Integrated Approach to Security in the Organization* (1 st, ss. 1-24). New York: Auerbach Publications. Doi: https://doi.org/10.1201/9781420031034

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi rehberi. (2018). KVKK. Kişisel Verileri Koruma Kurulu Yayınları, Ankara.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi hakkında

yönetmelik. (2017, 28 Ekim). *Resmî Gazete.* (Sayı: 30224). http://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm adresinden erişildi.

Kişisel sağlık verilerinin işlenmesi ve mahremiyetinin sağlanması hakkında yönetmelik. (2016, 20 Ekim). *Resmî Gazete.* (Sayı: 29863). http://www.resmigazete.gov.tr/eskiler/2016/10/20161020-1.htm adresinden erişildi.

Kişisel sağlık verileri hakkında yönetmelik. (2019, 21 Haziran). *Resmî Gazete.* (Sayı: 30808). http://www.resmigazete.gov.tr/eskiler/2019/06/20190621-3.htm adresinden erişildi.

KVKK. (2018). Kişisel verilerin korunması alanında uluslararası ve ulusal düzenlemeler. 7 Mayıs 2019 tarihinde https://kvkk.gov.tr/SharedFolderServer/CMSFiles/ead8e671-e01e-4ca7-a6a3-bc3c6f79f7c7.pdf adresinden erişildi.

Kocamustafaoğulları, M. (2013). *A prototype for assessment of information security awareness and ımplementation level* (Master Thesis). Çankaya University, Ankara.

Korn, N., ve Tullo, C. (2018). *A practical guide to data protection for information professionals.* Chartered Institute of Library and Information Proffessionals: the library and information association. 6 Ekim 2018 tarihinde https:c.ymcdn.com/sites/www.cilip.org.uk/resource/resmgr/CILIP/Campaigns/GDPR/CILIP/PGDP_2018_WEB.pdfadresinden erişildi.

Kutlu, Ö., ve Kahraman, S. (2017). Türkiye'de kişisel verilerin korunması politikasının analizi. *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi*, *5*(4), 45-62.

Kuzucuoğlu, A.H. (2014). Kütüphanelerde yapısal olmayan malzeme kaynaklı riskler. *Bilgi ve Belge Araştırmaları Dergisi*, *2*, 21-38.

Kuzucuoglu, A. (2016, Mayıs 12). *Yerel yönetimlerdeki bilgi ve kültür merkezlerinde acil durum planlamasının önemi*. 121-133. http://bkahs.org/?bildiri=1311 adresinden erişildi.

Kuzucuoğlu, A. H. (2018). Kütüphanelerde yapısal olmayan malzeme kaynaklı riskler. *Bilgi ve Belge Araştırmaları Dergisi*, (2), 21-38.

Kuzucuoğlu, A.H. (2018, Nisan). *Kütüphane Güvenlik Yaklaşımları.* ANKOSLINK Konferasında sunulan poster, Antalya.

Küçükcan, B., ve Öztürk, A. (2017). Kütüphane binalarında engelli kullanıcılara yönelik tasarım ilkeleri. (Yay. Haz. Özgür Külcü, Tolga Çakmak ve Şahika Eroğlu) Içinde *Kamusal Alan Olarak Bilgi Merkezleri ve Yenilikçi Yaklaşımlar* (1. Baskı, ss. 293-324). İstanbul: Hiperlink Yayınları.

Külcü, Ö. (2018). Dijital çağda kamusal bilginin oluşumu, güvenilirliği, korunması ve erişilebilirliği. BBY Yaz Semineri. Bilgi ve Belge Yönetimi Bölümü, Hacettepe Üniversitesi. 14 Mayıs 2019 tarihinde http://www.acikders.net/pluginfile.php/7974/mod_resource/content/1/BBY_YazSemineri2018_OzgurKulcu.pdf adresinden erişildi.

Külcü, Ö. (20-24 Kasım, 2017). Dijital çağda bilginin güvenilirliği kurumsal arşiv ve belge yönetimi stratejilerinin geliştirilmesi. Uluslararası Osmanlı Coğrafyası Arşiv Kongresi. Bilgi ve Belge Yönetimi Bölümü, Hacettepe Üniversitesi. 14 Mayıs 2019 tarihinde http://bby.hacettepe.edu.tr/akademik/ozgurkulcu/file/Digital%20Du%CC%88nyada%20Bilgi%20Gu%CC%88venlig%CC%86i.ppt adresinden erişildi.

Küzeci, E. (2010). *Kişisel verilerin korunması* (Doktora Tezi). Ankara Üniversitesi, Ankara.

Maidabino, A. A, ve Zainab, A. N. (2011). Collection security management at University libraries: Assessment of its implementation status. *Malaysian Journal of Library & Information Science*, *16*(1), 15-33.

Maidabino, A. A., ve Zainab, A. N. (2012). A holistic approach to collection security implementation in university libraries. *Library Collections, Acquisitions, & Technical Services*, *36*(3-4), 107-120. Doi: https://doi.org/10.1080/14649055.2012.10766335

McCumber, J. (2004). *Assessing and managing security risk in IT Systems: A structured methodology*. Doi: https://doi.org/10.1201/9780203490426

McMenemy, D., Poulter, A., ve Burton, P. (2007). *A handbook of ethical practice* (1st Edition). England: Chandos Publishing.

Mesleki etik ilkeleri. (1996). *Türk Kütüphaneciler Derneği.*

Muharremoğlu, G. (2013). *Kurumsal bilgi güvenliğinde zafiyet, saldırı ve savunma öğelerinin incelenmesi* (Yüksek Lisans Tezi). İstanbul Üniversitesi, İstanbul.

National Conference of StateLegislatures. (2018). Security Breach Notification Laws. 21 Ağustos 2019 tarihinde http://www.ncsl.org/research/ telecommunications-and-information-technology/security-breach-notification-laws.aspx adresinden erişildi.

Nedir.com. (2016). IDS nedir?. Erişim adresi: https://www.nedir.com/ids

NIST Special Publication 800-series General Information. (2018, May 21). *NIST Information Technology Laboratory.* 26 Aralık 2018 tarihinde https://www.nist.gov/itl/nist-special-publication-800-series-general-information adresinden erişildi.

Noh, Younghee. (2017). A Critical Literature Analysis of Library and User Privacy. *International Journal of Knowledge Content Development &Technology, 7*(2), 53-83. Doi: https://doi.org/10.5865/IJKCT.2017.7.2.053

Noh, Y. (2014). Digital library user privacy: Changing librarian view points through education. *Library HiTech, 32*(2), 300-317.Doi: https://doi.org/10.1108/LHT-08-2013-0103

NSTISSI. (1994). National training standard for ınformation systems security (ınfosec) professionals. 16 Aralık 2018 tarihinde https://cec.nova.edu/ Documents/nstissi_4011.pdf adresinden erişildi.

OECD. (1980). Guidelines on the protection of privacy and transborder flows of personal data. https://www.oecd.org/internet/ieconomy/oecdguideline sonthe protectionofprivacyandtransborderflowsofpersonaldata.htm adresinden erişildi.

OECD. (2013). *New data for understanding the human condition: international*

perspectives. 3 Ekim 2018 tarihinde https://www.oecd.org/sti/sci-tech/new-data-for-understanding-the-human-condition.pdf adresinden erişildi.

Office of the PrivacyCommissioner of Canada. (2019). PIPEDA in brief. 19 Nisan 2019 tarihinde https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal- information-protection-and-electronic-documents-act-pipeda/pipeda_brief/adresinden erişildi.

Öztemiz, S., ve Yılmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği. *Bilgi Dünyası, 14*(1), 87-100.

Öz, Z. O. (1992). Kütüphane binalarının mekânsal organizasyonlarında ergonominin önemi ve standardizasyon. *Türk Kütüphaneciliği, 6*(3), 159-171.

Paraschiv, P. (2018, 9 February). GDPR compliance for libraries 5 general aspects. [Blog post]. 6 Ekim 2018 tarihinde *https://princh.com/gdpr-compliance-for-libraries-libraries-5-general-aspects-that-you-need-to-cover/#.W-IfZ5MzbIX* adresinden erişildi.

PCI DSS Council. (2018). Requirements and security assessment procedures. (Version 3.2.1).21 Aralık 2019 tarihinde https://www.pcisecuritystandards.org/ documents/PCI_DSS_v3-2-1.pdf adresinden erişildi.

Personal Data Protection Commission Singapore. (2015). *Your personal data your choice: A quick guide to Personal Data Protection Act for individuals*. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/pdpa-for-individuals-v1-0.pdf adresinden erişildi.

Poore, R.S. (1990, Fall). Generally Accepted System Security Principles. International Information Security Foundation. (27-77). 25 Aralık 2018 tarihinde http://www.infosectoday.com/Articles/gassp.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. 13 Ekim 2018 tarihinde https://www.ifla.org/files/assets/faife/publications/misc/ dilemmas-in-the-information-society.pdf adresinden erişildi.

Personal Information Protection and Electronic Documents Act. (June 20, 2019). 21 Ağustos 2019 tarihinde https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

adresinden erişildi.

Polater, S. (2019). Kişisel verilerin reklam amaçlı işlenmesinde hukuka uygunluk sebepleri. *Kişisel Verileri Koruma Dergisi*, *1*(1), 1-20.

Privacy Sheld Framework. (t.y.). *Privacy Shield Overview.* 19 Kasım 2018 tarihinde https://www.privacyshield.gov/Program-Overview adresinden erişildi.

Punch, K.F. (2005). *Sosyal araştırmalara giriş: Nicel ve nitel yaklaşımlar*. (Bayrak, D., Arslan, H.B. ve Akyüz, Z.). Ankara : Siyasal Kitabevi.

Qureshi, M.S. (2011). *Measuring efficiacy of information security policies: A case study of UAE based 0company.*

Robson, C. (2015). *Bilimsel araştırma yöntemleri: Gerçek dünya araştırması.* (Ed. Çınkır, Şakir ve Demirkasımoğlu, N.) Ankara: Anı Yayıncılık.

Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname (2011, 2 Kasım). *Resmî Gazete* (Sayı:28103). 10 Ekim 2018 tarihinde http://www.resmigazete.gov.tr/eskiler/2011/11/20111102M1-3.htm adresinden erişildi.

Seferoğlu, S.S., Durak, H.Y., Yılmaz, F.G ve Yılmaz, R. (2018). Bilgi güvenliği farkındalığı ve bilgi güvenliği politikalarıyla ilgili bir inceleme. B. Akkoyunlu, A.İşman ve H.F. Odabaşı (Ed). Eğitim teknolojileri okumaları 2018, (3. Bölüm, ss. 29-43). TOJET ve Sakarya Üniversitesi, Adapazarı.

Sequiera, D. (2002). Librarianship ethics in Costa Rica. A. Vaagan ve diğerleri (Ed.), *The ethics of librarianship: An international survey* (s.59-80) içinde. Saur, München, IFLA.

Sert, Ş. (2019). *Kişisel verilerin Türk Ceza Kanunu* kapsamında korunması. Ankara: Seçkin yayıncılık.

Sezgen, D. A. (1992). *Ankara'da üniversite kütüphane binaları* (Yüksek lisans tezi). Hacettepe Üniversitesi, Ankara.

Shuler, J.A. (2004). Privacy and academic libraries: Widening the frame of discussion. *The Journal of Academic Librarianship, 30*(2), 157-159.Doi:

https://doi.org/10.1016/j.acalib.2004.01.008

Sing, A., Vaish, A., ve Keserwani, P. K. (2014). Information security: Components and techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(1), 1072-1077.

Smith, J. (2018, Ocak 10). Members [Text]. European Data Protection Board—5 Eylül 2019 tarihinde https://edpb.europa.eu/about-edpb/board/members_en adresinden erişildi.

Solms, B. V. (2000). Information Security—The Third Wave? *Computers& Security*, *19*(7), 615–620. Doi: https://doi.org/10.1016/S0167-4048(00)07021-8

Solms, B. V. (2006). Information Security – The Fourth Wave. *Computers& Security*, *25*(3), 165-168. Doi: https://doi.org/10.1016/j.cose.2006.03.004

Surwade, Y., ve Patil, H. (2019, Ocak 24). *Information security*. 458-466.

Sturges, P., Davies, E., Dearnley, J., Iliffe, U., Oppenheim, C. ve Hardy, R. (2003). User privacy in the digital library environment: an investigation of policies and policies and preparedness. *Library Management*, *24*(1/2), 44-50. Doi: https://doi.org/10.1108/01435120310454502

Sturges, P., Teng, V. ve Iliffe, U. (2001). User privacy in the digital library environment: a matter of concern for information professionals, *Library Management*, *22*(8/9), 364-370.
Doi: https://doi.org/10.1108/01435120110406309

Swanson, M. ve Guttman, B. (1996). Generally Accepted Principles and Practices for Securing Information Technology Systems: Computer Security. NIST Special Publication 800-14. 25 Aralık 2018 tarihinde https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-14.pdf adresinden erişildi.

Şahinaslan, E., Kantürk, A., Şahinaslan,Ö. ve Borandağ, E. (2009). Kurumsal bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *Akademik Bilişim'09-XIAkademik Bilişim Konferansı* içinde (s.597-602). Şanlıurfa: Harran Üniversitesi.3 Ocak 2020 tarihinde https://www.guvenliweb.org.tr/dosya/cCvJ7.pdf adresinden erişildi.

Şimşek, O. (2008). *Anayasa hukukunda kişisel verilerin korunması*. İstanbul: Beta Kitap.

Şişkin, D. Ş. ve Çakmak, T. (2019). Türkiye'de kişisel verilerin korunması:1996-2019 yılları arasındaki bilgi politikası belgelerine yönelik bir değerlendirme. *e-BEYAS 2019: Endüstri 4.0 Sürecinde Bilgi Yönetimi ve Bilgi Güvenliği:eBelge-eArşiv-eDevlet-Bulut Bilişim-Yapay Zekâ* içinde (s. 465-482). Ankara: Ankara Üniversitesi. ISBN: 978-605-136-473-5. 3 Ocak 2020 tarihinde https://dspace.ankara.edu.tr/xmlui/handle/123456789/68967 adresinden erişildi.

Tamre, M. (2002). Collaboration between Estonian Librarians Association and Estonian Libraries. A. Vaagan ve diğerleri (Ed.), *The ethics of librarianship: An international survey* (s.81-95) içinde. Saur, München: IFLA.

Taştan, F. G. (2017). *Türk sözleşme hukukunda kişisel verilerin korunması.* İstanbul: Oniki Levha Yayıncılık.

Tatar, N. (2015). *The comporasion of information security standards by using analytic hierarchy process* (Master Thesis). Çankaya University, Ankara.

TBMM. (2013). *Haberleşme özgürlüğüne ve özel hayatın gizliliğine yönelik ihlallerin tespiti ve önlenmesine ilişkin tedbirlerin belirlenmesi amacıyla kurulan meclis araştırması komisyonu raporu*. https://acikerisim.tbmm.gov.tr/xmlui/bitstream/handle/11543/102/ss489.pdf?sequence=1&isAllowed=y adresinden erişildi.

TBMM İnsan Haklarını İnceleme Komisyonu. İnsan Hakları ve Temel Özgürlükleri Korumaya Dair Avrupa Sözleşmesi. 4 Ekim 2018 tarihinde http://uhdigm.adalet.gov.tr/sozlesmeler/coktaraflisoz/ak/turkce/009_tur.pdf adresinden erişildi.

T.C. Anayasası. (2010). Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun. 4 Ekim tarihinde https://www.tbmm.gov.tr/kanunlar/k5982.html adresinden erişildi.

T.C. Anayasası. (2004). Türk Ceza Kanunu. 7 Mayıs 2018 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf adresinden

erişildi.

T.C. Anayasası. (1982). Türkiye Cumhuriyeti Anayasası. 4 Ekim tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf adresinden erişildi.

TCDDK. (2013). *Kişisel verilerin korunmasına ilişkin ulusal ve uluslararası durum değerlendirmesi ile bilgi güvenliği ve kişisel verilerin korunması kapsamında gerçekleştirilen denetim çalışmaları (Sy 3).*https://www.memurlar.net/common/news/documents/439122/ddk56.pdf adresinden erişildi.

T.C. Kalkınma Bakanlığı, Bilgi Toplumu Dairesi. (2013). Bilgi toplumu stratejisinin yenilenmesi projesi. 7 Ekim 2018 tarihindehttp://www.bilgitoplumustratejisi.org/download/docfile/8a3247663ecdf0f3013ef45408fd0005adresinden erişildi.

T.C. Başbakanlık. (2008). Kişisel Verilerin Korunması Kanun Tasarısı. 4 Ekim 2018 tarihindehttp://www2.tbmm.gov.tr/d23/1/1-0576.pdf adresindenerişildi.

Tofan, D. C. (2011). Information Security Standards. *Journal of Mobile, Embedded and Distributed Systems*, *3*(3), 128-135.

Toğuz, Ö. (2010). *Data protection and intellectual property in the EU and Turkey* (Master Thesis). Middle East Technical University, Ankara.

Tuğ İlçin, E., Adak, F. ve Çakır, H. (2014). Bilişim Güvenliği Tedbirleri ve TKDK Kurumunda Uygulama Örneği. *Bilişim Teknolojileri Dergisi, 7*(1), 11-18. Doi: https://doi.org/10.12973/bid.2012

Turan, M. (2018). A *systematic review of 6698-Law on theProtection of Personal Data in Turkey according to the information security practices and applicability of law perspective.* (Yüksek Lisans Tezi). Bahçeşehir Üniversitesi, İstanbul.

Türk Ceza Kanunu (2004, 26 Eylül). *Resmî Gazete.* (Sayı: 25611). 25 Haziran 2019 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf adresinden erişildi.

Uygun, M. (2010). *Avrupa Birliğinin 95/46 sayılı veri koruma yönergesi ışığında kişisel verilerin korunması* (Yüksek lisans tezi). Gazi Üniversitesi, Ankara.

United States Congress. (2002) Federal Information Security Management Act of 2002.

Pp.48-62. (Çevrimiçi). 14 Haziran 2019 tarihinde https://www.govinfo.gov /Content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf adresinden erişildi.

Ülker, M., Canbay, Y., ve Sağıroğlu, Ş. (2017). Nesnelerin internetinin kişisel, kurumsal ve ulusal bilgi güvenliği açısından incelenmesi. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, *10*(2), 28-41.

Ünsal, Ç. Z. (2013). Google'ın yeni gizlilik politikası Google Inc. tarafından 1 mart 2012 tarihinde yayımlanan politikasının kişisel verilerin korunması ilkeleri ile uyumluluğu ve Avrupa Birliği'nin 95/46/EC sayılı veri koruma direktifi açısından değerlendirilmesi. *Hacettepe Hukuk Fakültesi Dergisi*, *3*(1), 99-124.

Ünver, Ö., Gamgam, H. ve Altunkaynak, B. (2019). *SPSS uygulamalı temel istatistik yöntemler.* Ankara: Seçkin yayıncılık.

Vardal, N. (2009). *Yükseköğretimde bilgi güvenliği: Bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması* (Doktora Tezi). Gazi Üniversitesi, Ankara.

Veiga, A. D., ve Eloff, J. H. P. (2007). An ınformation security governance framework. *Information Systems Management*, *24*(4), 361-372. Doi: https://doi.org/10.1080/10580530701586136

Verton, D. (2000). Companies aim to build security awareness. *Computer world, 34*(48), 24.

Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri* (Yüksek Lisans Tezi). Gazi Üniversitesi, Ankara.

Vural, Y., ve Sağıroğlu, Ş. (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi,23*(2), 507-522.

Vural, Y., ve Sağıroğlu, Ş. (2011). Kurumsal bilgi güvenliğinde güvenlik testleri ve öneriler. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, *26*(1),

89-103. Doi: https://doi.org/10.17341/gummfd.27313

Waddell, S. A. (2013). *A study of the effect of information security policies on information security breaches in higher education institutions* (Doctoral Thesis). Nova Southeastern University, Florida. Proquest Dissertations and Theses veri tabanından erişildi (UMI No. 3604516).

What is FOIA? (t.y.). FOIA.gov. 12 Eylül 2019 tarihinde https://www.foia.gov/about.html adresinden erişildi.

Whitman, M. E., ve Mattord, H. J. (2017). *Principles of information securtiy* (Sixth edition). Boston, MA: Cengage Learning.

Whitman, M. E., ve Mattord, H. J. (2016). *Principles of information security* (Fifth edition). Boston, MA: Cengage Learning.

Whitman, M.E. ve Mattord, H.J. (2009). *Principles of Information Security.* 3th Edition. Cengage Learning, USA.

Wilson, T. (2000). Human ınformation behavior. *Information Science Research*, *3*(2), 49-56.

Wolters, P. T. J. (2017). Thesecurity of personal data under the GDPR: A harmonized duty or a shared responsibility? *International Data Privacy Law*, *7*(3), 165-178. Doi: https://doi.org/10.1093/idpl/ipx008

Wylder, J. (2003). *Strategic ınformation security.* Auerbach Publications.Doi: https://doi.org/10.1201/978020349708

Yamson, G. C., ve Cobblah, M. (2016). Assessments of collection security management in academic libraries: A case study of Central University Library. *European Scientific Journal, ESJ*, *12*(10). Doi: https://doi.org/10.19044/esj.2016.v12n10p%p

Yıldırım, C. (2015, Mart). *Kişisel verilerin korunması ve mahremiyet*. Kişisel verilerin korunması ve mahremiyet konferansında sunulan bildiri, Gelişim Hukuk Topluluğu.

Yıldız, B. (2007). *Bilgi güvenliği ve e-devlet kapsamında kamu kurumlarına bilgi güvenliği yönetimi standartlarının uygulanması* (Yüksek Lisans Tezi).

Gebze Yüksek Teknoloji Enstitüsü.

Yıldız, K. A. (2017). Türk kütüphaneciliğinde mekân, kullanıcı ve hizmet sorunlarının bir değerlendirmesi. *Marmara Türkiyat Araştırmaları Dergisi*, *4*(2), 417-430. Doi: https://doi.org/10.16985/MTAD.2017233887

Yılmaz, H. (2014). TS ISO/IEC 27001 bilgi güvenliği yönetimi standardı kapsamında bilgi güvenliği yönetim sisteminin kurulması ve bilgi güvenliği risk analizi. *Denetişim*, (15), 45-59.

Yılmaz, E. (2002). *Hukuk sözlüğü.* (7. Bsm.). Ankara: Yetkin Hukuk Yayınları.

Yüksek Öğretim Kurulu, Üniversite Kütüphaneleri Çalışma Grubu. (2014). *2023'e Doğru Türkiye'de Üniversite Kütüphaneleri: Mevcut Durum, Sorunlar, Standartlar ve Çözüm Önerileri.* 28 Aralık 2018 tarihinde http://yok.gov.tr/documents/9273450/9459025/Üniversite+Kütüphaneleri+Raporu+Yeni/ adresinden erişildi.

Yüksel Civelek, D. (2011). *Kişisel verilerin korunması ve bir kurumsal yapılanma önerisi* (Uzmanlık Tezi). Bilgi Toplumu Dairesi Başkanlığı, Devlet Planlama Teşkilatı.

EK-1: ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLERİN KORUNMASI : ANKARA'DAKİ ÜNİVERSİTE KÜTÜPHANELERİNİN DEĞERLENDİRİLMESİ

Değerli Katılımcı,

Bu çalışma, Ankara'da bulunan üniversite kütüphanelerinin kişisel verilerin yönetilmesi ve bilgi güvenliği konusunda karar vericilerin bilinç ve farkındalıklarını belirlemek amacıyla uygulanmaktadır. Görüşme formu sonucunda elde edilecek veriler, üniversite kütüphanelerinde kişisel verilerin yönetimi ve bilgi güvenliğine yönelik mevcut durumun ve karşılaşılan sorunların tespiti için kullanılacaktır.

Formun uygulanması için gerekli etik kurul izni alınmıştır. Elde edilecek veriler kişisel değerlendirmeye tabi tutulmayacak, sadece bilimsel amaçla kullanılacak olup, değerlendirmelerde kurum adı ya da kurum adını gösterecek tanımlamalara kesinlikle yer verilmeyecektir. Forma adınızı yazmanıza gerek yoktur. Görüşme formuna sağlayacağınız katkılar tamamen gönüllülük esasına dayanmaktadır. Formun uygulanması 10 dakikadan fazla zamanınızı almayacaktır. Bu forma vereceğiniz samimi yanıtlar araştırmanın başarısına önemli ölçüde katkı sağlayacaktır.

Formdan elde edilecek veriler Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı'nda Dr. Öğr. Üyesi Tolga Çakmak danışmanlığında yürütmekte olduğum yüksek lisans tezinde kullanılacaktır. Çalışma ile ilgili ayrıntılı bilgi almak ve çalışma hakkındaki sorularınız için dilansiskin@hacettepe.edu.tr adresinden iletişime geçebilirsiniz. Araştırmaya katılımınız ve değerli görüşleriniz için şimdiden teşekkür ederim.

Dilan Şerife ŞİŞKİN
Hacettepe Üniversitesi
Sosyal Bilimler Enstitüsü
Bilgi ve Belge Yönetimi Anabilim Dalı
Yüksek Lisans Öğrencisi

Bölüm I – Demografik Bilgiler

1. Yaşınız: ……
2. Eğitim Düzeyiniz
( ) Ortaokul
( ) Lise
( ) Yüksekokul
( ) Ön lisans
( ) Lisans
( ) Yüksek lisans
( ) Doktora

3. Göreviniz
( ) Daire Başkanı/Başkan Vekili
( ) Daire Başkan Yardımcısı
( ) Müdür/Direktör
( ) Müdür Yardımcısı/İdari Asistan
( ) Şube Müdürü
( ) Diğer (lütfen açıklama
yapınız:):……....

4. Kütüphanedeki çalışma süreniz (Yıl olarak belirtiniz): ……..

5. Lisans eğitiminizi Bilgi ve Belge Yönetimi (Kütüphanecilik, Dokümantasyon veya Arşivcilik anabilim dallarından birinde) bölümünde mi tamamladınız? (Eğer, lisansüstü/doktora eğitiminizi Bilgi ve Belge Yönetimi Bölümünde aldıysanız, lütfen diğer seçeneğinde belirtiniz.)
( ) Evet
( ) Hayır
( ) Diğer…… ……

Bölüm II – Kişisel Verilerin Yönetimi

6. Kütüphanenizde kullanıcı ve personel ile ilişkili olarak tutulan kişisel veriler nelerdir? (Kullanıcı : K, Kütüphane Personeli: KP olacak şekilde işaretlemelerinizi yapınız.)
K KP
( ) ( ) TC kimlik numarası
( ) ( ) Adı soyadı
( ) ( ) Nüfus bilgileri (yaş, cinsiyet, şehir, aile bilgileri)
( ) ( ) Kan grubu
( ) ( ) İletişim bilgileri
( ) ( ) Adresi
( ) ( ) Sicil Numarası
( ) ( ) Bölümü/Fakültesi/Enstitüsü
( ) ( ) Öğrenci Numarası
( ) ( ) Sınıfı

( ) ( ) Üyelik kartları
( ) ( ) Personel kartları
( ) ( ) Öğrenci kartları
( ) ( ) Unvanı
( ) ( ) Özgeçmişi
( ) ( ) Dili
( ) ( ) Kullanıcı adı
( ) ( ) Şifre
( ) ( ) Kişisel/Kurumsal e-posta hesabı
( ) ( ) Kişisel bilgisayarlara ait IP/MAC adresleri
( ) ( ) Kurumsal bilgisayarlarda web sayfasına yapılan ziyarete ilişkin kayıtlar
( ) ( ) Veri tabanı arama kayıtları
( ) ( ) Kurumsal bilgisayarlarda yapılan tarama oturumları
( ) ( ) Kullanıcının araştırma konuları
( ) ( ) Kütüphaneyi kullanma saatleri (giriş-çıkış)
( ) ( ) Ödünç işlemlerine (alınan kaynaklar, cezalar, uzatma talepleri gibi) yönelik bilgiler
( ) ( ) Kütüphane tarafından düzenlenen etkinliklere dair kayıtlar (konferans, seminer, kurs vb.) bilgileri

7. Kütüphanenizde kişisel veriler nasıl toplanıyor? (Birden fazla seçeneği işaretleyebilirsiniz.)

*Üçüncü parti kuruluş, kütüphanenizin veri paylaşımı gerçekleştirdiği kurum, dernek, vb. gerçek ve tüzel kuruluşlar.

( ) Öğrenci İşleri Dairesi Başkanlığından ilgili kütüphane sistemine aktarılarak
( ) Bilgi İşlem Dairesi Başkanlığından ilgili kütüphane sistemine aktarılarak
( ) Üçüncü parti (gerçek/tüzel) kuruluşlardan (örneğin kullanıcı bazında giriş-çıkış saatleri gibi) ilgili kütüphane sistemine aktarılarak
( ) Kullanıcı kitlesine sunulan kayıt formları aracılığıyla
( ) Personel Dairesi Başkanlığı aracılığıyla
( ) Diğer……

8. Kişisel veriler ilk olarak ne zaman kayıt altına alınmaktadır?

( ) Her dönem başında üniversitenin ilgili sistemlerinden otomatik olarak alınmaktadır.
( ) Kullanıcı bilgisi üniversitenin ilgili sistemine (öğrenci işleri, personel işleri gibi) kaydedildiği anda kütüphane sistemine de aktarılmaktadır.
( ) Kullanıcının üyelik formlarını doldurduğu bir zamanda alınmaktadır.
( ) Diğer:……

9. Kişisel Verilerin Korunması Kanunu kapsamında kütüphanenizde veri sorumlusu bulunmakta mıdır?

( ) Evet
( ) Hayır (Nedenini belirtiniz: ……..)

10. Kütüphanenizde tutulan kişisel verilerin sınıflanmasına yönelik bir düzenlemeniz var mı? (Cevabınız evet ise, onbirinci soruya geçiniz.)
( ) Evet
( ) Hayır

11. Sınıflamanızı hangi özelliklere bağlı kalarak yapıyorsunuz?
(Birden fazla seçeneği işaretleyebilirsiniz.)
( ) Kullanıcı grubuna göre bir düzenleme yapılıyor (öğrenci, akademisyen, idari personel gibi)
( ) Gizlilik derecelerine göre (çok gizli, gizli, özel, hizmete özel, tasnif dışı)
( ) Bilginin karakteristik özelliklerine göre (gizlilik, bütünlük, kullanılabilirlik)
( ) İşlem öncelik sıralarına göre
( ) Güvenlik hassasiyet düzeyine göre (kamuya açık, kaybolduğunda kişiler ya da kurumlar için zararlı olabilecek, kesinlikle erişime açılmayacak veriler gibi)
( ) Tür ve özelliklerine göre (özel ve genel nitelikli veriler)
( ) Belge isimlerine, konuya ve kronolojik sıraya göre
( ) Standart dosya planına göre

12. Kullanıcılarınıza ilişkin kişisel veriler en çok hangi birimlerinizde işlenmektedir? (En çok işlenen beş birimi 1'den başlayarak sıralayınız.)
( ) Basılı Süreli Yayınlar Birimi
( ) Elektronik Kaynaklar Birimi
( ) Enformasyon Teknolojileri Birimi
( ) Kalite Yönetim Birimi
( ) Kurumsal İletişim Birimi
( ) Ödünç Verme Birimi
( ) Raf Hizmetleri Birimi
( ) Referans Birimi
( ) Sağlama ve Kataloglama Birimi
( ) Satın Alma ve Muhasebe Birimi
( ) Taşınır Kayıt Birimi
( ) Açık Erişim ve Kurumsal Arşiv Birimi
( ) Diğer

13. Kütüphanenizde tutulan kişisel verileri hangi amaçlarla kullanıyorsunuz? (Birden çok işaretleme yapabilirsiniz.)
( ) Hizmet sunumu
( ) Hizmet geliştirme
( ) Kütüphane güvenliğini sağlama
( ) Koleksiyon güvenliğini sağlama
( ) Raporlama/kullanım istatistiği alma (etki değerlendirme)

14. Kütüphanenizde kullanıcılara ve personele ait kişisel veriler nerede tutulmaktadır? (Birden çok işaretleme yapabilirsiniz.)
( ) Hizmet aldığımız firmanın/şirketin sunucularında
( ) Kütüphanenin kendi sunucularında
( ) Üniversitenin merkezi sunucularında
( ) Taşınabilir medyada

( ) Şifreli/korumalı dolaplarda
( ) Şifresiz/korumasız klasör ya da dolaplarda
( ) Diğer……

15. Kullanıcılara/personele ait kişisel verilerin hangi gerekçe ile kullanılmasına ve paylaşılmasına izin verilmektedir? (Birden çok işaretleme yapabilirsiniz.)
( ) Yasal çerçevede savcılık tarafından istenmesi durumunda
( ) Bilgi edinme hakkı kanunu çerçevesinde
( ) İstatistik amaçlı olarak istenmesi halinde
( ) Bilimsel araştırmada kullanılmak şartıyla
( ) Üniversite üst yönetimi ya da güvenlikten sorumlu birimler tarafından istenmesi halinde
( ) Kamu menfaati için gerekli olması halinde (kişisel haklar gözetilmeksizin)
( ) Veri sahibinin kendisi hakkında tutulan bilgileri istemesi halinde
( ) Kullanıcı/personel bilgileri hangi sebeple olursa olsun verilmez.
( ) Diğer……

16. Kütüphanenize diğer üniversite birimlerinden kişisel veriler nasıl aktarılıyor?
( ) Kullandığımız bütün sistemler birbirine entegre bir şekilde çalıştığından kişisel veriler otomatik olarak Personel Dairesi Başkanlığı, Bilgi İşlem Dairesi Başkanlığı, Öğrenci İşleri Dairesi başkanlığı gibi birimlerden aktarılmaktadır.
( ) Yetkili kişilerin ya da bilgi işlem uzmanlarının çalışmalarıyla
( ) Diğer……

17. Kütüphanenize üniversitenin diğer birimlerinden kişisel veri aktardığınız üç birimi öncelik sırasına göre belirtiniz.(1 en çok kişisel veri aktarımında iletişimde bulunulan birim olmak üzere):

1-)……
2-)……
3-)……

18. Üçüncü parti kuruluşlar(gerçek/tüzel) kütüphanenizde tutulan hangi sistemlerdeki kişisel verilere ulaşabiliyor? (Birden çok işaretleme yapabilirsiniz.)
( ) Kapı (giriş-çıkış) turnike sistemleri
( ) Kütüphane otomasyon sistemi
( ) Kütüphane kurumsal arşiv sistemi
( ) Kütüphanenin abone olduğu veri tabanı sistemleri
( ) Üçüncü parti kuruluşlarla kişisel veri paylaşmıyoruz

19. Kütüphanenizde tutulan kişisel verilerin kullanımına yönelik olarak kullanıcılardan bir onay alıyor musunuz? (Cevabınız evet ise, yirminci soruya geçiniz.)
( ) Evet
( ) Hayır

20. Aydınlatma metninin içeriği aşağıdakilerden hangilerini kapsamaktadır? (Birden fazla seçeneği işaretleyebilirsiniz.)
( ) Bir bilgilendirme yapılmamaktadır.
( ) Kişisel verilerin tutulma amacını kapsamaktadır.
( ) Hangi kişisel verilerin farklı amaçlarla kullanılabileceği bilgisini kapsamaktadır.
( ) Kişisel verilerin saklanma süresini kapsamaktadır.
( ) Kişisel verilerin silinmesine yönelik bilgileri kapsamaktadır.
( ) Kişisel verilerin yeniden kullanımına yönelik bilgileri kapsamaktadır.
( ) Diğer……

21. Kütüphaneniz üçüncü parti kuruluşlarla yaptığı anlaşmalarda kullanım anlaşmalarında kişisel verilerin korunmasına yönelik gizlilik sözleşmesi var mıdır?
( ) Evet
( ) Kısmen
( ) Hayır

22. Kişisel verilerin kaldırılması(silme/yok etme/anonimleştirme) aşamasında hangi işlemleri uygulamaktasınız?
( ) Silme/Yok etme/Anonimleştirme
( ) Hiçbiri
( ) Diğer …….

23. Kütüphanenizde tutulan kişisel verilerin saklanma sürelerine yönelik bir uygulamanız var mı?
( ) Var
( ) Geliştirme aşamasında
( ) Yok

24. Kütüphanenizde kişisel veri koleksiyonunuz (ayrı sistem/tek sistem) var mı?
( ) Evet
( ) Hayır

25. Şu anda aktif olmayan ancak sistemlerinizde tutulan kişisel verilere tekrar ihtiyacınızolacağını düşünüyor musunuz?
(Cevabınız evet ise, kısaca nedenini açıklayabilir misiniz?)
( ) Evet ……....
( ) Hayır

26. Kütüphanenizde kişisel verilerin yönetilmesini içeren sizin (kütüphane yöneticisi) ya da üst yönetimin imzaladığı, belirli zaman aralıklarında güncellenen bir politikanız var mı?
( ) Evet ( ) Hayır

27. Kütüphanenizde kişisel verilerin yönetilmesini içeren sizin (kütüphane yöneticisi) yada üst yönetimin imzaladığı politikaya ne düzeyde ihtiyaç duyuyorsunuz?

( ) Fikrim yok
( ) Hiç ihtiyaç duymuyoruz
( )İhtiyaç duymuyoruz
( ) İhtiyaç duyuyoruz
( ) Çok ihtiyaç duyuyoruz

28. Kütüphanenizde kişisel veri ya da bilgi güvenliği ile ilgili bir sorunla karşılaştığınızda başvuracağınız kaynaklardan ilk beşini işaretleyiniz.

( ) Etik ilkeler
( ) Uluslararası bilgi güvenliği standartları
( ) Uluslararası sözleşmeler ve düzenlemeler
( ) Veri koruma direktifleri
( ) Politikalar
( ) Rehberler
( ) Kılavuzlar
( ) Bilimsel çalışmalar
( ) Hukuk müşavirliği
( ) Üniversitenin etik kurul komisyonları
( ) Kişisel Verileri Koruma Kurumu
( ) Diğer (Lütfen belirtiniz……)

29. Kişisel Verileri Koruma Kanunu kapsamında kütüphanenizde bir uygulamanız oldumu?

……
…….....
……

Bölüm III – Bilgi Güvenliği

Aşağıda üniversite kütüphanelerinde bilgi güvenliği uygulamalarını (kurumsal, bina, koleksiyon vb.) tespit etmek amacıyla sorular yer almaktadır.

30. Kurumsal Güvenlik				
Güvenlik Ölçümleri	**Evet**	**Hayır**	**Geliştirilme Aşamasında**	**Açıklama**
30.1.Üst yönetim tarafından onaylanmış bilgi güvenliği politika belgesi var mı?	( )	( )	( )	
30.2.Kütüphanenizde ISO standartlarına uygun olarak kalite yönetim sistemi ve/veya bilgi güvenliği yönetim sistemi bulunmakta mıdır?	( )	( )	( )	
30.3.Kütüphanenizdeki bilgi güvenliği politikasında kişisel verilerin korunması ile bilgi güvenliği birlikte ele alınıyor mu?	( )	( )	( )	
30.4. Bilgi güvenliği denetlemeleri kütüphane içerisinden bir personel tarafından mı yapılmaktadır?	( )	( )	( )	
30.5. Kütüphaneye yeni bir sistem alınırken güvenliği denetleniyor mu?	( )	( )	( )	
30.6. Kütüphanenizde bilgi güvenliği risk analizi yapılmakta mıdır?	( )	( )	( )	
30.7. Kütüphanenizde özel hayatın gizliliğine yer veren etik ilkeler var mı?	( )	( )	( )	

31.Bina Güvenliği				
Güvenlik Ölçümleri	**Evet**	**Hayır**	**Geliştirilme Aşamasında**	**Açıklama**
31.1. Kütüphanenizde bina güvenliğine yönelik bir politikanız var mı?	( )	( )	( )	
31.2. Kütüphanenizin binası kütüphane binası olarak mı tasarlandı?	( )	( )	( )	
31.3. Kütüphanenizde iç hava kalitesi ölçümleri yapılıyor mu?	( )	( )	( )	
31.4. Kütüphanenizde nem ölçümleri yapılıyor mu?	( )	( )	( )	
31.5. Kütüphanenizde gürültü ölçümleri yapılıyor mu?	( )	( )	( )	
31.6. Kütüphane binasında ışıklandırma yeterli mi?	( )	( )	( )	
31.7. Deprem, sel vb. afetler için erken uyarı sistemleriniz var mı?	( )	( )	( )	
31.8. Doğal afetlere karşı önlem ve tedbirlerinizi aldınız mı?	( )	( )	( )	
31.9. Kütüphanemizin tüm birimlerinde (Süreli Yayınlar, Arşiv vb.) insan ve koleksiyon güvenliğini sağlamak amacıyla tedbirler alındı mı?	( )	( )	( )	
31.10. Acil durumlara karşı levhalar ve tabelalar, yönlendirmeler var mı?	( )	( )	( )	
31.11. Bilgi güvenliği politikası içerisinde bina güvenliğine yer verildi mi?	( )	( )	( )	
31.12. Kütüphanenizin binası (iç-dış) bir denetleyici tarafından denetleniyor mu?	( )	( )	( )	
31.13. Kütüphanenizde bina otomasyon sistemleri (ısıtma- soğutma ve havalandırma, aydınlatma, yangın algılama ve alarm sistemleri) var mı?	( )	( )	( )	
31.14. Gerektiğinde emniyet, itfaiye vb. kuruluşlarla kimin ne zaman iletişim kurulacağının ve olayın nasıl rapor edileceğini tarif eden bir prosedür mevcut mu?	( )	( )	( )	

32.Koleksiyon Güvenliği				
Güvenlik Ölçümleri	**Evet**	**Hayır**	**Geliştirilme Aşamasında**	**Açıklama**
32.1. Kütüphanenizde kütüphane koleksiyon güvenliğine yönelik yazılı bir politikanız var mı?	( )	( )	( )	
32.2. Koleksiyon güvenliği politikaları ve prosedürleri düzenli olarak gözden geçirilip güncelleniyor mu?	( )	( )	( )	
32.3. Kütüphanedeki çeşitli koleksiyonlara yönelik riskleri (küflenme, yıpranma, hasar görme vb.) tanımlanıyor mu?	( )	( )	( )	
32.4. Acil durumlar ve güvenlik ihlali için uygun ve test edilmiş prosedürler bulunmakta mıdır?	( )	( )	( )	
32.5. Kayıp, hasar görmüş, yıpranmış koleksiyonlar için yedekleme politikanız var mı?	( )	( )	( )	
32.6. Kütüphane tarafından edinilen tüm materyaller kayıt altına alınıyor ve numaralandırılıyor mu?	( )	( )	( )	
32.7. Tüm koleksiyonlar manyetik şeritlerle işaretlendi mi?	( )	( )	( )	
32.8. Güvenlik sistemleri izinsiz ve yetkisiz girişleri engellemek için kütüphanenin giriş, çıkış ve depo alanlarına yerleştirildi mi ? (elektronik anti hırsızlık sistemi, görsel kameralar, duman algılama sistemi, CCTV, manyetik algılama sistemi)	( )	( )	( )	
32.9. Genel ve özel koleksiyon alanlarına girişlere yönelik bir denetim uygulamanız var mı?	( )	( )	( )	
32.10. Koleksiyonları korumak için kütüphanelerde önleyici tedbirler alınıyor mu?	( )	( )	( )	
32.11. Rafların düzeni ve boyutları, oturma ve okuma alanlarının düzeni, yangın önleme ekipmanlarının yerleştirilmesi gibi işlemler TSE standartlarına uygun olarak yapıldı mı?	( )	( )	( )	

33.Personel ve Kullanıcı Güvenliği				
Güvenlik Ölçümleri	**Evet**	**Hayır**	**Geliştirilme Aşamasında**	**Açıklama**
33.1. Kütüphanenizde personel ve kullanıcı güvenliğine yönelik yazılı bir politikanız var mı?	( )	( )	( )	
33.2. Kütüphanenize personel alımı yapılmadan önce güvenlik soruşturması yapılıyor mu?	( )	( )	( )	
33.3. Kütüphanenizde yapılacak iş ve işlemler için hassas görevler listesi yapıldı mı?	( )	( )	( )	
33.4. Kütüphanenizde personelin güvenliğini sağlamak için tedbirler alındı mı?	( )	( )	( )	
33.5. Kütüphanenizdeki personelin kişisel eşyaları için kişisel dolaplar/alanlar var mı?	( )	( )	( )	
33.6. Kullanıcılar kütüphanenin ortak kullanım alanlarında kişisel eşyalarının güvenliği ile ilgili olarak işaret ve levhalarla bilgilendiriliyor mu?	( )	( )	( )	
33.7. Kullanıcı şifrelerinin belirlenmesi ve kullanılması ile ilgili güvenlik tedbirleri uygulanıyor mu?	( )	( )	( )	
33.8. Kütüphanenizde her bir kullanıcının görev listesinde (tanımlarında) kullanıcı verilerinin güvenliği ve korunması konularına yer verildi mi?	( )	( )	( )	

34.Yazılım ve Donanım Güvenliği				
Güvenlik Ölçümleri	**Evet**	**Hayır**	**Geliştirilme Aşamasında**	**Açıklama**
34.1. Kütüphanenizde yazılım ve donanım güvenliği konusunda politika var mı?	( )	( )	( )	
34.2. Kütüphanenizde ortak kullanım alanlarında bulunan teknoloji varlıklarını (masa üstü bilgisayar, taşınabilir bilgisayar, tablet, sunucular, projeksiyon, fotokopi, tarayıcı gibi) güvenliği tam olarak sağlanabiliyor mu?	( )	( )	( )	
34.3. Kullanıcı ve personele ait hassas verilerin doğruluğunun ve güvenilirliğinin sağlanması için doğrulama araçları[18] kullanılıyor mu?	( )	( )	( )	
34.4. Sistem açma/kapama, yedekleme, teknolojik varlıkların bakımı ve bilgisayar odasının kullanılması gibi sistem faaliyetleri için bir prosedürünüz var mı?	( )	( )	( )	
34.5. Kütüphanenizdeki bilgisayarların yazılım ve donanım güvenliği sağlanıyor mu?	( )	( )	( )	
34.6. Kullanıcıların kütüphane içerisinden internet erişiminde kullanıcı adı ve şifre isteniyor mu?	( )	( )	( )	

[18] Doğrulama araçları, veri ve bilgilerin doğruluğunu, gizliliğini sağlamak amacıyla kullanılan araçlardır. Bu soruda ise, kimlik doğrulama(authentication) anlamında kullanılmıştır. Kimlik doğrulama ise, bir kullanıcının veya programın bir sisteme erişirken kim olduğunu kanıtlama işlemidir.

34. Yazılım ve Donanım Güvenliği				
34.7. Kullanıcıların ortak kullanım alanlarındaki bilgisayarlara yazılım yüklemelerine yönelik bir güvenlik uygulamanız var mı?	( )	( )	( )	
34.8. Ortak kullanım alanlarındaki bilgisayarlardaki kullanıcı faaliyetleri merkezi bir noktadan izleniyor mu?	( )	( )	( )	
34.9. Kütüphaneniz bilgi veya bilgi işlem araçları ile ilgili olarak temiz ekran masa politikası[19] uyguluyor mu?	( )	( )	( )	
34.10. Kullanıcıların ve personelin güvenliğini sağlamak amacıyla kötü amaçlar için kullanılan sitelere güvenlik duvarı kısıtlamaları getirildi mi?	( )	( )	( )	
34.11. Satın alınan ürünler (elektronik araç ve gereç, bilgi sistemi, vb.) için herhangi bir denetleme yapılıyor mu?	( )	( )	( )	
34.12. Kütüphanenizde siber saldırılara yönelik (anti-virüs, şifreleme, yedekleme) önlemler alındı mı?	( )	( )	( )	

[19] Bilgiye yetkisiz erişim, bilgi kaybı ve hasarı, risklerini azaltmak amacıyla; kâğıtlar, taşınabilir depolama ortamları ve kişisel bilgisayarların güvenliği için gerekli şartları tanımlayan politika.

35. Aşağıdaki konularda kütüphanenizde gerçekleştirdiğiniz güvenlik uygulamalarını ne derece yeterli bulduğunuzu ve gelecek beş yılın sonunda bu uygulamalarınızın yeterlilik durumunun ne düzeyde olacağını değerlendiriniz. (1 çok yetersiz, 5 çok yeterli olmak üzere değerlendiriniz.)

Uygulamalar	Mevcut uygulamalarınıza yönelik değerlendirmeniz					Gelecek beş yıla yönelik değerlendirmeniz				
	1	2	3	4	5	1	2	3	4	5
Genel kurumsal güvenlik uygulamalarınız	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )
Bina güvenliği uygulamalarınız	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )
Koleksiyon güvenliği uygulamalarınız	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )
Personel ve kullanıcı güvenliği uygulamalarınız	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )
Donanım ve yazılım güvenliği uygulamalarınız	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )
Kişisel verilerin güvenliğine yönelik uygulamalarınız	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )

Yanıtlarınız için teşekkür ederim.

EK-2: ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLERİN KORUNMASI : ANKARA'DAKİ ÜNİVERSİTE KÜTÜPHANELERİNİN DEĞERLENDİRİLMESİ ARACI

Değerli Katılımcı,

Bu çalışma, Ankara'da bulunan üniversite kütüphanelerinin kişisel verilerin yönetilmesi ve bilgi güvenliği konusunda personellerin bilinç ve farkındalıklarını belirlemek amacıyla uygulanmaktadır. Anket sonucunda elde edilecek veriler, üniversite kütüphanelerinde kişisel verilerin yönetimi ve bilgi güvenliğine yönelik mevcut durumun ve karşılaşılan sorunların tespiti için kullanılacaktır.

Anketin uygulanması için gerekli etik kurul izni alınmıştır. Elde edilecek veriler kişisel değerlendirmeye tabi tutulmayacak, sadece bilimsel amaçla kullanılacak olup, değerlendirmelerde kurum adı ya da kurum adını gösterecek tanımlamalara kesinlikle yer verilmeyecektir. Ankete adınızı yazmanıza gerek yoktur. Görüşme formuna sağlayacağınız katkılar tamamen gönüllülük esasına dayanmaktadır. Anketin uygulanması 5 dakikadan fazla zamanınızı almayacaktır. Bu ankete vereceğiniz samimi yanıtlar araştırmanın başarısına önemli ölçüde katkı sağlayacaktır.

Anketten elde edilecek veriler Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı'nda Dr. Öğr. Üyesi Tolga Çakmak danışmanlığında yürütmekte olduğum yüksek lisans tezinde kullanılacaktır. Çalışma ile ilgili ayrıntılı bilgi almak ve çalışma hakkındaki sorularınız için dilansiskin@hacettepe.edu.tr adresinden iletişime geçebilirsiniz. Araştırmaya katılımınız ve değerli görüşleriniz için şimdiden teşekkür ederim.

Dilan Şerife ŞİŞKİN
Hacettepe Üniversitesi
Sosyal Bilimler Enstitüsü
Bilgi ve Belge Yönetimi Anabilim Dalı
Yüksek Lisans Öğrencisi

Bölüm I - Demografik sorular

1. Yaşınız?

……..

2. Eğitim Düzeyiniz?

( ) Ortaokul
( ) Lise
( )Önlisans
( ) Lisans
( ) Yüksek Lisans
( ) Doktora

3. Göreviniz?

( ) İdari Hizmetler
( ) Teknik Personel
( ) Uzman Kütüphaneci
( ) Kütüphaneci
( ) Yönetici
( ) Diğer……

4. Kurumdaki çalışma süreniz?

…….....

5. Lisans eğitiminizi Bilgi ve Belge Yönetimi (Kütüphanecilik, Dokümantasyon veya Arşivcilik anabilim dallarından birinde) bölümünde mi tamamladınız? (Eğer, lisansüstü/doktora eğitiminizi Bilgi ve Belge Yönetimi Bölümünde aldıysanız, lütfen diğer seçeneğinde belirtiniz.)

( ) Evet
( ) Hayır
( ) Diğer……

Bölüm II - Bilgi güvenliği koşullarına yönelik sorular

6. Kişisel verilerin korunması hakkındaki bilgi düzeyiniz?
( ) Kavram hakkında bilgim yok.
( ) Kavram hakkında kısmen bilgi sahibiyim.
( ) Kavram hakkında bilgi sahibiyim.
( ) Kavram hakkında bilgi sahibiyim ve çalıştığım kurumda nasıl uygulanacağına yönelik bilgi sahibiyim.

7. Kütüphanenizde kişisel verilerin korunmasına yönelik olarak gerçekleştirilen uygulamaları değerlendiriniz.

1 Çok yetersiz 2 3 4 5 Çok yeterli

8. Kütüphanedeki iş süreçleriniz/tanımınız kişisel verilerden yararlanmayı ya da kütüphanede tutulan bu verileri içeren sistemlere erişmeyi gerektiriyor mu?

( ) Evet
( ) Zaman zaman
( ) Hayır

9. Kütüphaneye ait sistemlerdeki personele ya da kullanıcılara ait kişisel verilere (Örneğin OPAC üzerinde bir bilgi kaynağını kimin ödünç aldığını görme, kütüphaneye kimlerin giriş-çıkış yaptığını görme gibi) erişim yetkiniz var mı?
( ) Evet, kütüphanemizde tüm sistemlerdeki - personel ve kullanıcı dahil- kişisel verilere erişebilirim.
( ) Evet, kütüphanemizde yalnızca kullanıcılarla ilgili tüm sistemlerdeki kişisel verilere erişebilirim.
( ) Evet, kütüphanemizde yalnızca personelle ilgili tüm sistemlerdeki kişisel verilere erişebilirim.
( ) Tüm sistemlere değil ancak yetkim dahilinde bulunan sistemlerdeki kişisel verilere erişebilirim.
( ) Hayır, çalıştığım pozisyon doğrultusunda herhangi bir kişisel veriye erişimim bulunmamaktadır.
( ) Diğer:.....

10. Kütüphanenizdeki kullanım alanlarını ve unsurlarının (bina, koleksiyon, insan, donanım ve yazılım gibi) genel güvenlik düzeyini değerlendiriniz.

1 Çok yetersiz 2 3 4 5 Çok yeterli

11. Kütüphane binanızın yeterlilik düzeyini güvenlik koşulları (ısı, nem, ışık, gürültü, doğal afetler ve hırsızlık gibi) açısından değerlendiriniz.

1 Çok yetersiz 2 3 4 5 Çok yeterli

12. Kütüphane koleksiyonunuzun yeterlilik düzeyini güvenlik koşulları (saklama koşulları, tahribat, doğal afetler ve hırsızlık gibi) açısından değerlendiriniz.

1 Çok yetersiz 2 3 4 5 Çok yeterli

13. Kütüphanenizde kullanıcı erişimine sunulan donanımların (bilgisayar, klavye, mouse gibi birimlerin) yeterlilik düzeyini sağlanan güvenlik koşulları açısından değerlendiriniz.

1 Çok yetersiz 2 3 4 5 Çok yeterli

14. Kütüphanenizde kişisel verilerin korunmasına yönelik olarak gerçekleştirilen uygulamaların yeterlilik düzeyini değerlendiriniz.

1 Çok yetersiz 2 3 4 5 Çok yeterli

15. Kütüphanenizde kişisel verilerin korunmasına yönelik olarak politikaların yeterlilik düzeyini değerlendiriniz.

0 Politika belgemiz yok

1 Çok yetersiz 2 3 4 5 Çok yeterli

16. Kütüphanenizde bilgi güvenliği uygulamalarına yönelik olarak politikaların yeterlilik düzeyini değerlendiriniz.

0 Politika belgemiz yok

1 Çok yetersiz 2 3 4 5 Çok yeterli

17. Aşağıdaki konularda kütüphanenizde gerçekleştirdiğiniz güvenlik uygulamalarınızın gelecek beş yılın sonundaki yeterlilik durumunun ne düzeyde olacağını öngörüyorsunuz? (1 çok yetersiz, 5 çok yeterli olmak üzere değerlendiriniz.)

Uygulamalar	Gelecek beş yıla yönelik değerlendirmeniz				
	1	2	3	4	5
Genel kurumsal güvenlik uygulamalarınız	( )	( )	( )	( )	( )
Bina güvenliği uygulamalarınız	( )	( )	( )	( )	( )
Koleksiyon güvenliği uygulamalarınız	( )	( )	( )	( )	( )
Kullanıcı güvenliği uygulamalarınız	( )	( )	( )	( )	( )
Donanım ve yazılım güvenliği uygulamalarınız	( )	( )	( )	( )	( )
Kişisel verilerin güvenliğine yönelik uygulamalarınız	( )	( )	( )	( )	( )
Kişisel verilerin korunmasına yönelik politikalar	( )	( )	( )	( )	( )
Bilgi güvenliğine yönelik politikalar	( )	( )	( )	( )	( )

Yanıtlarınız için teşekkür ederim.

EK-3: ETİK KURUL İZNİ

Tarih: 01.07.2019 17:34
Sayı: 35853172-300-E.00000655288

E.00000655288

T.C.
HACETTEPE ÜNİVERSİTESİ
Rektörlük

Sayı : 35853172-300
Konu : Dilan Şerife ŞİŞKİN (Etik Komisyon İzni)

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Enstitünüz Bilgi ve Belge Yönetimi Anabilim Dalı Yüksek Lisans programı öğrencilerinden **Dilan Şerife ŞİŞKİN**'in **Dr. Öğr. Üyesi Tolga ÇAKMAK** danışmanlığında hazırladığı **"Üniversite Kütüphanelerinde Bilgi Güvenliği Risk Değerlendirmesi: Ankara'daki Üniversite Kütüphanelerinin Analizi"** başlıklı tez çalışması Üniversitemiz Senatosu Etik Komisyonunun **25 Haziran 2019** tarihinde yapmış olduğu toplantıda incelenmiş olup, etik açıdan uygun bulunmuştur.

Bilgilerinizi ve gereğini saygılarımla rica ederim.

e-imzalıdır
Prof. Dr. Rahime Meral NOHUTCU
Rektör Yardımcısı

Hacettepe Üniversitesi Rektörlük 06100 Sıhhiye-Ankara
Telefon:0 (312) 305 3001-3002 Faks:0 (312) 311 9992 E-posta:yazimd@hacettepe.edu.tr İnternet
Adresi: www.hacettepe.edu.tr

Sevda TOPAT

EK -4 : ORİJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 29/02/2020

Tez Başlığı: ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLERİN KORUNMASI: ANKARA'DAKİ ÜNİVERSİTE KÜTÜPHANELERİNİN DEĞERLENDİRİLMESİ
Yukarıda başlığı gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 125 sayfalık kısmına ilişkin, 29/02/2020 tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda işaretlenmiş filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 10'dur.

Uygulanan filtrelemeler:
1- ☒ Kabul/Onay ve Bildirim sayfaları hariç
2- ☒ Kaynakça hariç
3- ☐ Alıntılar hariç
4- ☒ Alıntılar dâhil
5- ☒ 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Dilan
29.02.2020

Adı Soyadı: DİLAN ŞERİFE ŞİŞKİN
Öğrenci No: N16222934
Anabilim Dalı: BİLGİ VE BELGE YÖNETİMİ
Programı: BİLGİ VE BELGE YÖNETİMİ

DANIŞMAN ONAYI

UYGUNDUR

T. Çakmak

Dr. Öğr. Üyesi Tolga ÇAKMAK

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
MASTER'S THESIS ORIGINALITY REPORT

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF INFORMATION MANAGEMENT

Date: 29/02/2020

Thesis Title: INFORMATION SECURITY AND PROTECTION OF PERSONAL DATA IN UNIVERSITY LIBRARIES: EVALUATION OF UNIVERSITY LIBRARIES IN ANKARA

According to the originality report obtained by myself/my thesis advisor by using the Turnitin plagiarism detection software and by applying the filtering options checked below on 29/02/2020 for the total of 125 pages including the a) Title Page, b) Introduction, c) Main Chapters, and d) Conclusion sections of my thesis entitled as above, the similarity index of my thesis is 10%.

Filtering options applied:

1. ☒ Approval and Decleration sections excluded
2. ☒ Bibliography/Works Cited excluded
3. ☐ Quotes excluded
4. ☒ Quotes included
5. ☒ Match size up to 5 words excluded

I declare that I have carefully read Hacettepe University Graduate School of Social Sciences Guidelines for Obtaining and Using Thesis Originality Reports; that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

I respectfully submit this for approval.

29.02.2020

Name Surname:	DİLAN ŞERİFE ŞİŞKİN
Student No:	N16222934
Department:	INFORMATION MANAGEMENT
Program:	INFORMATION MANAGEMENT

ADVISOR APPROVAL

APPROVED

Assist. Prof. Tolga ÇAKMAK