Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü
Bilgi ve Belge Yönetimi Anabilim Dalı

HASSAS BİLGİ VARLIKLARININ VE KİŞİSEL VERİLERİN HUKUKSAL DÜZENLEMELER İLE KORUNMASI VE BU KAPSAMDA ÜNİVERSİTELER İÇİN BİLGİ GÜVENLİĞİ POLİTİKASININ GELİŞTİRİLMESİ

Türkay HENKOĞLU

Doktora Tezi

Ankara, 2015

HASSAS BİLGİ VARLIKLARININ VE KİŞİSEL VERİLERİN HUKUKSAL DÜZENLEMELER İLE KORUNMASI VE BU KAPSAMDA ÜNİVERSİTELER İÇİN BİLGİ GÜVENLİĞİ POLİTİKASININ GELİŞTİRİLMESİ

Türkay HENKOĞLU

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü
Bilgi ve Belge Yönetimi Anabilim Dalı

Doktora Tezi

Ankara, 2015

KABUL VE ONAY

Türkay Henkoğlu tarafından hazırlanan "Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler İle Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi" başlıklı bu çalışma, 9 Ocak 2015 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Doktora Tezi olarak kabul edilmiştir.

Prof. Dr. Bülent YILMAZ (Başkan)

Prof. Dr. Nazan ÖZENÇ UÇAK (Danışman)

Prof. Dr. Fahrettin ÖZDEMİRCİ

Doç. Dr. Özgür KÜLCÜ

Yrd. Doç. Dr. Muammer KETİZMEN

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Prof. Dr. Yusuf ÇELİK

Enstitü Müdürü

BİLDİRİM

Hazırladığım tezin/raporun tamamen kendi çalışmam olduğunu ve her alıntıya kaynak gösterdiğimi taahhüt eder, tezimin/raporumun kâğıt ve elektronik kopyalarının Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü arşivlerinde aşağıda belirttiğim koşullarda saklanmasına izin verdiğimi onaylarım:

☐ Tezimin/Raporumun tamamı her yerden erişime açılabilir.

☐ Tezim/Raporum sadece Hacettepe Üniversitesi yerleşkelerinden erişime açılabilir.

☑ Tezimin/Raporumun 1 yıl süreyle erişime açılmasını istemiyorum. Bu sürenin sonunda uzatma için başvuruda bulunmadığım takdirde, tezimin/raporumun tamamı her yerden erişime açılabilir.

09.01.2015

_____

Türkay HENKOĞLU

TEŞEKKÜR

Bu çalışmanın öneri aşamasından savunma aşamasına kadar olan tüm süreci büyük bir özveri ile takip eden, çalışma notlarını sabırla ve aynı zamanda itinayla okuyarak değerlendiren, araştırmanın zor aşamalarında bilgi ve tecrübesiyle her an desteğini ve yardımını yanımda hissettiğim değerli hocam ve danışmanım Prof. Dr. Nazan Özenç Uçak'a ne kadar teşekkür etsem azdır.

Tez önerisi ve tez izleme sınavlarında görüş, öneri ve eleştirileri ile bu çalışmanın daha üst seviyede olmasına katkı sağlayan değerli hocalarım Prof. Dr. Fahrettin Özdemirci ve Yrd. Doç. Dr. Muammer Ketizmen'e ve jüri üyesi olarak sağladıkları önemli katkılardan dolayı Prof. Dr. Bülent Yılmaz ve Doç. Dr. Özgür Külcü'ye,

Gizlilik bildirimi nedeniyle isimlerini sayamadığım; uygulamalar hakkındaki eksiklikleri, düşüncelerini ve önerilerini tüm samimiyeti ile ifade ederek çalışmaya katkı sağlayan araştırma kapsamında yer alan 15 üniversitenin kütüphane ve dokümantasyon, bilgi işlem ve personel daire başkanlarına,

Hayatımın her döneminde vermiş olduğu destek için annem, babam, ablam ve çalışmanın en başından itibaren göstermiş olduğu sabır ve desteği için sevgili eşim Halise Henkoğlu'ya,

Ve son olarak; "2211-C Öncelikli Alanlara Yönelik Yurt İçi Doktora Burs Programı" kapsamında burs imkânı sağlayarak bu çalışmayı destekleyen TÜBİTAK'a teşekkürlerimi sunarım.

ÖZET

Henkoğlu, Türkay. *Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi,* Doktora Tezi, Ankara, 2015.

Güvenilir bilgiye erişim ve büyük ölçüde elektronik ortamda saklanan mevcut bilginin korunmasına yönelik ihtiyaçların arttığı günümüzde, korunacak bilgi varlıkları içinde kişisel veriler önemli bir yer tutmaktadır. Bu bilgi varlıklarının korunması ve risk yönetiminin yapılabilmesi; hukuksal, teknik ve idari boyutların dikkate alındığı bilgi güvenliği politikalarının gücü ile mümkün olabilmektedir. Üniversitelerde kişisel verilerin korunmasında ne kadar ihtiyatlı olunduğu, uygulanan güvenlik politikaları ve veri sahibinin temel hak ve özgürlüklerin nasıl korunduğu konusunda belirsizlikler bulunmaktadır.

Bu tez çalışmasıyla kişisel verilerin korunmasına ilişkin hususlar kapsamlı bir bilgi güvenliği modeli ve hukuksal koşullar çerçevesinde değerlendirilerek, üniversiteler için uygulanabilir bir bilgi güvenliği politikasının geliştirilmesi ve üniversitelerde bilgi güvenliği kültürünün oluşturulmasına katkı sağlanması amaçlanmıştır. Çalışmada Türk Hukuk Mevzuatında yer alan hassas bilgi varlıklarının korunması ile ilişkili düzenlemeler belirlenerek, Avrupa Birliği (AB) bilgi güvenliği politikaları kapsamında yapılan hukuksal düzenlemeler ve kuramsal bir bilgi güvenliği modeli çerçevesinde değerlendirilmiştir. Bununla beraber, Ankara'da bulunan 15 üniversitenin bilgi işlem daire başkanlığı (BİDB), personel daire başkanlığı (PDB) ve bilgi merkezlerini kapsayacak şekilde görüşme yoluyla anket uygulanmış ve alınan bilgi güvenliği önlemleri mevcut hukuksal düzenlemeler çerçevesinde değerlendirilmiştir.

Çalışma sonucunda; yasal düzenlemelerin yeterli ve önleyici nitelikte olmadığı, üniversitelerde kişisel verilerin korunmasına ve verilerin güvenli olarak imha edilmesine ilişkin politikaların bulunmadığı, mevcut politika ve kurallar içinde kişisel verilerin korunmasına ilişkin maddelere yer verilmediği, veri koruma konusunun sadece teknik boyutuyla değerlendirildiği ve risk yönetiminin yapılmadığı, üniversite

birimleri arasında sorumlulukların paylaşılmadığı, kişisel verileri işleyen personele veri korumaya ilişkin bilinçlendirme eğitimi verilmediği ve kişisel verileri işleyen birimlerin hangi verilerin kişisel veri olduğu konusunda dahi tereddütlerinin bulunduğu görülmektedir. Araştırma bulgularına bağlı olarak elde edilen bu sonuçlarla birlikte; kişisel verilerin korunmasına ilişkin hukuk literatürü, uluslararası bilgi güvenliği politikaları, bilgi güvenliği ve risk yönetimine yönelik uluslararası standartlar, kurumlara yönelik bilgi güvenliği denetleme raporları ve kişisel verilerin korunmasına ilişkin evrensel ilkelerden yararlanılarak üniversitelerin uygulayabileceği bir bilgi güvenliği politika önerisi geliştirilmiştir.

Anahtar Sözcükler

Bilgi güvenliği, kişisel veri, hassas veri, risk yönetimi, bilgi güvenliği politikası

ABSTRACT

Henkoğlu, Türkay. *The Protection of Personal Data and Sensitive Information Assets by Legal Regulations, and in This Context the Development of an Informatıon Security Policy for Universities,* Ph.D. Dissertation, Ankara, 2015.

Today, with the significant increase in the need for the access to reliable information and for the protection of available information stored electronically; personal data has become the one of the most important information assets that must be protected. The protection of these information assets and the implementing a risk management are only possible with the power of information security policies considering legal, technical, and administrative dimensions. There are some uncertainties about how universities are cautious in the protection of personal data, whether they implement a security policy, and how they protect the fundamental rights and freedoms of the data subject.

In this thesis study, it has been aimed to make an information security policy that can be applied in universities in order to protect personal data, and to contribute to the creation of information security culture by evaluating the matters relating to the protection of personal data within the framework of a comprehensive information security model and the legal conditions. In this study, upon determining the regulations related to the protection of sensitive information assets in the Turkish Law Legislation, these regulations have been evaluated within the scope of the legal regulations made under the European Union (EU) information security policies and in the framework of a theoretical information security model. In addition, by applying a questionnaire through interviews with the computer centers, the directorate of personnel affairs and the libraries of 15 universities in Ankara; the adequacy of the information security policies of universities has been examined and their compatibility with the existing legal regulations has been investigated.

The results of the study show that the legal regulations are not adequate and preventive in nature, the universities do not have any security polies concerning the protection and the safe destruction of personal data, existing policies and rules do not include any

articles concerning the protection of personal data, the issue of data protection is evaluated only within the scope of technical aspects and there is not any risk management, the responsibility is not shared within the units of universities, training for personal data protection awareness is not provided for the staff responsible for data processing, and the units responsible for the data processing have hesitation even in deciding whether data is personal or not. In addition to the results obtained based on the findings of the study, an information security policy that can be applied in universities in order to protect personal data has been developed within the framework of the legal literature related to the protection of personal information assets, international information security policies, international standards for information security and risk management, information security inspection reports for institution, and the universal principles relating to the protection of personal data.

Keywords

Information security, personal data, sensitive data, risk management, information security policy

İÇİNDEKİLER

KISALTMALAR LİSTESİ

AB	Avrupa Birliği
ABAD	Avrupa Birliği Adalet Divanı
ABD	Amerika Birleşik Devletleri
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AK	Avrupa Konseyi
APEC	Asia-Pacific Economic Cooperation
BEHK	Bilgi Edinme Hakkı Kanunu
BİDB	Bilgi İşlem Daire Başkanlığı
BSI	British Standards Instute
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CNSS	Committee on National Security Systems
COBIT	Control Objectives for Information and related Technology
DDK	Cumhurbaşkanlığı Devlet Denetleme Kurulu
EBYS	Elektronik belge yönetim sistemleri
EİK	Elektronik İmza Kanunu
ENISA	European Union Agency for Network and Information Security
FERPA	The Family Educational Rights and Privacy Act
FSEK	Fikir ve Sanat Eserleri Kanunu
GAISP	Generally Accepted Information Security Principles
GASSP	Generally Accepted System Security Principles
GMITS	The Guidelines for the Management of IT Security
IEC	International Electrotechnical Commission
IFS	Information Security Forum
ISO	International Organization for Standardization
KDB	Kütüphane Daire Başkanlığı (Üniversite Bilgi Merkezi)
KVKK	Kişisel Verileri Koruma Kanunu
KVKKT	Kişisel Verileri Koruma Kanun Tasarısı
NIST	National Institute of Standards and Technology
ODTÜ	Orta Doğu Teknik Üniversitesi
OECD	Organisation for Economic Co-operation and Development

PDB	Personel Daire Başkanlığı
SSE-CMM	System Security Engineering Capability Maturity Model
TCK	Türk Ceza Kanunu
TİB	Telekomünikasyon İletişim Başkanlığı
TKD	Türk Kütüphaneciler Derneği
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TTK	Türk Ticaret Kanunu
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
YÖK	Yükseköğretim Kurulu

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

1. BÖLÜM

GİRİŞ

Bilgi, içinde bulunduğumuz internet çağının en önemli unsurlarından biri durumundadır. Ancak kontrol edilemeyen bilginin de negatif güç olarak maddi ve manevi kayıplara neden olduğu her geçen gün daha iyi anlaşılmaktadır. Elektronik ortamda bulunan bilgi kaynaklarının artışı ile birlikte, güvenilir bilgiye erişim ve var olan bilginin korunması konularının önemi fark edilmiş ve bilgi güvenliğinin sağlanması, bilgi yönetim süreçlerinin ayrılmaz bir parçası haline gelmiştir. Bilgi güvenliği, fiziksel şartların sağlanmasından iletişim ortamının korunmasına kadar geniş bir alanın konusudur. Ancak bu geniş alanda değişmeyen unsur korunacak bilgi varlığıdır. Korunacak bilgi varlıkları içinde en önemli payı oluşturan ve son yıllarda üzerinde en fazla tartışılan kişisel verilerin korunması konusu, bu çalışmanın ana temasını oluşturmaktadır.

Kurumsal ve kişisel bilgilerin kaydedilmesi, dağıtılması, kullanılması, depolanması ve kullanım süresi sonunda imha edilmesi, günümüzde büyük ölçüde bilgi sistemleri kullanılarak gerçekleştirilmekte ya da bir kopyası elektronik veri depolama ortamına aktarılarak muhafaza edilmektedir. Ancak bilgi sistemleri ya da elektronik veri depolama ortamları üzerindeki bilgilerin korunması, yazılı ortamlarda yer alan bilgilerin korunmasından çok daha farklı ve daha fazla birimin sorumluluk alanını ilgilendiren yöntemlerin uygulanmasını gerektirmektedir. Bu nedenle, bilgi sistemleri altyapısının oluşturulması ile başlayan ve her geçen gün standartları artarak daha karmaşık ve maliyetli hale gelen bilgi güvenliğinin sağlanması sürecinin, bilgileri işleyen çalışanların sorumluluğunu da içerecek şekilde yönetilmesi sağlanmalıdır. Bu sürecin iyi yönetilebilmesi, küresel çaptaki gelişmelerin ve mevcut hukuksal düzenlemelerin de göz önüne alınarak hazırlandığı yazılı bilgi güvenliği politikalarının gücü ile mümkün olabilmektedir.

Hassas ve kişisel verilerin korunması, bilgi ve iletişim teknolojilerinin daha yaygın kullanımıyla ilişkili olarak her geçen gün zorlaşmaktadır. Bireylerin toplum içerisinde ayrımcılığa uğramasına ya da kişisel hak ve özgürlüğün ihlaline sebep olabilecek

bilgilerin yeterince korunamaması halinde; birkaç dakika içinde dünyanın hangi noktasında kullanılacağı ya da ne kadar sayıda kopyasının oluşacağını önceden kestirebilmek ya da sonrasında kontrol altında tutabilmek mümkün değildir. Bu yüzden alınacak olan koruma tedbirlerinin önleyici niteliği öne çıkmaktadır. Kişisel verilerin korunabilmesi için kullanılacak yöntemler, hukuksal düzenlemeler ve bilgi güvenliği kapsamında alınacak önlemlerle sınırlıdır. Ancak bu kapsamlı ve iki farklı alan içinde yer bulan veri korumanın en üst seviyede gerçekleştirilebilmesi, her iki alan içinde belirlenmiş olan ilkelerin birlikte uygulanması ile mümkün olabilmektedir. Bu nedenle geliştirilecek olan bilgi güvenliği politikalarında bu farklı disiplinlerin konuya yaklaşımı göz önünde bulundurularak mevcut risklerin mümkün olan en düşük seviyeye indirilmesi hedeflenmelidir.

Bilgi güvenliği politikalarının geliştirilmesinde dikkate alınması gereken en önemli hukuksal düzenlemeler veri koruma kanunlarıdır. Veri koruma kanunları, bilginin nasıl elde edileceği, işleneceği, saklama süresi ve nasıl imha edileceğine ilişkin olarak en kapsamlı kaynak ve aynı zamanda uygulanabilir hukuksal düzenlemelerdir. Ancak Türkiye'de henüz veri koruma kanununun olmaması, Türk Hukuk Mevzuatındaki diğer birçok düzenlemelerin içinde yer alan ilgili kısımların dikkate alınmasını gerektirmektedir. Bu işlemin zorluğu ve çoğu zaman ihmal edilmesi nedeniyle, hukuksal anlamda daha fazla ihlal gerçekleşmekte ve hukuksal düzenlemeleri dikkate alan bilgi güvenliği politikalarının geliştirilmesinde eksiklikler bulunmaktadır. Kişisel verilerin korunmasıyla sadece verinin gizliliğinin değil, kişisel hak ve özgürlüğün korunması da hedeflenmektedir. Hukuksal koşulların dikkate alınmadığı bilgi güvenliği politikalarının kişisel hak ve özgürlüğü korumadan yoksun olacağı açıktır.

Bilgi güvenliğinin sağlanması konusunda alınacak önlemlere yeni boyutlar eklenerek daha karmaşık hale gelmiş ve belirli bir uzmanlık alanının kontrol edebileceği sınırları aşmıştır. Veri korumaya ilişkin olarak sadece karakteristik özelliklerin dikkate alındığı geleneksel bakış açısı terk edilerek, bilginin durumunun ve bilgi güvenliği politikalarını da içeren kapsamlı güvenlik önlemlerinin alınması anlayışı benimsenmektedir. Bu yeni anlayış içerisinde bilgi güvenliği önlemlerinin hukuksal düzenlemeleri de dikkate alması,

bilinçliliğin arttırılması ve bilgi güvenliği politikaları kapsamında farkındalık eğitimlerinin düzenlenmesi gibi bir takım önleyici tedbirlerin alınması öngörülmektedir.

Hukuksal düzenlemeler ve geleneksel bilgi güvenliği önlemleri veri korumanın sağlanması konusunda tek başına yetersiz kalmaktadır. Bu nedenle, literatürde her iki yönteme ilişkin çözüm önerilerinde de diğer alanın göz ardı edilmemesi gerektiğinin altının çizildiği görülmektedir. Türkiye için örnek alınabilecek AB Veri Koruma Direktifi de, veri kayıplarına neden olan ya da veri bütünlüğünün bozulması amacıyla yapılan yetkisiz ve hukuk dışı erişimlere karşı teknik ve idari önlemlerin alınmasını öngörmektedir. Veri koruma direktifleri, teknolojik gelişmelerin ve maliyetlerin de göz önünde bulundurulduğu güvenlik önlemlerinin uygulanması ve bunun için gelişmelerin takip edilerek bilgi güvenliği politikalarının sürekli olarak güncellenmesini istemektedir (Johnston, 2011). Bu çerçevede hukuksal düzenlemeleri de dikkate alan kapsamlı bilgi güvenliği önlemlerinin alınabilmesi için, öncelikle bilgi varlıklarının değerlendirilerek risk yönetiminin uygulanması ve bir kurumsal bilgi güvenliği politikasının geliştirilmesi gerekmektedir. Bu çalışmada, diğer kurum ve kuruluşlar tarafından da temel olarak alınabilecek bir bilgi güvenliği politikasının, kişisel verilerin yoğun olarak işlendiği üniversiteler için geliştirilmesi hedeflenmiştir.

Bilgi teknolojilerindeki gelişmeler üniversitelerde daha fazla kişisel verinin işlenmesine ve bu bilgilerin daha fazla transfer edilmesine neden olmaktadır. Bilgi güvenliği ilkelerine bağlı kalındığı müddetçe kolaylıklar sağlayan bu gelişmeler, daha fazla riski de beraberinde getirmektedir. Üniversitelerde kayıt altına alınan bilgilerin güvenliğinin sağlanması birçok nedene bağlı olarak önemsenmektedir. Üniversitenin itibarının korunması, doğru ve güvenilir bilgi kaynaklarının kesintisiz olarak hizmete sunulması ve bilgi teknolojilerinin eğitim-öğretim içinde yaygın ve güvenli kullanımının sağlanması başlıca nedenler arasında yer almaktadır. Ancak çalışanlara, öğretim elemanlarına ve öğrencilere ait kişisel bilgilerin korunmasında ne kadar ihtiyatlı oldukları, hangi güvenlik politikalarını uyguladıkları, kişisel verilerin işlenmesinin disiplin altına alınıp alınmadığı ve temel hak ve özgürlüklerin nasıl korunduğu konusunda belirsizlikler bulunmaktadır.

Üniversiteler belirli bir amaca yönelik olarak elde edilen kişisel verilerin işlenmesi ve korunmasından sorumludurlar. Üniversitelerde kişisel verilerin korunabilmesi için, güvenlik ihlaline neden olabilecek girişimlerin engellenmesi, üniversitede bilgi güvenliği konusunun kimlerin sorumluluk alanına girdiğinin belirlenmesi, güçlü politika ve prosedürlerin geliştirilmesi ve güvenlik ihlâllerine karşı hazırlıklı olunması gerekmektedir. Böylece bilginin yanlış kullanımından, yönetiminden ya da ihmallerden kaynaklanan kayıplara karşı uygun güvenlik önlemlerinin alınması sağlanabilecektir. Bir üniversite için hangi ve ne kadar bilginin ihtiyaç olduğu, bu bilgilerin kim tarafından kullanılacağı ve kullanım süresinin ne zaman dolacağı hukuksal düzenlemeler çerçevesinde önceden belirlenmeli ve gerekli önlemler alınmalıdır.

1.1. KONUNUN ÖNEMİ

Bilgi sistemlerindeki gelişmelere bağlı olarak artan bilgi transferi, bilgi varlıkları içinde en fazla kişisel bilgilerin korunması konusundaki endişeleri arttırmıştır. Bulut bilişim ve e-ticaret ile birlikte, kişisel ve kurumsal bilgisayarlar internet hizmetleri üzerinde daha fazla kullanılmakta ve risk alanı genişlemektedir (Henkoğlu ve Külcü, 2013). Ancak bu verileri işleyen kurum, kuruluş ve şirketlere güç kazandıran kişisel bilgiler, yeni hukuksal ve etik sorumlulukları da beraberinde getirmektedir. Bu durum, siber saldırılara karşı daha dikkatli olunmasını ve internete bağlı bilgisayarlar üzerinde bulunan kişisel verilerin korunması amacıyla kullanıcı farkındalığının geliştirilmesini zorunlu hale getirmektedir. Kişisel verilerin korunması için alınan önlemlerin ve uygulanacak yöntemlerin çeşitliliğinin artması, bu konunun disiplinler arası boyutunun da gelişmesine ve çok yönlü yaklaşımın benimsenmesine neden olmaktadır. Bu nedenle, farklı bakış açılarını birleştiren ya da konunun farklı boyutlarının da görülebilmesini sağlayan ilke ve politikaların varlığına ihtiyaç duyulmaktadır. Politikaların olmaması ya da basite indirgenmesi, kurumsal olarak konuya ilişkin vizyon sahibi olunamamasının başlıca nedenleri arasında yer almaktadır.

Bilgi güvenliğine ilişkin her boyutta riskler artmakla birlikte, en fazla tartışılan konular arasında kişisel verilerin korunması konusu yer almaktadır (King ve Raja, 2012). 2013 yılı itibariyle dünyanın farklı bölgelerinden 101 ülkenin verilerin korumasına ilişkin

olarak hukuksal düzenlemeleri yapmış olduğu görülmektedir (Greenleaf, 2013b). 1970 yılında Almanya ve 1973 yılında İsveç tarafından yapılan ilk hukuksal düzenlemelerden 2012 yılına kadar olan 40 yıllık süreçte veri koruma kanunlarına duyulan gereksinim bilgi sistemlerinin kullanımına bağlı olarak artış göstermiştir (Greenleaf, 2013a). Yapılan araştırmalarda, Avrupa dışındaki ülkelerin yapmış oldukları veri koruma kanunlarının büyük bölümünde AB tarafından hazırlanan veri koruma standartlarının etkisinin bulunduğu görülmektedir (Greenleaf, 2012). AB sınırları içinde özellikle çevrimiçi ticareti canlandırabilmek amacıyla, kişisel verilerin daha iyi korunmasına yönelik çalışmalar aralıksız olarak devam etmektedir. Bu çalışmaların hukuksal kısmı yeni bir veri koruma direktifi üzerinde yoğunlaşırken, etkin denetim kurumlarının oluşturulması ve uluslararası sözleşmelerin yapılması için de çaba gösterilmektedir. Bu nedenle, literatürde bilgi güvenliğinin sağlanmasına ilişkin alınan önlemler ve uluslararası boyuttaki çalışmalarda, kişisel verilerin korunması konusuna daha fazla odaklanıldığı görülmektedir.

AB'de 1980'li yıllardan itibaren tartışılan ve hukuksal, sosyal ve teknik boyutları bulunan kişisel verilerin korunması konusunun, Türkiye'de henüz ilgiden uzak olduğu ve bu konuda yeterli seviyede önlemlerin alınmadığı bilinmektedir. Türkiye'de kişisel verilerin korunmasına ilişkin hukuksal düzenlemeler, AB hukuk mevzuatı ve bu konuda belirlenen uluslararası normları karşılamamaktadır. Açık ve anlaşılır hukuksal düzenlemelerin ve uygulanabilir yazılı politikaların bulunmaması, kişisel bilgileri işleyen personelin bu konudaki sorumluluklarının sınırlarını çizmekte zorlanmalarına neden olmaktadır. Alınan güvenlik önlemlerinin yetersizliği ya da personelin farkındalık eksikliği nedeniyle meydana gelen veri ihlalleri, bireylerin kişisel hak ve özgürlüğünün ihlal edilmesi anlamına gelmektedir. İhlallerin önlenmesi ve korumanın sağlanmasına ilişkin sorumlulukların yalnızca bilişim alanına bırakılması, bu konunun teknik önlemlerin alınması ile sınırlı kalması ve bireyi korumaya yönelik etkin korumanın sağlanamamasına neden olmaktadır. Uluslararası bilgi güvenliği standartları çerçevesinde devlet kurumlarına yönelik olarak yapılan bilgi güvenliği denetlemeleri, bilgi güvenliği politikalarından yoksun kurumların bilgi güvenliği farkındalığının çok düşük ve endişeleri arttıracak boyutta olduğunu göstermektedir (DDK, 2013). Kurumların yeterli bilgi güvenliği seviyesine ulaşması ve bireylerin kişisel verilerin korunması konusunda

kurumlara olan güveninin yeniden sağlanabilmesi, birtakım önlemlerin alınmasıyla mümkün olabilecektir. Bu kapsamda alınacak önlemler; etik ilkeler, uluslararası bilgi güvenliği standartları, çok yönlü bilgi güvenliği modelleri, uluslararası sözleşmeler ve ulusal hukuk düzenlemeleri çerçevesinde olmalıdır.

Türkiye'de son yıllarda kişisel verilerin korunması konusunda artan kaygılar, kamu kurum ve kuruluşlarını bu konuda önlem almaya zorlamaktadır. Nitekim yakın zamanda bazı bakanlıklar tarafından konunun önemine dikkat çeken ve bağlı kurumlarda acil olarak önlemler alınmasını isteyen yazılar yayınlanmıştır (MEB, 2014). Ancak bu yazılarda alınması gereken önlemlerin hangi ilke, politika ve/veya hukuksal düzenlemelere bağlı olarak alınacağı ve önlem alınmaması halinde uygulanacak yaptırımlar açık değildir. Ayrıca kişisel verilerin korunması konusu sadece bu bilgilerin internet üzerinde açık hale gelmesi ile sınırlı değildir. Kişisel bilgilerin ihtiyaç duyulan ölçüde elde edilmesi ve bu verilerin işlendiği bilgi sistemlerin güvenliğinin sağlanması da bu sürecin önemli bileşenleridir.

Kişisel verilerin korunması konusuna üniversiteler açısından bakıldığında; her üniversitenin sadece bir birimi tarafından belirli etik kurallar çerçevesinde oluşturulan bilgi güvenliği önlemleri, uygulamada farklılıkların oluşmasına neden olabilmekte ve kişisel verileri işleyen personeli yönlendirme, bilinçlendirme ve risklerden koruma konusunda yetersiz kalabilmektedir. Hukuksal düzenlemelerin yetersizliği, farklı disiplinlerin sorumluluklarını tek çatı altında birleştiren yazılı politikaların bulunmaması ve literatürün yetersiz olması, risk yönetiminin bir bütün halinde yapılamamasına ve kişisel hakların yeterince korunamadığı bilgi güvenliği ihlallerine neden olmaktadır. ABD'de bulunan üniversitelerde bilgi güvenliği politikaları yasal düzenlemelere bağlı kalınarak uygulanmaktadır. Alınan önlemler ve geliştirilen uygulamalar, "bilgi güvenliğinin sağlanması" konusu çerçevesinde tanımlanmaktadır[1]. AB sınırları içinde yer alan üniversitelerde de aynı hassasiyetin korunduğu görülmektedir. AB içinde, veri koruma kanunu çerçevesinde kişisel verilerin elde edilmesi ve işlenmesi sürecinin tümünü kapsayan yazılı bilgi güvenliği ve kişisel verileri koruma politikalarının birlikte oluşturulduğu birçok üniversite örneği bulunmaktadır. Türkiye'deki üniversitelerde ise

[1]Konuya ilişkin detaylı bilgi ve örneklere "3.1.1. Üniversitelerde Kişisel Veri Algısı" başlığı altında yer verilmiştir.

henüz ortak bir platformda kişisel verilerin korunmasına yönelik çalışma yapılmamış olduğu ve bu nedenle kişisel verilerin korunmasına ilişkin yazılı bilgi güvenliği politikalarının bulunmadığı görülmektedir. Üniversitelerde bilgi güvenliğinin hukuksal, teknik ve farkındalığı ilgilendiren boyutları ortak bir platformda ele alınmadığı müddetçe kalıcı başarıya ulaşılması mümkün değildir. Ortak bir platformun oluşabilmesi için, bu üç zeminde çalışan farklı disiplinlerin görüşleri ve sınırlılıkları değerlendirilerek, yazılı bilgi güvenliği politikaları ve bilgi güvenliği standartlarının oluşturulması önemlidir.

Kişisel verilerin korunmasına yönelik problemin özünde, bu bilgilerin bilgi teknolojileri sayesinde kontrolsüz ve hızlı bir şekilde çoğaltılabilmesi, depolama maliyetlerinin düşük olması nedeniyle gereğinden fazla bilginin kayıt altına alınması, kısa sürede uzak mesafelere transfer edilebilmesi, tehditlere karşı korunamayan bilgilerin kısa süre içinde sınırsız sayıda kişinin erişimine açık hale gelmesi ve bu sürecin kontrol dışına çıktığı andan itibaren geri dönüşü olmayan sonuçlar doğurabilmesi bulunmaktadır. Kişisel verilerin dijital ortamda işlenmesinin engellenemeyeceği ya da kısıtlanamayacağı açıktır. Bununla beraber, dijital ortamda özel hayatın ihlal edilmesi halinde tekrar güvenli hale getirilmesi de mümkün olamamaktadır. Mevcut yasal düzenlemeler de hassas ve kişisel verilerin tüm kurum, kuruluş ve şirketlerde hassasiyet gösterilerek işlenmesi ve özel hayatın gizliliğinin korunması konusunda yetersiz kalmaktadır. Tüm bu sorunların önüne geçebilmenin en etkin yolu, kişisel verilerin korunmasına yönelik risk yönetimi uygulamak ve var olan risklerle bilinçli olarak mücadele edilebilmesi için politikaların geliştirilerek çok boyutlu önlemlerin alınmasıdır.

Özel kuruluşlar ve devlet kurumları tarafından bireylerin bilgisi dâhilinde ya da rızası olmaksızın birçok bilgi toplanmaktadır. Özel kuruluşlar karlılığı arttırmaya yönelik olarak bilgi davranışlarını ortaya çıkarmak amacıyla kişisel verilere ihtiyaç duyarken, devlet kurumları kamu hizmetlerinde ve bilgi yönetiminde kaliteyi arttırmak amacıyla kişisel verileri toplamakta ve işlemektedir. Kim tarafından ve nasıl işlendiği bilinmeyen kişisel veriler hangi kurum ya da kuruluş tarafından toplanmış olursa olsun, veri sahibi için risk oluşturmaktadır. Diğer kamu kurum ve kuruluşlarında olduğu gibi, ne yazık ki üniversitelerin web sayfaları üzerinden yapılan ön araştırma sonuçları Türkiye'deki üniversitelerin hukuksal düzenlemeleri de dikkate alan bilgi güvenliği politikalarının

bulunmadığını göstermektedir. Üniversite bilgi sistemleri üzerinde bulunan personel bilgileri, öğretim elemanlarına ait bilgiler ve mezun olduktan sonra dahi sistem üzerinden silinmeyen öğrenci bilgileri, bu bilgilerin nasıl işleneceği ve korunacağı hakkında politikaların belirlenmemiş olması nedeniyle risk altındadır. Kişisel verilerin korunmasına ilişkin bir veri koruma yasasının ve üniversitelerde bu açığı kapatabilecek nitelikte yazılı bilgi güvenliği politikaları ve etik ilkelerin bulunmaması, var olan riskleri endişe duyulacak boyutlara taşımaktadır. Kişisel verilerin yoğun olarak işlendiği üniversitelerde bu verilerin yeterli düzeyde korunabilmesi için, verilerin elde edilmesi aşamasından itibaren AB içinde bulunan üniversitelerde (Stuttgart University, 2013) olduğu gibi hassasiyet göstermeleri önem taşımaktadır. Bilgi güvenliğinin sağlanması konusunda geliştirilen çözüm önerileri, bilgi işlem birimlerinin almaya çalıştığı teknik önlemlerle sınırlı kalmaktadır. Ancak alınacak hiçbir teknik önlem, bilgi güvenliğinin sağlanması ve kişisel verilerin korunması için tek başına yeterli değildir. Bilgi sistemleri ve iletişim ortamı en güvenilir kriptolama yöntemi ile korunuyor olsa dahi, kullanıcı zafiyeti ile güvensiz bir iletişim ortamı oluşabilmektedir. Bunun yanı sıra kişisel verilerin sadece teknik yöntemlerle korunmasının amaçlanması, bilginin gizliliğinin korunmasına odaklanıldığını düşündürmektedir. Oysa kişisel verilerin korunmasındaki asıl amaç kişinin hak ve özgürlüğünün korunması olmalıdır.

Kişisel verilerin korunması konusunda hukuk alanı dışında yapılan ve daha geniş boyutta alınabilecek bilgi güvenliği önlemlerini içeren çalışmalar yok denecek kadar azdır. Kurum ve kuruluşların kişisel verilerin korumasını da amaçlayan kapsamlı bilgi güvenliği politikalarından yoksun olmalarının en önemli nedenlerinden biri, bu konuda örnek alınabilecek çalışmaların bulunmamasıdır. Bir kurum ya da kuruluş için kapsamlı bilgi güvenliği politikası geliştirilebilmesi için, bu konudaki tüm koşulların değerlendirildiği araştırma sonuçlarına gereksinim duyulmaktadır. Özellikle yeni açılan üniversitelerde bilgi yönetim süreçleri ve bilgi güvenliği sorumluluklarına ilişkin eksikliklerin tespit edilerek bu konuda rehber ilkelerin oluşturulması, diğer kurum ve kuruluşlara istihdam sağlayan öncü ve örnek kuruluşlar olarak üniversitelerde standartların belirlenmesi açısından önem taşımaktadır.

1.2. ARAŞTIRMANIN AMACI VE SORULARI

Bu çalışmada, AB ve Türkiye'de kişisel verilerin korunmasına ilişkin mevcut hukuksal düzenlemeler değerlendirilerek ve kapsamlı bir bilgi güvenliği modeli olan McCumber bilgi güvenliği modelinden faydalanılarak, Türkiye'deki üniversiteler için uygulanabilir yazılı bilgi güvenliği politikasının geliştirilmesi amaçlanmaktadır. Bu çalışmayla, yasal düzenlemelerin yeterliliğinin kuramsal bilgi güvenliği modeli çerçevesinde değerlendirilmesi yapılarak literatüre katkı sağlanması, üniversitelerdeki mevcut durumun tespit edilmesi, farkındalığının ölçülmesi ve bulgulara bağlı olarak kişisel verilerin korunmasına ilişkin yazılı bir bilgi güvenliği politikasının geliştirilmesi hedeflenmektedir. Bilgi çağının ve bilgi toplumunun üç önemli üretim faktörünün (bilgi, teknoloji ve iyi yetişmiş insan) kaynağı olan üniversiteler için geliştirilecek olan bilgi güvenliği politikaları, diğer kurum ve kuruluşlar için de rehber ilkelerin belirlenmesine katkı sağlayacaktır.

Çalışma kapsamında yanıt aranacak araştırma soruları şunlardır;

1. Hassas bilgi varlıklarını korumaya yönelik yasal düzenlemeler bulunmakta mıdır? Mevcut yasal düzenlemeler kişisel verilerin korunmasına ilişkin kişisel hak ve özgürlüğü koruyabilecek yeterliliği taşımakta mıdır?
2. Üniversitelerde kişisel verilerin işlenmesi ve korunmasına yönelik politikalar belirlenmiş midir? Yazılı bilgi güvenliği politikaları mevcut mudur?
3. Üniversitelerde bireylerin özel alanına müdahale edilmekte ve gereğinden fazla kişisel/hassas bilgi işlenerek bireyler izlenmekte midir? Verilerin ne kadar süreyle saklanacağı konusunda politikalar belirlenmiş midir?
4. Mevcut bilgi güvenliği politikaları içinde kişisel verilerin korunmasına ilişkin önlemlere yer verilmiş midir?
5. Verilerin korunmasına yönelik önlemler hangi boyutlarda ve nasıl alınmaktadır? Bilgi yönetim stratejileri ve risk yönetimi planı var mıdır?
6. Kişisel verileri kaydeden personel, kişisel verilerin hangi amaçla, ne kadar süreyle ve kim tarafından işleneceği konusunda eğitim ve kurslar ile bilgilendirilmiş

midir? Yasal düzenlemelerden haberdarlar mıdır? Bu konudaki meslek içi eğitim durumu ve ihtiyacı nedir?

7. Kişisel verileri işleyen birimlerin, bilgi güvenliği ve kişisel verilerin korunması konusundaki görüşleri nelerdir?

1.3. ARAŞTIRMANIN KAPSAMI

Araştırma kapsamında Türk Hukuk Mevzuatı, AB Hukuk Mevzuatı, McCumber bilgi güvenliği modeli ve Ankara'da bulunan 15 üniversitenin web siteleri kişisel verilerin korunmasıyla ilişkili olarak incelenmiştir. Bununla birlikte, üniversitelerin ilgili birimlerinden görüşme ve anket yöntemiyle bilgi toplanmıştır. Üniversitelerde bilgi güvenliğinin sağlanması konusunda en büyük sorumluluğu taşıyan birim olarak BİDB'lığı ve kişisel verilerin yoğun olarak işlendiği birimler olan PDB ve üniversite bilgi merkezleri araştırma kapsamına alınmıştır.

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

1.4. ARAŞTIRMANIN YÖNTEMİ

Kişisel verilerin korunması konusunun kendi koşulları içinde tanımlanması, açıklanması ve AB içindeki koşullarla etkileşiminin incelenerek kapsamlı bilgi güvenliği politika önerisi geliştirilebilmesi için, bu çalışmada betimleme yöntemi kullanılmıştır. Betimleme, geçmişte ya da halen var olan bir durumu veya araştırmaya konu olan olayı kendi koşulları içinde olduğu gibi tanımlamaya çalışan bir araştırma yöntemidir (Karasar, 2012). Betimleme yöntemi, sosyal bilimlerde en sık ve geniş bir grubu tanımlamak ve eğilimi ölçmek için kullanılan en iyi araçtır (Rubin ve Babbie, 2011).

Bu araştırmanın verileri, görüşme ve anket tekniği birlikte kullanılarak elde edilmiştir. Verilerin korunması ve merkezi olarak üniversitelerde bilgi güvenliğinin sağlanmasından sorumlu BİDB, üniversitelerde kişisel bilgilerin yoğun olarak işlendiği PDB ve bilgi merkezlerine yapılandırılmış sorular yöneltilmiştir. Kişisel verilerin işlenmesi ve korunması konusunda BİDB, PDB ve üniversite bilgi merkezlerinin bakış açılarının farklı olabileceği ve sorulara farklı anlamlar verebilecekleri (Karasar, 2012) göz önüne alınarak, katılımcılara görüşme yoluyla anket uygulanmıştır. Anket yöntemi, üniversitelerde kişisel bilgilerin yoğun olarak işlendiği PDB ve bilgi merkezlerinden elde edilen verilerin karşılaştırılabilmesine ve verilen cevapların tekrar kontrol edilebilmesine olanak sağlamaktadır (Kaptan, 1995). BİDB, PDB ve bilgi merkezlerinde uygulanan anketler; posta yoluyla yapılan ankete olasılıkla yanıt alma oranının daha yüksek olması ve yanlışlıkları düzeltme, eksikleri tamamlama ve daha sağlıklı bilgi alarak farkındalığı en iyi şekilde ölçebilme olanağı sunması nedeniyle, yüz yüze görüşme yoluyla uygulanmıştır. Görüşme ve anketlerle üniversitelerde mevcut bilgi güvenliği politikaları, farkındalık, eğitim durumu ve bilgi güvenliğinin sağlanmasına yönelik uygulamalar hakkında detaylı bilgi alınmıştır.

1.4.1. Araştırma Evreni

Araştırma evrenini Ankara'da bulunan 5 devlet ve 10 vakıf üniversitesinin BİDB, PDB ve üniversite bilgi merkezleri oluşturmaktadır. Araştırmada örneklem alınmamış, tüm evren üzerinde çalışılmıştır. Kuruluş işlemlerini tamamlamış ancak yapılanma çalışmaları devam eden 1 devlet ve 2 vakıf üniversitesi araştırma kapsamına alınmamıştır.

Ankara'daki üniversitelerin, köklü ya da yeni kurulan devlet ve vakıf üniversiteleri olmaları açısından temsil gücü göz önüne alındığında; bu üniversitelerden elde edilen veriler ışığında geliştirilecek bilgi güvenliği politikalarının Türkiye'deki tüm üniversiteler için uygulanabilirlik seviyesinin yüksek olacağı öngörülmektedir. Türkiye'deki diğer bütün kurum ve kuruluşlar için temel standartları oluşturabilecek bilgi güvenliği politikasının oluşturulmasına katkı sağlayacağı ve geçerliğinin de yüksek olacağı öngörülerek; araştırma için üniversite BİDB, PDB ve bilgi merkezleri seçilmiştir. Üniversitelerde bilgi güvenliğinin sağlanması konusunda öncelikli olarak sorumlu

bulunan BİDB'lerin yetersiz kaldıkları sorunların arkasındaki eksikliklerin tespit edilmesi de, geliştirilecek olan bilgi güvenliği politikasının güvenilirliği ve uygulanabilirliğine katkı sağlamaktadır.

1.4.2. Veri Toplama Süreci

Bu araştırmada Ankara'da bulunan 15 üniversitede yapılan görüşme ve anket sonucunda elde edilen veriler değerlendirilmektedir. Araştırma kapsamında üniversitelerin BİDB, PDB ve bilgi merkezlerinden verilerin toplanması amacıyla hazırlanan anket soruları için, ODTÜ ve Hacettepe Üniversitesi'nden etik kurul onayı alınmıştır. Ayrıca, araştırma kapsamında yer alan iki üniversitenin isteği üzerine, etik kurul kararına ilâve olarak Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü tarafından hazırlanan araştırmaya ilişkin üst yazı ile görüşme başvurusu yapılmıştır.

Araştırma kapsamında yer alan 15 üniversitenin web sayfaları üzerinden yapılan ön incelemede, üniversitelerde kişisel verilerin en yoğun olarak işlendiği birimlerin PDB ve bilgi merkezleri olduğu görülmüştür. Bu verilerin korunması ve genel olarak üniversitelerde bilgi güvenliğinin sağlanmasından ise BİDB'nin sorumlu olduğu görülmektedir. Bu nedenle mevcut durumun ve farkındalığın ölçülebilmesi amacıyla bu üç birim üzerinden veri elde edilmesine karar verilmiştir. Üniversitelerin BİDB, PDB ve bilgi merkezlerinden elde edilen veriler görüşme yoluyla anket uygulanarak toplanmıştır. Üniversitenin bu üç biriminde bilgi güvenliğine ilişkin farkındalığın oluşturulması ve belirlenen politikaların uygulanması konusunda yönetici sorumluluğunu taşıyan kişiler olmaları nedeniyle, görüşme ve anket soruları üç birimin daire başkanları ya da yardımcılarına yöneltilmiştir.

BİDB ile yapılan görüşme soruları (Bkz. EK-1); mevcut bilgi güvenliği politikalarının varlığı, uygulanan bilgi güvenliği standartlarına ilişkin bilgiler, bilgi güvenliğinin sağlanmasına yönelik ihtiyaçların belirlenmesi, kişisel verilerin korunması amacıyla alınan önlemlerin tespit edilmesi, hukuksal düzenlemelerin uygulamaya yönelik etkileri, güvenlik denetimleri ve veri ihlali durumunda atılacak adımlara ilişkin bilgileri elde etmek amacıyla hazırlanmıştır. PDB'de uygulanan anket soruları (Bkz. EK-2); kişisel

verileri işleyen personeli bilinçlendirmek amacıyla yapılan çalışmalar, bilgi güvenliği politikaları hakkındaki farkındalık, kişisel verilerin elde edilmesinden imhasına kadar olan sürecin yönetimi, personel hatalarına ilişkin idari yaptırımlar ve bilgi erişim yetkilendirmelerine ilişkin mevcut durum hakkında bilgi sağlayacak içerikte hazırlanmıştır. Bilgi merkezlerinde uygulanan anket soruları ise (Bkz. EK-3), bilgi güvenliği konusundaki tüm uygulamalar hakkında kapsamlı bilgi edinmek ve aynı zamanda farkındalığı ölçmek amacıyla hazırlanmıştır.

Araştırma için hazırlanan anket soruları tek seçimli sorular, çok seçimli sorular, dizi soruları, yanıtı tanımlı sorular ve uygulamaya ilişkin görüşlerin alınabileceği açık uçlu sorulardan oluşmaktadır. Anket sorularına ilişkin eksikliklerin belirlenebilmesi amacıyla üç üniversitede pilot (ön) çalışma uygulanmış ve öneriler doğrultusunda anket soruları tekrar düzenlenmiştir.

Görüşme ve anket sorularının hazırlanmasında; uluslararası bilgi güvenliği standartları, diğer kurumlarda yapılmış olan bilgi güvenliği denetimleri sonucunda yayınlanan raporlar, kişisel verilerin korunmasına yönelik etik ilkeler, AB Veri Koruma Kanunu ve kişisel hakların korunmasına ilişkin hukuksal düzenlemelerden faydalanılmıştır. Görüşme ve anket soruları, araştırma kapsamında yer alan 15 üniversitenin web sayfaları üzerinde yapılan ön araştırma sonuçları ve kişisel verilerin korunmasına yönelik temel ilkeler çerçevesinde gruplandırılarak hangi birimlere hangi soruların sorulacağına karar verilmiştir.

1.4.3. Verilerin Değerlendirilmesi

Araştırma kapsamında hassas ve kişisel verilerin korunmasına ilişkin yazılı politikalara ve uygulamalara ilişkin mevcut durumu betimlemek amacıyla gerekli literatür taraması yapılmıştır. Öncelikle hassas bilgi varlıklarının ve kişisel verilerin korunmasına ilişkin şartları içeren AB Hukuk Mevzuatı ve Türk Hukuk Mevzuatı doküman analizi yöntemiyle incelenmiştir. Bu iki hukuk mevzuatının kişisel verilerin korunmasına yönelik yaklaşımları, farklılığı ve eksiklikleri, evrensel ilkeler ve uluslararası sözleşmelerle birlikte değerlendirilmiştir. Daha sonra kişisel verilerin korunmasına ilişkin hukuksal

koşullar ve düzenlemeler, çok yönlü ve uygulanabilir bir bilgi güvenliği modeli olan McCumber bilgi güvenliği modeli çerçevesinde değerlendirilmiştir. McCumber bilgi güvenliği modeli, çalıştırmanın çerçevesinin belirlenmesi ve çalışma haritasının daha belirgin hale getirilmesinde de önemli bir unsur olarak kullanılmıştır.

Üniversitelerde uygulanan bilgi güvenliği politikalarına ilişkin mevcut durumun tespit edilmesi amacıyla üniversite web sayfaları içerik analizi yöntemiyle incelenmiş ve bir ön değerlendirme yapılmıştır. Üniversitelerde kişisel verilerin korunmasına yönelik olarak hazırlanan yazılı politikalar, ilgili herkes tarafından erişilebilir durumdadır. Üniversitelerin BİDB, PDB ve bilgi merkezlerinden görüşme yoluyla anket uygulanarak elde edilen bulgular; mevcut durum, uygulamalar, farkındalık ve geliştirilecek olan bilgi güvenliği politikası açısından değerlendirilmiştir.

Mevcut durumun belirlenmesi amacıyla yapılan araştırmada, üniversitelerin içinde bulundukları riskler değerlendirilmiştir. Ancak bu üniversitelerin siber saldırıların ve kötü amaçlı girişimlerin hedefi haline gelmemesi amacıyla, çalışmada üniversite isimlerine ilişkin bilgiler kullanılmamıştır.

1.5. ARAŞTIRMANIN DÜZENİ

Bu çalışma altı bölümden oluşmaktadır.

Çalışmanın ilk bölümünde konunun önemi, araştırmanın amacı ve kapsamı, araştırma soruları, araştırmanın yöntemi, veri toplama teknikleri, örneklem, araştırmanın bölümleri ve yararlanılan kaynaklar hakkında bilgi verilmektedir.

İkinci bölümde hassas bilgi varlıklarının ve kişisel verilerin hukuksal düzenlemelerle korunması konusunda literatür değerlendirmesi yapılmıştır. Bu bölümde öncelikle kişisel veri, hassas veri ve korunan değerlere ilişkin temel kavramlar tanımlanmıştır. Daha sonra Türk Hukuk Mevzuatında yer alan bilgi güvenliğinin sağlanmasına ilişkin düzenlemeler AB bilgi güvenliği politikaları kapsamında yapılan hukuksal düzenlemeler ve kuramsal bir model çerçevesinde irdelenmiş ve mevzuattaki boşluklara dikkat çekilmiştir.

Üçüncü bölümde üniversitelerin web sayfaları üzerinden yapılan ön araştırmaya ilişkin bulgular ile araştırma kapsamında yer alan üniversite birimlerinin (BİDB, PDB ve bilgi merkezleri) almış oldukları önlemler, uygulamalar, belirlenmiş oldukları politikalar ve farkındalıklarına ilişkin değerlendirme yapılmıştır. Ayrıca bu bölümde üniversitelerde risk yönetimi, güvenlik önlemleri ve kişisel verilerin korunmasına yönelik algılar hakkında da bilgi sunulmuştur.

Dördüncü bölümde, üniversite BİDB, PDB ve bilgi merkezlerinde görüşme yoluyla uygulanan anketler sonucunda elde edilen bulgular sunulmuştur. Elde edilen bulgular temel ilkeler çerçevesinde; mevcut bilgi güvenliği politikaları, verilerin toplanması, düzenlenmesi, saklanması, kullanımı, paylaşımı, verilerin imhası, kişisel verilerin korunmasına ilişkin önlemler, sorumluluklar, risk yönetimi, eğitim ve farkındalık durumuna ilişkin bölümler altında sınıflandırılmıştır.

Beşinci bölümde, elde edilen verilere ilişkin değerlendirmeler yapılmıştır. Bu bölümde, katılımcıların görüş ve uygulamaya ilişkin olarak vermiş olduğu bilgiler; hukuksal sorumluluklar, temel ilkeler ve McCumber modeli çerçevesinde değerlendirilerek, üniversite bilgi güvenliği politikasında yer alacak genel unsurlar belirlenmiştir.

Altıncı ve son bölümde, Türkiye'de bulunan tüm üniversitelerin uygulayabileceği bir örnek bilgi güvenliği politikasına yer verilmiştir. Bilgi güvenliği politikası, çalışmanın bütününü oluşturan hukuksal koşullar, kuramsal bilgi güvenliği modeli ve araştırma bulgularına bağlı olarak geliştirilmiştir.

1.6. KAYNAKLAR

Araştırma kapsamında önceden yapılmış çalışmaların belirlenmesi ve literatür araştırmasının yapılması amacıyla aşağıda yer alan kaynaklardan yararlanılmıştır.

AB Hukuk Bilgi Bankası (http://eur-lex.europa.eu/)
Dissertations and Theses - Proquest

EBook Collection – EBSCOhost
Emerald Management
Google Books (http://books.google.com)
Google Scholar (http://scholar.google.com)
HukukTürk – Hukuk Bilgi Bankası
IEEE Xplore
Kazancı Mevzuat ve İçtihat Bilgi Bankası
McGraw Hill E-Books
OECD iLibrary
SAGE Journals
ScienceDirect
Scopus
Springer E-Books
Taylor & Francis Online Journals
YÖK Tez Veri Tabanı

Tezin yazımında Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü *Tez ve Rapor Yazım Yönergesi* (2004) ve *Kaynak Gösterme El Kitabı* (Kurbanoğlu, 2004) kullanılmıştır.

2. BÖLÜM

HASSAS BİLGİ VARLIKLARININ VE KİŞİSEL VERİLERİN HUKUKSAL DÜZENLEMELER İLE KORUNMASI

2.1. TEMEL KAVRAMLAR

2.1.1. Veri, Bilgi ve Kişisel Veri İlişkisi

Literatürde veri (data), enformasyon (information) ve bilgi (knowledge) kavramlarının farklılığını açıklayan birçok yayın bulunmaktadır. Türkçede veri, işlenmemiş, yorumlanması gereken (ham) gerçekler olarak ifade edilmektedir. Bilgi kavramı ise, İngilizce de information ve knowledge kavramlarının her ikisinin de karşılığı olarak Türkçede yer almıştır. Bu durum bilginin Türkçedeki ifadesinde anlam karmaşası oluşturmaktadır. Information (enformasyon) anlamında kullanılan bilginin veriden farklı olarak tek başına bir anlamı bulunmaktadır. Verinin kullanılması ile enformasyon oluşmaktadır. Bu nedenle enformasyon, bireyin düşünsel yapısında fark yaratabilecek veri olarak da ifade edilmektedir (Davenport ve Prusak, 2000). Knowledge olarak bilgi de her ne kadar Türkçede aynı anlamda kullanılsa da, bireyin kendi gerçekleri olması ve açıklamadığı takdirde erişiminin mümkün olmaması yönüyle enformasyondan ayrılmaktadır. Bireyin zihninde var olan ve karar verme aşamasında başvurduğu bilginin (knowledge) soyuttan somuta dönüşmesi ile enformasyon oluşur. Bu nedenle enformasyon anlamında kullanılan bilgi ile knowledge anlamında kullanılan bilgi arasında farklılık ve bir dönüşüm ilişkisi bulunmaktadır. Bu tanım ve açıklamalar çerçevesinde bakıldığında, bilgi güvenliğine ilişkin çözümlere konu olan "bilgi", information anlamında kullanılan, nesnesi olan bilgidir. Başka bir deyişle, yazılı, basılı, görsel, işitsel ve elektronik ortamlarda varlık bulan, depolanabilen, tanımlanabilen, düzenlenebilen, transfer edilebilen ve erişilebilen bilgidir. Bilgi bilimi açısından bilgi güvenliğinin sağlanması esnasındaki işlemleri, bilen (insan, süje) ve bilinen (nesne, obje) arasında kurulan bağın ya da bilgiye erişimin güvenli olarak tesis edilmesi şeklinde özetlemek mümkündür.

Farklı disiplinlerin bilgiye farklı açılardan bakışı, bilgi kavramına ilişkin farklı tanımların yapılmasına neden olmuştur. Bilgi kavramının günlük kullanımı da, bilimsel tanımlardan farklılık göstererek karışıklığa neden olabilmektedir. Bilgi güvenliği, bilgi sistemleri, bilgi yönetimi ve kişisel verilerin korunması gibi kavramların kullanımında bilimsel tanımlardaki ayrımın açık olarak yapılmamış olması, kavramlar arasında çelişki ve karmaşanın oluşmasına neden olmaktadır (Özenç Uçak, 2010). Ancak tüm bu kullanımlarda "bilgi" kavramı ile ifade edilmek istenen; yazılı, basılı ve elektronik ortamlarda yer alan (nesnesi olan) ve bilişsel yapıda değişiklik yaratan olgudur. Hukuksal düzenlemeler ve bilgi güvenliğine ilişkin literatürde "kişisel veri" ya da "kişisel bilgi" olarak ifade edilen bilgiler de aynı anlamda kullanılmaktadır. Literatürdeki kavramsal farklılıkların günlük kullanıma ve hukuksal düzenlemelere yeterince yansımamış olması, bu konuda tartışmaların devam edeceği ama yaygın kullanım nedeniyle değişiminin de kolay olmayacağını göstermektedir. Bu çalışmada da, disiplinler arası ifade çeşitliliği ve günlük kullanımdaki farklılıklarından kaynaklanan çelişkiler göz ardı edilerek, veri ve bilgi güvenliği yaygın olarak ifade edildiği gibi aynı anlamda kullanılmıştır.

2.1.2. Kişisel ve Hassas Veri Nedir?

Kişisel verilerin tanımı yapılırken, dünyanın farklı bölgelerinde farklı ifadelerin kullanıldığı görülmektedir. Örneğin ABD'nin Kaliforniya Eyaleti'nde "bireyin isim ve soyadının; sosyal güvenlik numarası, güvenlik kodu, erişim kodu, kredi kartı numarası, sağlık bilgileri, kişisel uygulamalara ait kayıtlar ve/veya sigorta bilgileri ile birlikte kullanılması" şeklinde tanımlanırken (California Information Practices Act, 2012); AB ülkelerinde "belirli ya da kimliği belirlenebilir (doğrudan ve/veya dolaylı yollarla) gerçek kişi ile ilgili her türlü bilgi" şeklinde tanımlanmaktadır (Avrupa Konseyi, 1995). Tanım üzerinde farklılıklar olmakla birlikte, korunan değer açısından bakıldığında farklılık bulunmamaktadır. Türkiye'de de AB veri koruma kanununda yapılan tanım 2014 yılında hazırlanan Kişisel Verilerin Korunması Kanun Tasarısı'nda (KVKKT) kullanılmıştır (T.C. Başbakanlık, 2014a).

Hassas veriler, açıklanması halinde kişinin toplum içinde ayrımcılığa uğramasına ya da ötekileştirilmesine neden olabilecek inanç, politik görüş, sağlık bilgileri, cinsel yaşamı,

etnik kökeni vb. bilgilerdir. Uluslararası hukuksal düzenlemelerde[2], hassas verilerin özellikli veri kategorileri altında yer aldığı ve bu bilgilerin iç hukukta uygun güvence sağlanmadıkça otomatik işleme tabi tutulamayacağı temel ilke olarak belirtilmektedir. 2014 yılında hazırlanan KVKKT'de de özel hayatın ve aile hayatının gizliliğini ihlal edebilecek özel niteliği olan kişisel veriler olarak; kişilerin ırkı, etnik kökeni, siyasî düşüncesi, felsefî inancı, dini, mezhebi veya diğer inançları, dernek, vakıf ya da sendika üyeliği, sağlığı veya cinsel hayatı ile ilgili bilgiler tanımlanmıştır.

AB'nin özel hayatın gizliliği ile ilişkili olarak gördüğü başlıca kişisel veriler arasında; telefon bilgileri, kimlik bilgileri, adres bilgileri, e-posta adresi, fotoğraflar, vatandaşlık numarası, kurum/öğrenci kimlik numarası, eğitim bilgileri, çevrimiçi kullanıcı hesapları, sosyal paylaşım siteleri üzerinden yapılan gönderiler, banka bilgileri ile sağlık kayıtları bulunmaktadır (Avrupa Komisyonu, 2012c). IP adresi, biyometrik bilgiler, genetik bilgileri, yer bilgileri çevrimiçi kimlik ve internet üzerinde ziyaret edilen sitelerden alınan çerezler de kültürel ve sosyal kimliği açığa çıkartan önemli bilgiler arasında yer almaktadır.

KVKKT'nin 3. Maddesinde yapılan kişisel veri tanımına ilişkin olarak, gerekçede kişisel verilerin sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi kesin teşhisi sağlayan bilgilerin değil, kişinin fiziki, ailevi, ekonomik, sosyal vb. özelliklerinin de bu kapsamda olduğu belirtilmiştir. Ayrıca fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliği ifade eden somut içerikler veya kimlik, vergi ve sigorta numarası gibi kişinin belirlenmesini sağlayan veriler kişisel veri olarak nitelendirilmektedir. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri ve genetik bilgiler de dolaylı olarak kişiyi belirlenebilir kılabilmeleri nedeniyle kişisel veri olarak nitelendirilmiştir (T.C. Başbakanlık, 2014a).

[2] **AK 108 Sayılı Sözleşme – Madde 6:**
İç hukukta uygun güvenceler sağlanmadıkça, ırk menşeini, politik düşünceleri, dini veya diğer inançları ortaya koyan kişisel nitelikteki verilerle sağlık veya cinsel yaşamla ilgili kişisel nitelikteki veriler ve ceza mahkûmiyetleri, otomatik bilgi işlemine tâbi tutulamazlar.

2.1.3. Kişisel Verilerin Korunması Hakkı

Kişisel verilerin korunması hakkı, kişisel verilere yönelik yetkisiz erişimler sonucunda meydana gelebilecek maddi ve manevi zarara karşı bireyin korunması ve bireyin kendisine ait kişisel bilgilerin geleceğini belirleme hakkını sağlamaktadır (Şimşek, 2008). Bireyin kendisine ait verilerin geleceğini belirleme hakkı, demokratik bir ülkede bireyin temek hak ve özgürlüğünün sağlanmış olması ile ilişkili olarak elde edilen bir haktır. Kişisel verilerin korunmasına yönelik haklar ulusal hukuksal düzenlemelerde 1970'li yıllardan itibaren yer almaya başlamıştır. 1970 yılında Almanya, 1973 yılında İsveç, 1976 yılında İspanya, Avusturya ve Portekiz'de kişisel verilerin koruma altına alınması konusunda yapılan yasal düzenlemeler, Avrupa'daki ilk örneklerdir (Küzeci, 2010). Bilgi sistemleri ve bilgisayar ağlarının devlet kurumları, kuruluşlar, şirketler ve bireysel kullanıcılar tarafından kullanımının yaygınlaşmaya başlamasıyla birlikte, 1980'li yıllardan itibaren uluslararası sözleşmelerde ve hukuksal düzenlemelerde kişisel verilerin korunmasının bir hak olarak yer aldığı görülmektedir (Avrupa Komisyonu, 1981). Bu nedenle, kişisel verinin bugünkü anlamda tanımının yapıldığı ilk uluslararası hukuksal düzenlemelerin 30-35 yıllık geçmişi bulunmaktadır. Ancak bilgi teknolojilerindeki hızlı dönüşüm ve gelişiminin beraberinde getirdiği riskler, hukuksal düzenlemeler açısından kişisel verilerin korunması konusunda birçok çalışmanın yapılmasına neden olmuştur. Bazı ülkelerde (İspanya, Hollanda vd.) kişisel verilerin korunması hakkı anayasal bir hak olarak güvence altına alınırken, bazı ülkelerde ayrı bir veri koruma kanunu ile güvence altına alınmıştır. Türkiye'de ise 12.09.2010 tarihinde yürürlüğe giren 5982 sayılı Kanunun[3] 2/3. maddesi ile Anayasa'ya kişisel verilerin korunması hakkı eklenmiştir. Anayasa'ya eklenen bu maddeyle, veri sahibinin bilgisi dışında kişisel verilerin işlenmesi sonucunda meydana gelebilecek zarara karşı veri sahibinin temel haklarının korunarak güvence altına alınması hedeflenmiştir.

AB Temel Haklar Şartı'nda kişisel bilgilerin korunması konusu, "özgürlükler" başlıklı ikinci bölümde verilmiştir. Kişisel verilerin korunması ile özgürlükler arasında kurulan bu ilişki, AB ülkelerinin uygulamalarında açık olarak görülmektedir. Örneğin Alman Anayasa Mahkemesi'nin kişisel verilerin korunmasına ilişkin kararları, insan onuru ve

[3] Halkoyuna Sunulan Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun

kişiliğinin serbest geliştirilmesi hakkına dayanmaktadır. Alman Anayasa Mahkemesi, kamu organlarının faaliyetleri karşısında insanın öz değerlerinin hiçe sayılarak bir veri objesi olarak görülmesinin özel yaşamın gizliliğini ihlal ettiği ve bunun insan onuru ile bağdaşmadığı görüşünü benimsemektedir (Şimşek, 2008).

Bireyin öz iradesiyle yaşamını şekillendirmesine ilişkin olarak kendisine ait bilgilerin ne zaman ve ne kadarını açıklayacağına karar vermesi, genel kişilik hakkı kapsamında değerlendirilmektedir. Bu kapsamda kişisel verilerin korunması hakkı ile genel kişilik hakları arasında kuvvetli bir bağ bulunduğu ve bireylerin kendisine ait verilerin geleceğini belirleme hakkının da genel kişilik hakkı ile birlikte korunduğu değerlendirilmektedir (Şimşek, 2008). Kişisel verilerin korunmasına ilişkin olarak yayınlanan resmi yazılarda (MEB, 2014) konunun önemine vurgu yapılırken "kişisel verilerin korunması hakkının temel insan hak ve özgürlükleri arasında yer aldığının ve şahsiyetin korunması için hayati öneme sahip olduğunun" ifade edilmesi de, uygulamada kişisel verilerin korunması hakkı ile genel kişilik hakları arasında ilişki kurulduğunu göstermektedir.

Kişisel verilerin korunması hakkı, özel hayatın gizliliği hakkı ile de aynı kapsamda değerlendirilmektedir. Kişisel verilerin korunması ile ilgili olarak Anayasa Mahkemesi'nin vermiş olduğu kararlarda, Anayasa'nın 20. Maddesinde düzenlenen "özel hayatın gizliliği" hakkına atıf yapıldığı görülmektedir (Anayasa Mahkemesi, 2008). Kişisel verilerin korunması konusuna bireyin özel hayatının gizliliğinin korunması açısından bakılması, hukuksal yönüyle konuya ilişkin olarak ortaya çıkan sorunların çözümüne de katkı sağlamaktadır. Ayrıca, düşünce özgürlüğü, ifade özgürlüğü ve bilgi alma özgürlüğü gibi temel hak ve özgürlükler kapsamında internet ortamında yer alan bilgilerin, kişilerin özel hayatının gizliliğini ihlal etmesi halinde daha düşük önceliğe sahip olacağı ve veri sahibinin talebi halinde bu bilgilerin yayından kaldırılması gerektiği aşikârdır.

2.1.4. Korunan Değer Olarak Özel Hayatın Gizliliği ve Verinin Gizliliği

Gizliliğin korunması ve gizlilik hakkına ilişkin kaygılarla birlikte, bu konuya yönelik tanımlamaların da çok eskiye dayandığı ve günümüze genişleyerek geldiği görülmektedir. 1890'lı yıllarda gizliliğin tanımı "yalnız bırakılma hakkı" olarak ifade edilmiştir (Warren ve Brandeis, 1890). Özel hayatın gizliliğine ilişkin hukuksal düzenlemelerle işlemlerin kontrol edilmesinin amacı, özerkliğin en üst seviyeye çıkarılması ve güvenlik açıklarının en düşük seviyeye indirilmesidir (Margulis, 1977). Veri koruma ve özel hayatın gizliliğinin korunmasına ilişkin olarak dünya genelinde hukuksal düzenlemeler incelendiğinde, özünde bireyin kendisine ait kişisel verileri üzerinde kontrol imkânının sağlanması bulunmaktadır (Aksoy, 2008; Stone, Gueutal, Gardner ve McClure, 1983). Veri koruma kanunlarının içeriği detaylı olarak incelendiğinde ise, kişisel hak ve özgürlüğün veri gizliliğinin korunmasıyla sağlandığı görülmektedir. Farklı coğrafi bölgelerde bulunan ülkelerin, veri koruma ya da veri gizliliği ismiyle çıkarmış oldukları kanunların hemen hemen aynı içeriğe sahip ve aynı amaca yönelik olarak hazırlanmış olması da bu konuda açık bir ayrımın bulunmadığını göstermektedir (Greenleaf, 2012). Bilginin hukuka uygun olarak elde edilmesi, amacına uygun olarak kullanılması, gereğinden fazla bilgi toplanmaması, veri sahibi tarafından erişilebilir olması, doğru ve güncel olması, güvenli olarak tutulması ve kullanım süresi sona eren bilgilerin uygun yöntemlerle imha edilmesi, veri koruma kanunlarının başlıca unsurlarını oluşturmaktadır. Ancak tüm bu unsurların uygulamada yerine getirildiği sorumluluk alanı, bilgi güvenliğine ilişkin uygulamalardır. Bu açıdan bakıldığında; bilgi güvenliği içinde gizlilik, veri sahibinin onayı olmaksızın kişisel bilgilerin toplanması, işlenmesi, depolanması ve transferinin yapılmaması, yetkisiz erişimlere kapatılması ve böylece kişisel hak ve özgürlüğün korunması anlamını taşımaktadır. Literatürde bilgi güvenliğinin sadece veri gizliliğini koruma yönüyle ele alındığı ve tanımlamaların bu yönde yapıldığı yayınlar daha fazladır. Bu durumun, bilgi güvenliği konusunun daha çok bilişim alanında çalışılması ve hukuksal boyutunun genelde ihmal edilmesinden kaynaklandığı değerlendirilmektedir. Ancak bilgi güvenliğinin sağlanmasına ilişkin birçok güvenilir kaynakta da, gizliliğin kişilere sahip oldukları kişisel verilerin gizliliğinin korunmasını isteme hakkıyla ilgili bir bilgi güvenliği unsuru olduğu belirtilmektedir (Chirillo ve Danielyan, 2005). Aynı kaynaklarda kişisel verilerin AB

hukuku ve ABD hukukunda nasıl tanımlandığına da yer verildiği ve bunun bilgi güvenliğine ilişkin "gizlilik" ilkesi ile açıklandığı görülmektedir. Bilgi politikaları içinde hukuksal düzenlemeler ile birlikte yer alan bilgi güvenliğine ilişkin bu çalışmalar, kişisel verilerin gizliliğinin korunarak, veri sahibinin bireysel hak ve özgürlüğünün korunmasının nihai amaç olması gerektiğini göstermektedir.

Literatürde gizliliğin bilginin karakteristik özelliklerinin tanımı ve kişinin hak ve özgürlüğünün hukuksal düzenlemeler ile korunması anlamındaki tanımı üzerine tartışmalar devam etmektedir (Grama, 2010). Kişisel verilerin ve kişisel hak ve özgürlüğün korunmasına ilişkin gizlilik (mahremiyet) bilginin korunması gereken karakteristik özellikleri arasında yer alan gizlilikten çok ince bir çizgi ile ayrılsa da, bilgi güvenliği gereksinimleri içinde yer alan bilgi güvenliği politikalarında her iki gizliliğin korunması da ayrılmaz unsurlar olarak yer almaktadır.

Gizlilik konusuna Winter'in bakış açısıyla bakıldığında, kişinin temel hak ve özgürlüğünün korunmasını hedef alan yaklaşımların bilgi güvenliğinin sağlanması amacıyla da benimsendiği görülmektedir. Winter'e göre gizlilik; kullanıcıların kendilerine ait kişisel bilgilerin ne zaman, nasıl ve ne kadarının başkalarının erişimine açılacağına karar vermeleridir (Winter, 1997). Bu tanım, verinin nasıl işlendiği, nasıl saklandığı ve kim tarafından erişildiği konusunda veri sahibinin bilgilendirilmek zorunda olduğunu ifade eden 95/46/EC isimli AB direktifinin yaklaşımıyla da örtüşmektedir.

Miller'in kırk yıl önce mahremiyete ilişkin olarak yapmış olduğu tanım, hukuk ve bilişim dünyasının mahremiyet anlayışını ortak bir noktada birleştirmektedir. Miller'e göre mahremiyet, veri sahibinin verilerinin dolaşımını kontrol yeteneğidir ve bireyin kendisiyle ilgili verileri kontrol hakkını içermektedir (Miller, 1971). Kişisel verilerin bireyin rızası dışında işlenmesine ilişkin her türlü girişim, bilgi mahremiyeti olarak da özelleştirilen mahremiyetin ve aynı zamanda özgürlüğün ihlal edilmesi anlamına gelmektedir. Bilgisayarlaşmış toplumlarda tehdit altında olan mahremiyetin sadece hukuksal düzenlemelerle korunması sağlanamamaktadır (Fischer-Hübner, 2001). Bu değerlendirmeye bilgi güvenliği konusunda tanınmış bir otorite olan Bruce Schneier da "güvenlik bir işlem sürecidir, ürün değildir" sözleriyle bilişim alanından bakarak açıklık

getirmektedir (Chirillo ve Danielyan, 2005). Bir bilgi teknolojisi kendi içinde ne kadar güvenli olursa olsun, güvenlik işlem süreci doğru şekilde yönetilemediği ve diğer güvenlik önlemleri ile birlikte değerlendirilmediği sürece tehditlerden korunması mümkün olamamaktadır.

2.1.5. Uluslararası Bilgi Güvenliği Standartları ve Bilgi Güvenliği Politikalarına Sağladığı Katkılar

Bilgi sistemlerine ve veri depolama ortamlarına yönelik yetkisiz erişimler, çoğunlukla internet üzerinden gerçekleştirilmektedir. Kişisel verilerin de üzerinde bulunduğu kurum ve kuruluş bilgisayarlarının internete bağlı olması, bu bilgisayarlar üzerinde bulunan bilgilerin güvenlik riskini arttırmaktadır. İnternet üzerinden gerçekleşen yetkisiz erişimlerin küresel çapta olması ve alınabilecek güvenlik önlemlerinin de benzer nitelikte olması, bu konuda uluslararası boyutta çalışmaların yapılmasını ve standartların geliştirilmesini zorunlu hale getirmiştir. Güvenlik yönetim modeli olarak da adlandırılan uluslararası standartlar, kurum ve kuruluşların kendi özel yapısına ve korunması gereken verilerin niteliğine bağlı olarak, bilgi güvenliği politikalarını geliştirmelerine de katkı sağlamaktadır (Höne ve Eloff, 2002).

Bilgi güvenliğinin sağlanmasına ilişkin standartların geliştirilmesi, bilgi teknolojilerinin gelişimine bağlı diğer alanlarda da olduğu gibi 1990'lı yıllarda başlamıştır. Bilgi güvenliği yönetimi konusunda İngiltere'nin 1995 yılında geliştirmiş olduğu BS7799 standardı, bilgi güvenliği politikalarında hangi unsurların kesinlikle bulunması gerektiği konusunda bilgi içeren ilk bilgi güvenliği standartlarından biri olması yönüyle önemlidir. Standartların yanı sıra BSI (British Standards Instute) tarafından bilgi güvenliğine ilişkin olarak yapılan farklı çalışmalar ve rehber dokümanlar da bulunmaktadır (Höne ve Eloff, 2002). BS7799 standardının birinci bölümü, günümüzde bilgi güvenliği standartları konusunda en çok bilinen ISO (International Organization for Standardization) ve IEC (International Electrotechnical Commission) tarafından 2000 yılında yeniden uyarlanarak ISO/IEC 17799 adıyla uluslararası standarda dönüştürülmüştür. ISO/IEC 17799 standardı 2005 yılında yeniden düzenlenerek ISO 17799:2005 adını almış ve 2007 yılında tekrar gözden geçirilerek ISO bilgi güvenliği standartlarını içeren 27000 serisi içinde ISO/IEC

27002 ismini almıştır. 2005 yılında yayınlanan ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi Standardı ise BS7799 standardının ikinci bölümünden uyarlanarak oluşturulmuştur. 2013 yılında tekrar güncellenen ve ISO/IEC 27001:2013 adını alan bu standart, her boyuttaki şirket ve kamu kuruluşuna uygulanabilir nitelikte olması nedeniyle, bilgi güvenliği yönetim sistemine ilişkin olarak en çok bilinen uluslararası bilgi güvenliği standardıdır (Gillon, Branz, Culnan, Dhillon ve Hodgkinson, 2011).

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri (BGYS), hassas ve kişisel verilerin güvenliğinin sağlanması konusunda sistematik bir yaklaşım ile gereksinimleri tanımlayan uluslararası bilgi güvenliği standardıdır. ISO/IEC 27001, BGYS kurmak isteyen kuruluşların risk analizleri yapıldıktan sonra gerekli bilgi güvenliği önlemlerinin alınmasını ve mevcut risklerin belirlenen kabul edilebilir risk seviyesinin altına indirilmesini sağlamaktadır. ISO/IEC 27001 BGYS ile yapılan denetimlerde, ISO/IEC 27002 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri standardından yararlanılmaktadır (Ottekin, 2008). ISO/IEC 27001 BGYS denetim listesi incelendiğinde, listede yer alan ilk bölümün bilgi güvenliği politikalarının varlığını sorgulaması dikkat çekicidir. Bir kurum ya da kuruluşta bilgi güvenliğine ilişkin olarak etkin önlemlerin alınabilmesi için, bir bilgi güvenliği politikasının oluşturulmuş olması gerekmektedir. Bu nedenle uluslararası standartlar çerçevesinde yapılan denetimlerde de öncelikli olarak bilgi güvenliği politikalarının varlığı ve etkinliğinin sorgulandığı görülmektedir.

2.2. MCCUMBER BİLGİ GÜVENLİĞİ MODELİ KAPSAMINDA BİLGİ GÜVENLİĞİ

2.2.1. Bilgi Güvenliği ve Kişisel Verilerin Korunması İlişkisi

Bilgi güvenliği konusunda yapılan ilk çalışmaların, askeri amaçlı bilgilerin gizliliğini ve kontrolünü sağlamaya yönelik olarak 1970'li yıllarda yapıldığı bilinmektedir. Gizliliğin korunmasına yönelik çalışmalar, bilgilerin dört gizlilik derecesi (tasnif dışı, özel, gizli ve çok gizli) altında sınıflandırılması ile devam etmiş ve bilgilerin bu sınıflandırmaya bağlı olarak korunması için stratejiler geliştirilmiştir (Waguespack, 2013). 1980'li yıllarda ise ticari alanda bilginin bütünlüğünün sağlanmasına yönelik kaygıların oluşması, bilgi

güvenliğinin bu boyutunun da dikkatleri üzerine çekmesine neden olmuştur. 1990'lı yıllarda da bilgi güvenliğinin gelişim sürecinde görülen kaygılar artmaya devam etmiştir. Bu süreçte iletişim teknolojisinin bilgisayar ağları ile gelişimine bağlı olarak tehditlerin çeşitliliğinin artması, bilgi güvenliği konusunda yeni boyutların oluşmasını (Landwehr, 2001) ve oluşan yeni boyutlar arasındaki karmaşık ilişkiyi açıklayacak bilgi güvenliği modellerinin geliştirilmesini sağlamıştır. 2000'li yıllardan itibaren kişisel haklara yönelik gelişmelere bağlı olarak kişisel verilerin korunması konusu da kamu kurumlarındaki verilerin gizliliğinin korunması kadar önemsenmeye başlanmıştır. AB ülkeleri ve diğer bilgi toplumuna dönüşüm sağlamış ülkelerde bu konuya ilişkin çalışmalar hukuk ve diğer sosyal alanlara da yayılarak disiplinler arası boyutun gelişmesi hız kazanmıştır (Whitman ve Mattord, 2011). Ancak farklı alanlarda yapılan çalışmaların genellikle bağımsız olarak yürütülmesi ve aralarında yeterli düzeyde iletişim sağlanamaması, bilgi güvenliği zincirinin kırılgan hale gelmesine neden olmuştur.

Bilgi güvenliği, bilgi ve bilgi sistemlerine yetkisiz erişim, bilginin kullanımı, ifşa edilmesi, bozulması, değiştirilmesi veya bilginin gizlilik, bütünlük ve kullanılabilirliğine zarar vermek için yapılan kötü niyetli girişimlere karşı sağlanacak korumadır (McCumber, 2005). Her ne kadar bu tanımda geleneksel vurgu yapılarak bilgi ve bilgi sistemlerine karşı koruma birlikte ifade edilse de, stratejik olarak bilgi güvenliğinin öncelikli konusu bilgi sistem altyapısının korunmasından ziyade bilgi içeriğinin korunmasıdır (Garigue, 2007). Bu kapsamlı tanımda koruma sağlanması öngörülen "bilgi", kişisel bilgileri de kapsayan genel bir ifade olarak kullanılmaktadır. Zira gerçekleşen veri ihlallerinde en fazla zarar gören kişi ve kurumlar, kişisel verilere yönelik olarak yapılan saldırılar nedeniyle zarara uğramaktadırlar. Bu nedenle verilerin korunması konusunda hazırlanan bilgi güvenliği politikalarında ve hukuksal düzenlemelerde, risk odaklı bilgi güvenliği[4] boyutunun daha fazla göz önünde bulundurulduğu ve aralarındaki ilişkiye yer verildiği görülmektedir (Avrupa Komisyonu, 2001b; Feiler, 2011). Bununla birlikte, bu düzenlemelerde yer alan bilgi güvenliğinin sağlanması konusu, literatürde yaygın olarak ifade edilen sadece teknik önlemlerin

[4] Bu bölümde "bilgi güvenliği" ifade ile kast edilen unsurlar, McCumber modelinde öngörülen bilginin karakteristik özellikleri, durumu ve güvenlik önlemlerine ilişkin tüm boyutları göz önünde bulunduran kapsamlı bir korumayı içine almaktadır. Konuya ilişkin detaylı bilgiye "2.2.4. McCumber Bilgi Güvenliği Modelinin Unsurları" başlığı altında yer verilmiştir.

alınmasının ötesinde, kişisel verilerin kapsamlı bilgi güvenliği önlemleri çerçevesinde korunarak hukuk dışı kullanımının önüne geçilmesi ve bireyin kendisine ait veriler üzerinde söz sahibi olmasının sağlanmasını da öngörmektedir (Backhouse, Bener, Chauvidul, Wamala ve Willison, 2005). Genel olarak büyük verilerin bulunduğu ortamlara yönelik bilgi güvenliği kapsamında teknik önlemler alınmaktadır. Ancak kurum ve kuruluşlarda bilgi güvenliği politikalarının geliştirilmesi ve farkındalığın arttırılması da, bilgi güvenliği kapsamında yer alan ve kişisel verilerin korunmasında en az teknik önlemler kadar etkili ve gerekli olan unsurlardır (Rhee, Ryu ve Kim, 2005).

Son yirmi yıl içerisinde bilgi işleme ve bilgi yönetimi alanında meydana gelen büyük değişim ve gelişim, McCumber tarafından 1991 yılında geliştirilen ve güncelliğini koruyan kapsamlı bilgi güvenliği modeli üzerinde görülmektedir (Simpson ve Endicott-Popovsky, 2010). Bu süreçte bilgi güvenliğine ilişkin politikalar, hukuksal önlemler ve hassas verileri işleyen personelin yeni yapısal değişikliklere uyum sağlamasına yönelik eğitim programlarında da değişimlerin olduğu görülmektedir. Hassas ve kişisel verilerin korunması da bu daha kapsamlı bilgi güvenliği modeli içinde, tüm etkenlerin (çevresel, kurumsal, hukuksal, personel ve teknoloji) dikkate alındığı bir yaklaşım ile sağlanabilmektedir (Backhouse ve diğerleri., 2005). Bu nedenle, hangi alanın diğer alanı kapsadığına ilişkin tartışmaların uzağında, bilgi güvenliği modeli içindeki tüm etken unsurları dikkate alarak belirlenen bilgi güvenliği politikalarının kurum ve kuruluşlarda kişisel verilerin korunmasına yönelik olarak daha büyük katkı sağlayacağı değerlendirilmektedir.

Kişisel verileri işleyen kurum ve kuruluşların sorumluluklarının belirlenmesinde hukuksal düzenlemeler öncelikli kaynaklar olarak kullanılmaktadır. KVKKT'nın 3. Maddesinde[5] "kişisel verilerin işlenmesi" ile ilgili tanımın, geniş bir alanı kapsadığı ve verilerin elde edilmesinden imha edilmesine kadar olan tüm süreci içine aldığı görülmektedir (T.C. Başbakanlık, 2014a). Bu ifade, üniversite birimleri tarafından kişisel veriler üzerinde bilgi sistemleri aracılığıyla ya da elden yapılan tüm işlemleri

[5] **KVKKT, 3. Madde:** d) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen, otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemdir.

kapsamaktadır. Bu nedenle, üniversitelerde verilerin işlenmesine yönelik olarak izlenen süreç ile McCumber'in bilgi güvenliği tanımında yer alan koruma aşamaları arasında önemli ölçüde yakınlık bulunmaktadır.

ABD'de yapılan araştırmalar (PrivacyRightsClearinghouse, 2014), 2005 yılından itibaren kurum ve şirketlerden 931.357.921 kayıt[6] çalındığını göstermektedir. Veri ihlali konusunda belirlenen hedefler arasında üniversitelerin de bulunduğu görülmektedir. ABD'de yaşayanların %55'ninden fazlasının kişisel verilerinin çalındığı ya da kaybedildiği tahmin edilmektedir (INVISUS, 2014). 2013 yılında meydana gelen en büyük veri ihlalleri incelendiğinde, tüm önlemlere rağmen hassas verilerin bulunduğu alanların ilk sıralarda hedef alınmış olması dikkat çekicidir (Westervelt, 2013). Veri ihlaline ilişkin 95/46/EC sayılı AB veri koruma direktifinin 17. Maddesinde gerekli hukuksal düzenlemelerin yapılmış olduğu görülmektedir. Ancak kullanıcı farkındalığının bulunmaması ve temel bilgi güvenliği standartlarının sağlanmaması nedeniyle AB'de de veri ihlallerinin hızla arttığı görülmektedir (Wong, 2013). AB'nin verilerin korumasına ilişkin hukuksal düzenlemeler üzerinde başlatmış olduğu reform çalışmaları kapsamında hazırlanan yeni veri koruma direktifi taslağında, veri ihlaline yönelik sorumluluklara da yer verilmektedir. Tasarının 31. ve 32. Maddelerinde[7], herhangi bir veri ihlali olması durumunda, veri koruma otoritesine ve veri sahibine karşı bilgilendirmeye ilişkin sorumluluklar belirlenmiştir (Wong, 2013).

2.2.2. Kişisel Verilerin Korunmasına İlişkin Hukuksal Düzenlemeler ile Bilgi Güvenliği Politikası İlişkisi

Hukuksal düzenlemeler, konusu suç teşkil eden fiillerin oluşması karşısında caydırıcı unsur olarak önem taşımakta ve yaptırımların uygulanabilmesi için gereklidir. Ancak hukuksal düzenlemelerin yeterli düzeyde olması durumunda dahi, farkındalığın istenilen seviyede oluşmadığı toplumlarda önleyici unsur olarak bu düzenlemelerin varlığı yeterli değildir. Kişisel verilere yönelik olarak gelişen teknoloji odaklı tehditlere karşı,

[6] Güvenlik ihlaline konu olan yaklaşık kayıt/belge sayısıdır. Bu ihlallerden farklı zamanlarda birkaç defa etkilenen kişiler de bulunmaktadır.
[7] Bkz. (Avrupa Konseyi, 2012)

teknolojinin de kullanıldığı kapsamlı ve farklı boyutlarda önlemlerin alınması zorunludur. Kişisel verilerin korunmasına yönelik olarak alınan teknik önlemler ve kullanıcı bilinçliliğinin arttırılması amacıyla düzenlenen eğitim programları, hukuksal düzenlemeleri tamamlayan ve sürecin ayrılmaz parçaları haline gelen diğer unsurlardır. Ayrıca hassas ve kişisel verilerin hukuksal düzenlemelerle koruma altına alınarak bireylerin korunması önemli olduğu kadar, teknik önlemlerin alınması suretiyle de bireylerin korunması aynı derecede önemlidir. Doğası gereği veri ihlalleri de veri koruma düzenlemelerinin bir parçası olarak düşünülmektedir (Wong, 2013). Bilgi güvenliği kapsamında alınan koruma tedbirlerinin sadece verileri korumayı öngördüğü algısı değişerek, bu kapsamda yer alan eğitim programları ve denetim kontrol listelerine kişisel verilerin korunması konusunun da eklendiği görülmektedir (Ottekin, 2008). Son yıllarda hazırlanan AB bilgi toplumu stratejileri ve daha önce hazırlanan stratejilere yönelik yenileme projelerinde bilgi güvenliği ve kişisel bilgilerin korunması konularının aynı başlık altında toplanarak bir bütün halinde çözüm önerileri öne sürülmesi bu açıdan dikkat çekicidir. Bu rapor ve projelerde hukuksal düzenlemelerin yanı sıra, bilgi güvenliğinin bir unsuru olan bilinçlendirme çalışmalarının önemine de vurgu yapılmaktadır (T.C. Kalkınma Bakanlığı, 2013). Bu unsurların ele alındığı ve uygulanacak politikaların geliştirildiği ortak zemin olarak, bilgi güvenliğinin sağlanması amacıyla geliştirilen modellerden faydalanılmaktadır.

Bilgi güvenliği modellerinin ortaya koyduğu çok yönlü çözüm önerileri ile hukuksal düzenlemeler arasındaki etkileşim AB dışında da görülmektedir. Bu çalışmada temel olarak alınan McCumber bilgi güvenliği modelindeki gizliliğin korunması ile kişisel verilerin korunması kapsamındaki özel hayatın gizliliğinin korunması arasındaki ilişki, ABD Teknoloji ve Standartları Ulusal Enstitüsü'nün (NIST) bilgi güvenliği konusunda hazırlamış olduğu belgelerde de benzer şekilde yer almaktadır. NIST tarafından yayınlanan bilgi güvenliği belgesinde bilgi güvenliği; bilgi ve bilgi sistemlerinin gizlilik, bütünlük ve erişilebilirliğinin, yetkisiz erişim, kullanım, açığa çıkarma, bozulma, değiştirme ve yok edilmeye karşı korunması şeklinde tanımlanmıştır (Barker 2003). Bilgi güvenliği konulu bu belgede ve NIST tarafından hazırlanan "Bilgi teknolojileri için risk yönetimi" isimli rehberde (Stoneburner, Goguen ve Feringa, 2002) bilgi sistemlerinin

ulusal güvenlik sistemi çerçevesinde tanımı ve alınacak güvenlik önlemleri, hukuksal düzenlemelere atıfta bulunularak ele alınmıştır.

2.2.3. McCumber Bilgi Güvenliği Modelinin Kapsamı ve Diğer Bilgi Güvenliği Modellerinden Farklılığı

1994 yılında ABD Milli Güvenlik Sistemleri Komitesi (CNSS)[8] tarafından yayınlanan "Bilgi Sistemleri Güvenliği Profesyonelleri İçin Ulusal Eğitim Standartları (NSTISSI No. 4011)" dokümanı (NSTISSI, 1994), bilgi güvenliğine ilişkin temel kaynak olarak kullanılan ve bilgi sistemlerinin güvenliğinde değerlendirme standardı olarak geniş kabul gören bir dokümandır (Whitman ve Mattord, 2011). Bu dokümanda sunulan kapsamlı bilgi güvenliği modeli, 1991 yılında McCumber tarafından geliştirilen ve bilgi güvenliği sistemlerine mimari yaklaşımı grafiksel olarak gösteren bilgi güvenliği modelidir. McCumber modeli, politika geliştiricilerin derin teknoloji bilgi birikimi olmaksızın da faydalanabileceği detaylı ve çok yönlü bir modeldir. McCumber modeli ile herhangi bir kurum ya da kuruluş için kapsamlı bilgi güvenliği politikası ya da bilgi güvenliği rehberinin geliştirilmesi mümkündür (McCumber, 2005). Bu bilgi güvenliği değerlendirme ve uygulama metodolojisi, tüm bilgi sistemlerine uygulanabilir ve teknolojinin hızlı değişiminden etkilenmeyecek niteliktedir. McCumber bilgi güvenliği modeli, 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 toplayan modellerden biridir. McCumber modeli bilgi sistemlerinin güvenliğini üç boyut üzerinde 27 hücre ile adreslemektedir. Örneğin teknoloji, bütünlük ve bilginin depolanması unsurlarının kesiştiği nokta, bilginin depolanması esnasında bütünlüğünün sağlanması için gerekli olan teknolojik önlemleri ifade etmektedir (Whitman ve Mattord, 2011). Bilgi güvenliğinin unsurlarını üç farklı boyut üzerinde gösteren ve kendi içinde ilişkilendiren bu model, 1991 yılından itibaren geçerliliğini korumuş ve daha sonra geliştirilen modeller

[8] "NSTISSI No. 4011" isimli dokümanın yayınlandığı 1994 yılında Komitenin ismi NSTISSC (National Security Telecommunications and Information Systems Security) iken, daha sonra CNSS (Committee on National Security Systems) olarak değişmiştir.

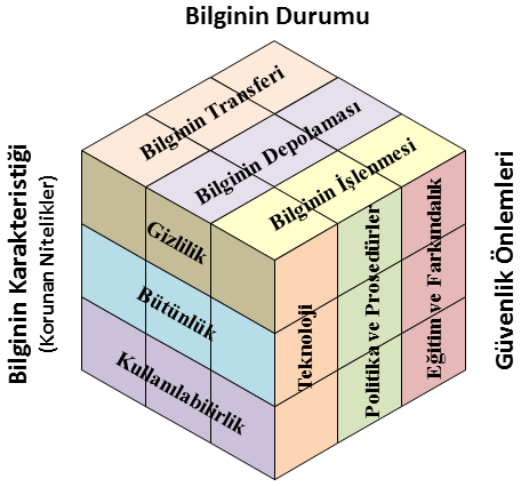
için önemli bir kaynak haline gelmiştir. Bilgi güvenliğinin sağlanmasına ilişkin standartların belirlenmesine öncülük eden kuruluşların da (CISCO, 2009) eğitim programlarında McCumber modelinin yer aldığı görülmektedir.

Literatürde yer alan diğer (CIA-triad vb.) bilgi güvenliği modellerinden farklı olarak McCumber bilgi güvenliği modeli, risk yönetimi temelli bakış açısıyla, kişisel verilerin korunmasının 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 modeldir. Bilgi güvenliği kapsamında alınan önlemler ile hukuksal düzenlemeler ve politikalar arasındaki ilişki, McCumber bilgi güvenliği modeli üzerinde daha açık ve anlaşılır biçimde görülmektedir. Güvenlik önlemleri içindeki çok yönlü bakış açısı, veri sahibine kendisine ait kişisel bilgilerin kontrolünü sağlama ve bu verilerin geleceğini belirleme konusunda geniş inisiyatif kullanma olanağı sunmaktadır. McCumber bilgi güvenliği modeli, güvenlik önlemleri kapsamında teknik önlemlerin alınmasının yanı sıra, politikaların geliştirilmesi ve alınan tüm güvenlik önlemleri hakkında kullanıcıların bilgilendirilerek farkındalığın oluşturulmasını da kapsamaktadır.

Hukuksal düzenlemeler ile alınacak güvenlik önlemlerinin ilişkilendirilmesinde yaşanan zorluklar, bilgi güvenliğinin sağlanmasına ilişkin tüm unsurların uygulanamamasına neden olabilmektedir. McCumber modeli bilgi güvenliğinin sağlanmasına etki eden tüm unsurları tek çatı altında toplayarak, bilginin korunmasına yönelik alınması gereken stratejik kararlara önemli bir dayanak oluşturabilecek ve katkı sağlayacak niteliktedir.

2.2.4. McCumber Bilgi Güvenliği Modelinin Unsurları

McCumber, bilginin karakteristiği, bilginin durumu ve güvenlik önlemlerinden oluşan üç farklı unsuru, bilgi güvenliğine ilişkin küp modeli üzerinde Şekil 1'de (McCumber, 2005) görüldüğü gibi alt unsurlarıyla birlikte gruplandırarak göstermektedir. McCumber bilgi güvenliği modelini oluşturan unsurlar, otomatik olsun ya da olmasın bilgi sistemleri üzerinde işlenen tüm bilgilerin güvenliğini kapsayacak şekilde tasarlanmıştır.



Şekil 1 McCumber Bilgi Güvenliği Modeli

2.2.4.1. Bilginin Karakteristiği / Korunan Nitelikleri

McCumber 1991 yılında geliştirmiş olduğu modelde, bilginin gizliliği, bütünlüğü ve kullanılabilirliğini "bilginin karakteristiği" grubu altında sınıflandırmış ve bilgi güvenliği bileşenlerini bu üç unsur üzerinden tanımlamıştır. Literatürde bu üç unsurun "bilgi güvenliğinin prensipleri" adı altında genişletilerek yeni unsurların (inkâr edememe ve kimlik doğrulama gibi) eklendiği görülmektedir. Ancak McCumber'in 2005 yılında yapmış olduğu değerlendirmede de ifade ettiği gibi, bu yeni unsurlar bilgi bütünlüğü kapsamı içerisinde yer almakta ve gerçekte yeni bir karakteristik özellik taşımamaktadır (McCumber, 2005). Bilginin karakteristiğine yönelik olarak McCumber modelinin bu haliyle güncel ve kapsamlı olduğunun en önemli göstergesi, bilgi güvenliğine ilişkin olarak kabul edilen diğer önemli modellerin de bu üç unsur üzerine kurulmuş olmasıdır (Solomon ve Chapple, 2005).

Bilginin gizliliği, var olan bilginin içeriğine erişim yetkisi bulunan kişilerin haricindeki erişimlerin ve bilginin ifşa olmasının engellenmesini ifade etmektedir. Yetkisiz erişimlere karşı korunan verilerin hassas ve kişisel veriler olması halinde, bilginin gizlilik değeri de artmaktadır. Organizasyon dışına gönderilen e-postalar ve kullanım süresi sonunda doğru yöntemlerle imha edilmeyen dokümanlar gizliliğin ihlalinde en sık karşılaşılan zafiyetlerdir (Whitman ve Mattord, 2011). McCumber modelinde bilginin depolanması

ve transferi esnasında gizliliğinin korunması amacıyla en etkin koruma yöntemi olarak kripto kullanımı önerilmektedir. Veriler kötü amaçlı kişilerin eline geçse dahi gizliliğinin korunması sağlanmalıdır. Çünkü hassas ve kişisel verilerin açık hale gelmesi, bu bilgilerin korunmasına yönelik olarak istenmeyen en kötü durumdur. Bu nedenle McCumber bilgi gizliliğinin sağlanmasını, bilgi sistemleri için belirlenen güvenlik politikalarının kalbi olarak nitelendirmektedir (McCumber, 2005). Bunun yanı sıra, verilerin bulunduğu merkezi sistem üzerinden yapılan yetkilendirmeler ve güçlü şifrelerin kullanımı da depolanan veriler için kullanılan yaygın koruma yöntemleridir. Kişisel verilerin ve kişilik haklarının korunması, bilginin gizliliğinin korunması ile yakın ilişkili konulardır (Whitman ve Mattord, 2011). Çoğu zaman kişisel verileri ve buna ilişkin kişilik haklarının korunmasına yönelik olarak, öncelikle bilginin gizliliğinin korunmasını amaçlayan bilgi güvenliği yöntemlerine başvurulduğu da görülmektedir.

Bilginin bütünlüğü, elektronik veri depolama ortamlarında bulunan bilgilerin ilk işlendiği andaki orijinal halinin muhafaza edilmesi, yetkisiz erişim sonucunda ya da yetkili olarak istem dışı değiştirilmesi veya silinmesine karşı korunmasıdır. Bilginin bütünlüğü ile ifade edilen bilginin karakteristik özelliği, doğruluk, ilgili olma ve tam olma anlamlarını da kapsamlı olarak içermektedir. Bilgi bütünlüğünün sağlanması, bilginin önceden sınıflandırılarak belirlenmiş olan değerinin korunması anlamına gelmektedir. Bilgi bütünlüğü, yetkisiz erişimlerle kasıtlı olarak ya da sistem hataları nedeniyle kullanıcılar tarafından istemeden de bozulabilmektedir. Hassas ve kişisel verilerin korunmasında, yetkisiz erişimler ya da veri transferi esnasında araya girme sonucunda kötü amaçlı olarak elde edilmiş olan verilerin bütünlüğünün sağlanması önem taşımaktadır. Bunun için en etkili koruma yöntemi olarak veri kriptolama yöntemi kullanılmaktadır. McCumber, kripto çözümleri, karşılaştırmalı analiz, inkâr edememe, kimlik doğrulama ve erişim kontrolü süreçlerini "bilgi bütünlüğü" içinde değerlendirmektedir (McCumber, 2005). Kapsamının geniş olması nedeniyle, verinin korunan nitelikleri arasında bilgi bütünlüğünün sağlanmasının maliyeti diğer niteliklerin korunmasından daha yüksektir. Bu konuda dikkate alınması gereken diğer nokta, var olan bilginin bütünlüğünün sağlanması için kullanılan kimlik doğrulama araçlarının da (kullanıcı adı, şifre, parmak izi vd.) kişisel veriler kapsamında sistem yöneticileri tarafından korunmasının gerekli olmasıdır.

Bilginin kullanılabilirliği, bilgiye erişim yetkisi bulunan kullanıcıların istediği zaman ihtiyacı olan bilgiye tanımlanan erişim yetkileri kapsamında ulaşabilmesi ve kullanabilmesidir. Bilginin kullanılabilirliği, erişim kolaylığının ve sürekliliğinin sağlanması süreçlerini karşılayacak şekilde ifade edilmektedir. Belirli bir bilgiye erişim ya da kullanım için yetkilendirilmiş kullanıcıya ihtiyaç duyduğu bilginin sağlanması süreci, bilginin kullanılabilir olması ile ifade edilen süreçtir. Bilgi güvenliği modeli üzerinde güvenlik ve kullanılabilirlik için alınan önlemlerin etkileri ters yönlü olabilmektedir. Bu nedenle risk yönetimine bağlı olarak denge sağlanmalı ve uygulanan güvenlik önlemleri bilgiye erişimi gereğinden fazla zorlaştırmamalıdır. Bilginin sürekliliğinin sağlanması konusunda, veri ve sistem yedekliliğinin sağlanması için yapılan işlemler öne çıkmaktadır. Güvenlik önlemleri yeterli olmadığı için veri ihlali ile karşılaşılması durumunda, hukuksal işlemlerle birlikte bilginin kullanılabilirliğine yönelik olarak belirlenen politikaların uygulanması gerekmektedir (McCumber, 2005). Üniversitelerde kişisel verilerin bulunduğu veri depolama alanlarına erişim sürekliliğinin sağlanması, günlük işlemlerin takibi açısından önemlidir. Bu nedenle, kişisel verilerin bulunduğu veri depolama alanlarından sorumlu birimlerin, veri ve sistem yedekliliğini sağlama sorumlulukları da bulunmaktadır. Herhangi bir kötü amaçlı girişim sonrasında meydana gelen hizmet kesintilerinin en kısa zamanda giderilerek verilerin en son güncel haliyle yeniden kullanılabilir hale getirilebilmesi için, önceden belirlenen bilgi güvenliği politikası kapsamında belirli aralıklarla yedekleri oluşturulmalıdır. Söz konusu bilgi güvenliği politikalarının oluşturulmasında ise, kişisel verilerin saklanmasına ilişkin hukuksal düzenlemelerin göz önünde bulundurulması, konunun özel durumu açısından önemlidir.

2.2.4.2. Bilginin Durumu

McCumber modelinde yapılan sınıflandırma dikkate alındığında, kişisel verilerin bilgi sistemleri üzerinde üç farlı şekilde bulunduğu görülmektedir. Bunlar; bilginin depolanması, transferi ve işlenmesidir. Buna göre kişisel veriler, bir bilgi sistemi üzerinde bu üç durumdan bir ya da birkaçının özelliğini taşıyarak bulunmaktadır. Öncelikli ve üst seviyede korunması gereken veri gurubu içinde yer alan hassas ve kişisel veriler, risk

yönetimine ilişkin koşullar göz önüne alınarak değerlendirilmekte ve sınıflandırılmaktadır. Bilginin değerinin belirlenmesi işlemlerinin ve daha geniş kapsamda risk yönetiminin yapılması için, bilginin durumunun göz önüne alınması gerekmektedir.

Bilginin işlenmesi sürecinde öncelikli olarak personel güvenliği göz önünde bulundurulurken, transfer sürecinde ağ güvenliği ve transfer edilen bilginin bir kopyasının bulunduğu veri depolama ortamına ilişkin olarak fiziksel güvenliğin sağlanması öne çıkabilmektedir. Depolanan ya da transfer edilen verilerin korunması için kriptolama yönteminin kullanılması en etkili güvenlik önlemlerinden biridir (Indiana University, 2012; McCumber, 2005).

2.2.4.3. Güvenlik Önlemleri

McCumber bilgi güvenliği modeli üzerinde bilginin durumuna bağlı olarak karakteristik özelliğinin korunması noktasında, güvenlik önlemleri tamamlayıcı unsur olarak kullanılmaktadır. McCumber modelini literatürde yer alan diğer modellerden farklı ve üstün hale getiren en önemli özelliği, bilgi güvenliğinin sağlanmasına ilişkin olarak McCumber küpünün üç farklı yüzünde yer alan unsurların, kesişen noktalarda aynı anda eksiksiz olarak uygulanabilmesidir. Yaygın olarak bilinen bilginin karakteristik özelliklerinin korunması ile birlikte bilginin durumu ve alınacak olan güvenlik önlemlerinin de aynı anda değerlendirilmesi, kişisel verilerin korunması konusunda tüm koşulları içeren daha etkin bir korumanın gerçekleşmesine katkı sağlamaktadır.

Bilgi güvenliği önlemleri kapsamında uygulamada yaygın olarak başvurulan yöntem, bilginin karakteristik özelliklerinin teknik önlemler ile korunmasıdır. McCumber modelinde ise teknik önlemler, alınacak diğer önlemlerin bir bileşeni olarak görülmektedir. Bilgi ve bilgi sistemlerine yönelik tehditlerin gelişen ve değişen koşulları göz önüne alındığında, her ne kadar yapılan yatırım miktarı arttırılsa da sadece teknik önlemlerin alınması ile bilgi güvenliğinin ihlallerinin sonlandırılmasının mümkün olmadığı görülebilmektedir (Charette, 2012a, 2012b). Ancak alınacak olan teknik önlemlerin de tehditlere bağlı olarak kendi içindeki gelişimi göz önünde alındığında,

model içerisinde kapsamlı bir alanı oluşturduğu söylenebilir. Teknik önlemler, bilgi güvenliği politikaları ve hukuksal düzenlemeler çerçevesinde, bilginin durumuna bağlı olarak uygulanan tüm donanımsal ve yazılımsal önlemlerdir. Biyometrik aygıtlar, kripto modülleri ve güvenliği arttırılmış işletim sistemi kullanımı, bu kapsamda yaygın olarak başvurulan teknik önlemlerdir (McCumber, 2005).

Bilgi erişimine yönelik olarak kurum ve kuruluşlarda güvenlik yetkilerin düzenlenmesi de teknik önlemler kapsamında değerlendirilmektedir. Erişim yetkilerinin düzenlenmesi, kişisel verilerin korunmasına ilişkin olarak AB hukuk sisteminin üzerinde önemle durduğu konulardan biridir. Veri sahibinin kendisine ait kişisel verilere erişim hakkının bulunması ve diğer yetkisiz erişimlere karşı bu verilerin korunması, erişim yetkilerinin düzenlenmesi ile sağlanmaktadır. Kurum ve kuruluşlarda erişim yetkilendirmeleri bilgi işlem merkezlerinin ve sistem yöneticilerinin sorumluluğu altında yapılmaktadır. Veri gizliliğinin korunması kapsamında da değerlendirilen bu yetkilendirmeler yapılırken; genel olarak veriye erişen ya da işleyen personele ihtiyacı olan en düşük yetkinin "bilmesi gereken" (need to know)[9] prensibine bağlı olarak verilmesi amaçlanmaktadır.

McCumber modelinin güvenlik önlemleri içerisinde yer alan "politikaların belirlenmesi" unsuru, kişisel verilerin ve buna bağlı olarak kişilik haklarının korunmasına ilişkin olarak model içinde tanımlanan en kapsamlı güvenlik önlemidir. Kurum içi kullanıcı şifre politikalarının belirlenmesinden bilgi güvenliği politikalarının oluşturulması için temel kaynak olarak hukuksal düzenlemelerin kullanılmasına kadar tüm süreç ve işlemler bu kapsamda değerlendirilmektedir. Bilgi güvenliği politikalarının belirlenmesi, bilginin durumuna bağlı olarak doğru ve güvenilir teknik önlemlerin uygulanmasının yanı sıra, hukuksal düzenlemelerle uyumlu işlemlerin yapılmasına katkı sağlamaktadır. Ayrıca, hukuksal düzenlemelerdeki eksikliklere ilişkin olarak benimsenen etik değerlerin (TKD, 2010) uygulamaya dönüştürülmesinde de yazılı bilgi güvenliği politikaları önemli bir araç olarak kullanılabilmektedir. Yazılı bilgi politikalarının geliştirilmesi ve yayınlanması sonrasında, bu politikaların uygulanması ile ilgili takip ve kontrolün de yapılması önem taşımaktadır (Fowler, Kling ve Larson, 2007). Kurum, kuruluş ya da üniversitelerde

[9] Bkz. http://www.cdse.edu/multimedia/need-to-know/need_to_know.pdf

kişisel verileri işleyen birimlerde çalışan personel, hazırlanmış olan bilgi güvenliği politikaları hakkında bilgilendirilmeli ve bu politikaları uygulamaları sağlanmalıdır.

İnsan faktörü ve ona bağlı olarak uygulanan bilgi güvenliği politikaları da bilgi güvenliğinin sağlanmasında bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması kadar büyük öneme sahiptir. Bilgi güvenliğinin sağlanmasına ilişkin olarak bilgi güvenliği profesyonelleri, zincirin en zayıf halkasının kullanıcı olduğu düşüncesinde birleşmektedirler (Chirillo ve Danielyan, 2005; Mitnick ve Simon, 2002; Sasse, Brostoff ve Weirich, 2001). Güvenlik önlemlerini oluşturan unsurlardan biri olan insan faktörünün dikkate alınmaması halinde, diğer unsurların uygulanması yetersiz kalabilmektedir. Teknik yöntem ve imkânlarla en iyi korunan sistemlerden dahi en etkili saldırı yöntemlerinden biri olan sosyal mühendislik ile korunan bilgilere kolaylıkla ulaşım sağlanabilmektedir (Mitnick ve Simon, 2002). Bu noktada eğitim ve farkındalığın koruma önlemleri içindeki ağırlığı öne çıkmaktadır. McCumber'a göre eğitim ve farkındalık, alınabilecek en önemli güvenlik önlemleridir (McCumber, 2005). Kişisel verilerin korunması için alınacak güvenlik önlemlerinin önemli unsurlarından biri olan eğitim ve farkındalık, birbirinin devamı olarak değerlendirilmelidir. Farkındalık, pasif bir süreci ifade etmekte ve kullanıcıların kısa süreli karar verme işlemleri esnasında konuya en doğru şekilde odaklanmalarını sağlamaktadır. Ancak farkındalığın oluşması, ne tür bilgi güvenliği önlemlerinin alınacağı ya da hangi yasal düzenlemelerin dikkate alınacağı konusunda kullanıcıların yeterli düzeyde bilgi sahibi oldukları anlamına gelmemektedir. Bunun için, aktif katılım sürecini de kapsayan eğitimin verilmesi gerekmektedir (Maconachy, Schou, Ragsdale ve Welch, 2001). Bilgi güvenliği konusunda verilecek eğitimlerle, daha önce hukuksal düzenlemelerin de dikkate alınarak belirlendiği bilgi güvenliği politikalarının nasıl uygulanacağı konusunda kullanıcılara uygulama becerileri de kazandırılabilmektedir.

Bilgi güvenliği bilinci konusunun kesin bir tanımı bulunmadığı için, bilgi güvenliği farkındalığının etkinliğine yönelik olarak yapılan ölçümlerin çoğu zaman yetersiz kaldığı görülmektedir. Buna bağlı olarak, birçok çalışmada farkındalık eğitimleri ile güvenlik politikalarına uyum sağlanması arasında ilgileşim olmadığı sonucuna ulaşılmıştır (Decker, 2011). Yapılan araştırmalarda geniş anketler ile kullanıcıların bilgi güvenliği

konusundaki farkındalıkları ölçülmeye çalışılmıştır. Ancak elde edilen sonuçlar, anket uygulanan kullanıcıların konu hakkındaki bilgi düzeylerini göstermektedir. Bilgi güvenliği davranışlarının ya da diğer ifadeyle uygulamadaki farkındalığın ölçülebilmesi için, öncelikle bilgi güvenliği bilincinin tanımının yapılması gerekmektedir. Literatürde birçok örneği görülebileceği gibi, McCumber da eğitim ve farkındalık konularının en önemli güvenlik önlemleri olabileceğini belirtmesine rağmen farkındalığın tanımını yapmamış ve bir organizasyonu nasıl etkileyebileceğine değinmemiştir. (Wolf, Haworth ve Pietron, 2011). Farkındalığın ölçülmesi öncesinde tanımlamanın yapılması ya da başka bir deyişle farkındalığın hangi unsurunun (haberdar/bilgi sahibi olma ya da davranış üzerindeki etkisi) ölçüleceğinin belirlenmesi, araştırma ve bilgi güvenliği politikalarının geliştirilmesinde istenilen hedefe ulaşma olasılığını etkilemektedir. Ayrıca, uygulamadaki farkındalığın ölçülmesinin amaçlandığı çalışmalarda, soruların yöneltildiği personelin yetkileri, sorumlulukları ve içinde bulunulan çalışma şartları da dikkate alınmalıdır. Örneğin bir bilgi merkezinde çalışan bilgi profesyonelinin bilgi güvenliğine ilişkin bilgi düzeyi yüksek olmasına rağmen, sistem üzerindeki yetkilerinin ve sorumluluğunun (güncel olmayan anti virüs programı gibi) kısıtlı olması nedeniyle sahip olduğu bilgiyi uygulamaya dönüştürememesi söz konusu olabilmektedir. Diğer taraftan, sistem yöneticisi tarafından uygulanan şifre politikaları gibi zorunlu güvenlik önlemleri de farkındalığın ölçülmesinde dikkate alınması gereken unsurlardır.

Farkındalığın iki önemli unsuru bulunmaktadır. Bunlar, tehditler ve bu tehditlere karşı alınacak önlemlere ilişkin olarak bireylere belirlenen politikalar hakkında doğru ve güncel bilginin verilmesi ve bu politikalarla bireylerin davranışlarında değişiklik yaratılmasıdır. Bu iki unsurdan birinin gerçekleşmemesi halinde diğerinin de etkili olması beklenmemelidir. Bununla birlikte bilgi güvenliği davranışını ölçmeye yönelik olarak yapılan araştırmaların sonuçları, kullanıcıları mümkün olduğunca teknik yöntemler de kullanılarak uyum sağlamaya zorlamanın, belirlenen güvenlik politikalarının uygulamaya dönüşmesinde en etkili yöntem olduğunu göstermektedir (Wolf ve diğerleri., 2011). Bu araştırma sonuçlarının tüm kurum ve kuruluşlar için genellenebilirliği tartışılabilir. Çünkü uygulanan araştırma yöntemine bağlı olarak, her kurum ve kuruluşta farkındalığın davranışa dönüşümü konusunda farklı sonuçlarla karşılaşma olasılığı bulunmaktadır. Ancak farkındalığın ölçülmesinin amaçlandığı bu tür araştırmalarda, bireylerin konuya

ilişkin bilgi seviyelerinin ölçülmesinin ötesinde bilgi güvenliği davranışının ölçülmesinin odak noktası olması önemlidir.

2.3. AB HUKUK MEVZUATINDA KİŞİSEL VE HASSAS VERİLERİN KORUNMASI

Hukuksal düzenlemeler çerçevesinde üniversitelerde kişisel verilerin korunmasına yönelik uygulamalar incelenirken, kişisel verilerin korunmasına ilişkin olarak yapılan hukuksal düzenlemelerin, AB uyumluluk süreci içinde AB hukuku dikkate alınarak yapıldığı göz önünde bulundurulmalıdır. AB'nin kişisel verilerin korunmasına yönelik yaklaşımı irdelenerek, Türkiye'de bu konuya ilişkin alınan kararlar, yapılan hukuksal düzenlemelerin gerekçeleri ve hedeflenen koruma düzeyi daha iyi anlaşılabilmektedir. AB için konunun özünde neler bulunduğu ve kişisel verilerin korunmasına yönelik olarak yapılan hukuksal düzenlemelerde AB hukukuna ne kadar uyum sağlanabildiğinin değerlendirilebilmesi için, AB hukukunda kişisel verilerin korunması konusu da bu çalışma kapsamına alınmıştır.

2.3.1. AB Hukuku ile Ulusal Hukuk İlişkisi ve AB'de Kişisel ve Hassas Verilerin Korunması Süreci

AB hukuku, uluslararası özellik gösteren bir hukuk sistemidir. Bu sistemin oluşmasını sağlayan AB antlaşmaları; AB kurumları ve üye devletler için anayasal nitelikte ve hiyerarşik olarak en üst seviyede normlardır. Bu nedenle üye ülkelerin vatandaşları da bu hukuk sisteminin özneleri haline gelmekte ve buradan elde ettikleri haklarını ulusal mahkemelerde de öne sürebilmektedirler. AB hukukunun uygulanmasından üye ülkelerin ulusal idare ve yargı organları sorumludur (T.C. AB Bakanlığı, 2013). AB Antlaşması'nın 4/3. Maddesi gereğince, ulusal makamlar AB hukuk düzeninden kaynaklanan yükümlülüğün yerine getirilmesi için her türlü tedbiri almak zorundadırlar (T.C. Başbakanlık, 2011). Avrupa Birliği Adalet Divanı'nın[10] (ABAD) yargı yetkileri sınırlı

[10] **Avrupa Birliği Adalet Divanı (ABAD):** AB hukukunu ilgilendiren konularda son sözü söyleyen en yüksek mahkemedir. AB üyesi ülke mahkemelerinin üst kuruma sevk ettiği uyuşmazlıklar ve temyiz davalarına bakar.

olduğu için, AB Antlaşması'nın 274. Maddesinde[11] de belirtildiği gibi, bireyler arasındaki AB hukukundan kaynaklanan uyuşmazlıkların çözüm yeri de ulusal yargı organlarıdır. Ancak AB hukuku ile ulusal hukuk arasındaki ihtilafın nasıl giderileceğine dair ilkelerin bulunduğu bir AB yazılı metni bulunmamaktadır. Ülkelerin ekonomik, siyasi ya da toplumsal çıkarları nedeniyle AB hukuku ile uyumsuz hukuksal düzenlemeleri yapmaları sonucunda oluşan ihtilaflar, kurucu anlaşmaların özünde yer alan "AB hukukunun birliği" ilkesine bağlı kalarak geliştirdiği ilkeler doğrultusunda ABAD tarafından çözülmektedir. Bu ilkelere bağlı olarak; AB hukuku ile ulusal hukuk kuralları arasında çatışma olduğunda, ABAD içtihatlarında AB hukukunun üstün ve öncelikli olarak değerlendirildiği görülmektedir. AB hukukunun önceliği ilkesi, Lizbon Antlaşması'na eklenen 17 nolu bildiride de yer almaktadır. Bu nedenle üye ülkeler AB hukuk kurallarına aykırı düzenlemeler yapmamalı ve çatışma halinde ulusal mahkemeler bireysel haklara ilişkin kararlar verirken AB hukuk kurallarına öncelik vermelidirler (T.C. AB Bakanlığı, 2013).

Bireyler "doğrudan[12]" ya da "dolaylı[13]" olarak AB hukukundan etkilenmektedirler. AB antlaşma, tüzük ve karar hükümleri dikey[14] ve yatay[15] olarak doğrudan etkili olabilirken; direktif hükümleri sadece dikey doğrudan etkili olabilmektedir. Doğrudan etki, bireyleri AB ile çelişen ulusal hukuk kurallarına karşı da korumaktadır. Direktiflerin uygulanabilmesi için ulusal hukuk düzenlemelerine ihtiyaç duyulmakta ve iç hukuka aktarılması öngörülmektedir (T.C. AB Bakanlığı, 2013). Direktiflerin iç hukuka aktarılması yükümlülüğü yerine getirilmediğinde, üye devlete karşı ulusal mahkemelerde hak öne sürülebilmektedir.

Avrupa'da gizlilik haklarına ilişkin ilgi, bilgi teknolojilerindeki gelişime bağlı olarak 1960 ve 1970'li yıllarında artmaya başlamıştır. Bu konudaki ilk hukuksal düzenleme 1970 yılında Almanya'da yapılmıştır. 1973 yılında İsveç, 1974 yılında ABD ve 1978

[11] **AB Antlaşması, 274. Madde:** Avrupa Birliği Adalet Divanı'na Antlaşmalar'la verilen yetkiler saklı kalmak kaydıyla, Birliğin taraf olduğu uyuşmazlıklar, bu gerekçeyle ulusal mahkemelerin yetkisi dışında bırakılamaz.
[12] **Doğrudan Etki:** Hak ve yükümlülüklerinin AB Antlaşmaları ya da ikincil mevzuattan kaynaklandığı etki.
[13] **Dolaylı Etki:** Hak ve yükümlülüklerin üye ülkenin AB hukuku uygulama sorumluluğunu yerine getirirken yaptığı ulusal düzenlemeden kaynaklanan etki.
[14] **Dikey Doğrudan Etki:** Bir hakkın bireyler tarafından üye ülkelere karşı ulusal mahkemede ileri sürülebilmesi.
[15] **Yatay Doğrudan Etki:** Bir hakkın bireyler tarafından diğer bireylere karşı ulusal mahkemede ileri sürülebilmesi.

yılında Fransa'da yapılan yasal düzenlemelerle bu alandaki modern mevzuat oluşmuştur. 1981 yılında Avrupa Konseyi tarafından hazırlanan veri korumaya ilişkin ilk uluslararası hukuksal düzenleme olan "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması"na ilişkin 108 sayılı sözleşme ve Ekonomik İşbirliği ve Kalkınma Teşkilatı'nın (OECD[16]) yayınlamış olduğu "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Transferine İlişkin Rehber İlkeler" de daha öncesinde oluşan bu hukuksal düzenlemelerden doğmuştur (Privacy International, 2013). AB'de kişisel verilerin korunmasına yönelik ilk hukuksal düzenlemeler, 28 Ocak 1981 tarihli 108 sayılı sözleşme ve 95/46/EC sayılı "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Direktifidir". AB'nin 2000'li yılların başından itibaren kişisel verilerin korunması konusunda alınan önlemleri sınır ötesi veri akışını da kapsayacak şekilde genişlettiği ve ticari ilişkilerin yoğun olduğu ülkelerle anlaşmalar yaptığı görülmektedir. Kişisel verilerin korunması temel haklar kapsamında da 2000 yılından itibaren AB hukukunda yer almaktadır. Temel hakların korunması amacıyla hazırlanan AB Temel Haklar Şartı ve Avrupa İnsan Hakları Sözleşmesi (AİHS), kişisel verilerin korunması ile ilgili olarak da başvurulan başlıca kaynaklar arasında yer almaktadır.

AB bilgi politikalarının temel amacı, toplumu bilgi ile buluşturmayı sağlayacak yol ve yöntemlerin geliştirilmesidir. Bunun için, bilgi kaynakları, bilgi sistemleri, bilgi altyapısı ve bilgi hizmetlerine ilişkin tüm alanlarda iyileştirme çalışmalarına hız kazandırılmıştır. Özellikle çevrimiçi ekonominin canlandırılması ihtiyacı, bu öncelikli hedefin belirlenmesinde en önemli etkendir. Ancak toplum içinde e-ticaret işlemleri için internet siteleri üzerinden şirketlere sunulan kişisel verilerin korunmasına ilişkin kaygıların artması, 1990'lı yıllardan itibaren bilgi politikaları içinde kişisel verilerin korunmasına yönelik çalışmaların da hızlanmasına neden olmuştur. Veri koruma direktifleri, tavsiye kararları, uluslararası sözleşmeler ve denetimi sağlamak amacıyla kurulan yeni kuruluşlar, bilgi politikalarının geliştirilmesi kapsamında yapılan çalışmalar arasında yer almaktadır (Henkoğlu ve Yılmaz, 2013). AB'de hukuksal düzenlemelerin yanı sıra, bilgi güvenliği kapsamında bir dizi önlemlerin alınması ve ülkeler arasındaki koordinasyonu sağlayan güvenlik kuruluşları da kurularak kişisel hak ve özgürlüğün tüm yönleriyle

[16] **OECD (Organisation for Economic Co-operation and Development / Ekonomik İşbirliği ve Kalkınma Teşkilatı):** 1960 yılında kurulan uluslararası ekonomi örgütüdür. 34 üye ülkenin 30'u yüksek gelirli ülkelerdir. Türkiye 1961 yılında OECD ülkeleri arasına katılmıştır.

sağlanması hedeflenmektedir. Kişisel hak ve özgürlüğün hukuksal düzenlemeler ve bilgi güvenliği konusunda alınacak etkin önlemlerle korunmasıyla, bireylerin e-ticarete olan güveninin artacağı ve böylece çevrimiçi ekonominin canlanacağı düşünülmektedir.

2.3.2. Avrupa İnsan Hakları Sözleşmesi ve Temel Haklar Şartı Çerçevesinde Kişisel ve Hassas Verilerin Korunması

7 Aralık 2000 tarihli AB Temel Haklar Şartı, 1 Aralık 2009 tarihinde yürürlüğe giren Lizbon antlaşmasıyla, AB antlaşmalarıyla eşit hukuksal statü kazanmıştır[17][18]. AB Hukukunda temel hakların korunmasına ilişkin başlıca kaynaklar, AB hukukunun genel ilkeleri ve AB Temel Haklar Şartı'dır. Bu kaynakların korunan temel haklar açısından AB için önemi, AB Antlaşması'nın 6. Maddesinde açıklanmaktadır. Anlaşmanın 6. Maddesinin ilk paragrafında, AB Temel Haklar Şartı'nda yer alan hakların, özgürlüklerin ve ilkelerin AB tarafından tanındığı ifade edilmektedir. Anlaşmanın 6. Maddesinin son paragrafında ise, AİHS ile güvence altına alınan temel hakların, AB hukukunun genel ilkelerinin parçası olduğu ifade edilmektedir (T.C. AB Bakanlığı, 2013). AB Temel Haklar Şartı ile birlik düzeyinde uygulanan temel haklar katalog haline getirilmiş ve açıklığa kavuşturulması sağlanmıştır (Avrupa Parlamentosu, Avrupa Konseyi ve Avrupa Komisyonu, 2000). AB üyelik sürecinde açılan yargı ve temel haklara ilişkin 23. fasılda da, "Üye Devletler müktesebat ve Temel Haklar Şartı ile garanti edilen temel haklara ve AB vatandaşlarının haklarına saygı gösterilmesini sağlamalıdır" ifadesine yer verilmektedir (T.C. AB Bakanlığı, 2011). Sosyal değişimler ve bilimsel ve teknolojik gelişmelere bağlı olarak temel hakların korunmasını sağlamak ve güçlendirmek amacıyla hazırlanan "Avrupa Birliği Temel Haklar Şartı"nın 8. maddesinde[19], "kişisel verilerin korunması" başlığı altında düzenlemeye yer verildiği görülmektedir.

---

[17] **AB Antlaşması, 6. Madde:** (1) Birlik, 12 Aralık 2007 tarihinde Strazburg'da uyarlandığı haliyle, Antlaşmalarla aynı hukuki değere sahip olan 7 Aralık 2000 tarihli Avrupa Birliği Temel Haklar Şartı'nda yer alan hakları, özgürlükleri ve ilkeleri tanır.

[18] AB kurumlarına yönelik olarak hazırlanan ve AB hukukunun uygulandığı alanlarda geçerli olan AB Temel Haklar Şartı, bazı ülkeler (İngiltere, Polonya, Çek Cumhuriyeti) tarafından özel protokolle reddedilerek ulusal mahkemelerde öne sürülmesi engellenmiştir.

[19] **AB Temel Haklar Şartı, 8. Madde:** (1) Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir. (2) Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir. (3) Bu kurallara uyulması, bağımsız bir makam tarafından denetlenir.

AB Temel Haklar Şartı'nın 51. ve 52. Maddelerinde şartın kapsamı ve üye ülkelere etkilerine yer verilmiştir. Buna göre AB kurum ve kuruluşlarının yanı sıra AB hukukunu uyguladıkları ölçüde üye ülkeler de şartın kapsamında yer almaktadır (T.C. AB Bakanlığı, 2013). Şart 'ta yer alan hükümler doğrudan üye devletleri muhatap almamaktadır. Bu nedenle, AB'nin antlaşmalarda tanımlanan görev ve yetkileri genişletilmemektedir. Ancak üye ülkelerin AB hukuk kurallarını uygulamaları esnasında ya da aday ülkelerin AB müktesebatına uyum sağlama çalışmaları sürecinde, AB Temel Haklar Şartı'nda öngörülen standartları karşılamaları gerekmektedir (T.C. AB Bakanlığı, 2013).

1950 yılında kabul edilen ve 1952 yılında yürürlüğe giren AİHS de AB hukukunda temel hakların korunmasına ilişkin olarak önemli bir yere sahiptir. AB Antlaşmasının 6. Maddesi[20] ve AB Temel Haklar Şartı'nın 52. ve 53. Maddelerinde, teminat altına alınan hakların AİHS ile ilişkisini açıklayan ifadeler bulunmaktadır. AİHS, AB Temel Haklar Sözleşmesinde yer alan temel hakların yorumlanmasına da katkı sağlamaktadır (T.C. AB Bakanlığı, 2013). Türkiye'nin de taraf olduğu AİHS'nin 8. Maddesi ile özel ve aile hayatı koruma altına alınmıştır. Avrupa İnsan Hakları Mahkemesi de (AİHM) bu düzenlemeye bağlı olarak kişisel verilerin korunmasına ilişkin kararlar vermektedir[21]. AİHM tarafından AİHS'nin 8. Maddesi ile ilgili olarak verilen diğer kararlarda da "kişisel bilgilerin kişinin özel yaşamıyla ilgili olduğu" ifadesinin kullanıldığı görülmektedir (AİHM, 2009).

AİHM kararlarında, AİHS'nin 8. Maddesinin esas amacının bireyi kamu otoritelerinin keyfi müdahalesine karşı korumak olduğunu vurgulanmaktadır (AİHM, 2009). Ancak burada dikkate edilmesi gereken nokta, bu ifadenin AİHS'ne taraf ülkenin organları tarafından işlenen verilere sağlanan koruma için kullanılmış olmasıdır. AİHS'nin 8. Maddesinin özel kişiler tarafından işlenen verilerin korunmasına ilişkin olarak da kullanılıp kullanılamayacağı konusu yeterince açık değildir. Ayrıca, AİHM'nin 8. Madde kapsamında vermiş olduğu kararlar, özel yaşamın sınırlarının belirgin olmaması nedeniyle, her olayın değişken koşullarına bağlı olarak farklılık gösterebilecektir. Üniversitelerde de kişisel verilerin korunmasına ve işlenmesine ilişkin usul ve esaslar

[20] **AB Antlaşması, 6. Madde:** (2)Birlik, İnsan Haklarının ve Temel Özgürlüklerin Korunmasına İlişkin Avrupa Sözleşmesi'ne katılır. Bu katılım, Birliğin Antlaşmalar'da belirlenen yetkilerinde değişikliğe yol açmaz. (3) İnsan Haklarının ve Temel Özgürlüklerin Korunmasına İlişkin Avrupa Sözleşmesi tarafından güvence altına alınan ve üye devletlerin ortak anayasal geleneklerinden kaynaklanan temel haklar, Birlik hukukunun genel ilkelerinin parçasıdır.

[21] Bkz. http://portal.nasstar.com/75/files/Peck-v-UK%20ECHR%2028%20Jan%2003.pdf

belirlenirken, bu madde kapsamında yer alabilecek ihlallerin önüne geçebilmek için gerekli düzenlemelerin yapılması önem taşımaktadır.

2.3.3. 108 Sayılı Sözleşme ve 181 Sayılı Ek Protokol Çerçevesinde Kişisel ve Hassas Verilerin Korunması

28 Ocak 1981 tarihinde Strazburg'da imzalanan ve 1 Ekim 1985 tarihinde yürürlüğe giren 108 Sayılı "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme", kişisel verilerin korunmasına yönelik olarak AB'de hazırlanan ilk ve en önemli sözleşmelerden biridir. AİHS'de yer alan özel hayatın gizliliğine ilişkin güvencelerin özellikle kişisel verilerin bilgisayar ortamında işlenmesi konusunda yetersiz ya da sınırlı kalabileceğinin düşünülmesi, kişisel verilerin bağımsız bir hak alanı olarak alındığı 108 sayılı sözleşmenin oluşturulma nedenleri arasında yer almaktadır. 1995 ve 2002 yıllarında hazırlanan 95/46/EC ve 2002/58/EC sayılı direktifler de bu sözleşmeyi tamamlayıcı niteliktedir. 8 Kasım 2001 tarihinde 108 sayılı sözleşmeye ek olarak; 181 sayılı Ek Protokol (Denetleyici Makamlar ve Sınır Ötesi Veri Akışına İlişkin Protokol) imzaya açılmıştır. (Avrupa Konseyi, 2001a). 2004 yılında yürürlüğe giren 181 sayılı ek protokolün amacı, 108 sayılı sözleşmenin geliştirilmesiyle, kişisel verilerin ve mahremiyetin daha üst seviyede korunmasını sağlamaktır. 108 sayılı sözleşmenin onaylanması, 181 sayılı Ek Protokolün de onaylanmasının ön şartıdır.

108 sayılı sözleşmeyle, bu sözleşmeyi imzalayan ülkelerdeki gerçek kişilerin hukuksal olarak temel hak ve özgürlüğü ve kişisel verileri güvence altına alınmaya çalışılmıştır. Ancak 108 sayılı sözleşmenin 12. Maddesinde[22], üye ya da sözleşmeye taraf ülkeler arasında (istisnaları olmakla birlikte) kişisel verilerin transferinin yasaklanamayacağı ifade edilmektedir (Avrupa Komisyonu, 1981). Bu ifadenin AB bilgi güvenliği politikaları ile yakın ilişkisi bulunmaktadır. Buna göre AB içinde kişisel verilerin korunması konusunda yasaklayıcı bir tutumun ötesinde, AB ülkeleri arasında kişisel

[22] **108 Sayılı Sözleşme, Article 12: Transborder flows of personal data and domestic law**
2) A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

verilerin bütünleştirici ve güvenli olarak kullanımını öngören bir yaklaşım benimsenmektedir.

108 sayılı sözleşmede yer alan kişisel verilere ilişkin tanım ve hükümler günümüzde de geçerliliğini korumaktadır. Bununla birlikte, bireylerin hak ve özgürlükleri ile kişisel mahremiyet hakkındaki esasların büyük ölçüde 95/46/EC sayılı veri koruma direktifiyle genişletildiği görülmektedir. 108 sayılı sözleşme ve 181 sayılı protokolden üye ya da taraf ülkelerin etkin olarak faydalanabilmeleri için, sözleşmenin 4. Maddesi[23] gereğince bu konuda gerekli olan iç hukuk düzenlemelerinin yapılması zorunludur. 108 sayılı sözleşmede imzası bulunduğu halde Avrupa Konseyi üyesi 47 ülke içinde bu sözleşmeyi onaylamayan tek ülke olan Türkiye'nin sözleşmeyi iç hukuka uyumlu hale getirebilmesi için, Kişisel Verilerin Korunması Kanunu'nun yapılması gerekmektedir. 1 Ağustos 2014 tarihinde 108 sayılı sözleşmenin onaylanmasının uygun bulunmasına dair kanun tasarısı ve gerekçesi (T.C. Başbakanlık, 2014b) hazırlanmış, ancak henüz kanunlaşmamıştır. 181 sayılı protokolün onaylanabilmesi için ise 108 sayılı sözleşmenin onaylanması şartı bulunmaktadır. Bu nedenle, bu protokol de Türkiye tarafından henüz onaylanmamıştır. Ancak 9 Kasım 2014 tarihi itibariyle 181 sayılı protokolü imzaladığı halde onaylamayan Türkiye ile birlikte 9 ülke bulunmaktadır (Avrupa Konseyi, 2014).

108 sayılı sözleşmenin temel amacı, tüm gerçek kişilerin temel hak ve özgürlüklerini ve kişisel verilerini otomatik bilgi işleme tabi tutulması karşısında özel yaşam haklarını güvence altına almaktır (Avrupa Komisyonu, 1981). Kişisel verilerin sınır ötesi transferinin artması, mahremiyetin ve özel hayatın korunmasına ilişkin riskleri de beraberinde getirmiştir. Bu nedenle sözleşmede, kişisel verilerin kaydı, işlenmesi, değiştirilmesi ve silinmesi gibi işlemlere karşı bireyin korunmasına ilişkin düzenlemelere ağırlık verilmiştir.

[23] **108 Sayılı Sözleşme, Article 4: Duties of the Parties**

1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.
2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

Sözleşmenin 6. Maddesinde[24], iç hukukta gerekli güvenceler alınmadığı müddetçe, ırk, dini inanç, politik düşünce, sağlık bilgileri, cinsel yaşam bilgileri ve ceza mahkûmiyetine ilişkin hassas bilgilerin otomatik işleme tabi tutulamayacağı belirtilmektedir. 95/46/EC sayılı veri koruma direktifinde de olduğu gibi, bu tür hassas veriler, özellikli veri kategorileri altında sınıflandırılmıştır. Bununla birlikte, sözleşmenin 8. Maddesinde[25] veri sahibine ilişkin ek güvencelere yer verilmiştir. Bireylere tanınan bu güvencelerin hangi hallerde sınırlandırılacağı ise, sözleşmenin 9. Maddesinde belirtilmiştir (Avrupa Komisyonu, 1981).

108 sayılı sözleşmenin 5. Bölümünde[26], danışma komitesinin kurulmasına ilişkin düzenlemelere yer verilmiştir. Bu danışma kurulunun, sözleşmenin uygulanmasının kolaylaştırılması ve geliştirilmesi için önerilerde bulunması ve sözleşme üzerinde yapılması gereken değişiklikler hakkında görüş bildirmesi öngörülmüştür. Sözleşmeye taraf olmayan Avrupa Konseyi üyelerinin de bu komitede kendisini bir gözlemci ile temsil ettirme hakkı bulunmaktadır (Avrupa Komisyonu, 1981). 181 sayılı ek protokolün kabul edilmesi, danışma kurulunun en önemli etkinliklerinden biri olarak görülmektedir.

1 Temmuz 2004 tarihinde yürürlüğe giren 181 sayılı protokol, kişisel verilerin korunması, başka bir ülkeye veri transferinin standartlaştırılması ve bağımsız bir denetleme kurumunun oluşturulması amacıyla imzalanmıştır. Kurulması öngörülen bağımsız denetleme kurumunun, kişisel verilerin ihlaline yönelik araştırma yapma, verilerin işlenmesiyle ilgili talep ve itirazları değerlendirme ve bunun sonucunda kanun yoluna başvurma yetkileri bulunmaktadır. Bununla birlikte, kurumun vereceği kararlara ilişkin olarak da yargı yolu açık tutulmuştur. Protokolün 1. maddesinde kurulması öngörülen bağımsız denetleme kurumunun, amacı ve sorumlulukları açısından 95/46/EC sayılı veri koruma direktifinde öngörülen bağımsız veri koruma organı ile benzer nitelikte olduğu görülmektedir. Protokolde ayrıca kişisel verilerin transfer edileceği üçüncü ülkenin ya da uluslararası kuruluşun yeterli veri koruma seviyesinde olması koşuluyla bu verilerin

[24] **108 Sayılı Sözleşme, Article 6: Special categories of data**
Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

[25] Bkz. (Avrupa Komisyonu, 1981)

[26] Bkz. (Avrupa Komisyonu, 1981)

transfer edilebileceği belirtilmektedir. Ancak protokolün 2/2. Maddesi gereğince, veri sahibinin yararı ya da kamu yararının bulunması halinde transfer işlemi yapılabilmektedir (Avrupa Konseyi, 2001a). Protokolde yer alan kişisel verilerin üçüncü ülkelere transferine ilişkin düzenlemeler de 95/46/EC sayılı veri koruma direktifi ile benzer içeriğe sahiptir.

108 sayılı sözleşmenin (95/46/EC sayılı veri koruma kanununda da olduğu gibi) gelişen ihtiyaçları karşılamadığı düşünülerek, 2010 yılından itibaren yenilenmesi için çalışmalar başlatılmıştır. Avrupa Konseyinin 2012-2015 veri koruma stratejisinde de yer alan güncelleme çalışmalarının amacı, bilgi ve iletişim teknolojilerinin gelişimi nedeniyle yetersiz olduğu düşünülen 108 sayılı sözleşmenin temel ilkelere bağlı kalarak genişletilmesidir. Ayrıca sözleşmeye Avrupa Konseyi üyesi olmayan ülkelerin de katılımının teşvik edilmesi ve kişisel verilerin korunmasına ilişkin çalışmaların diğer alanları da (polis teşkilatı, medikal ve iş alanları) kapsayacak şekilde genişletilmesi öngörülmektedir (Avrupa Konseyi, 2013a). Strateji planında, özellikle yeni medya ortamında çocukların, kişisel verilerin ve mahremiyetin korunması için 108 sayılı sözleşme çerçevesinde yeni önlemler alınmasının gerekli olduğu vurgulanmaktadır. Ancak 108 sayılı sözleşme Avrupa Konseyi üyesi olmayan ülkelerin imzasına da açık olması ve taraf olan ülkeler için bağlayıcı özellikte uluslararası metin olması nedeniyle, mevcut haliyle de önemli bir kaynak niteliğindedir.

2.3.4. 95/46/EC Sayılı Veri Koruma Direktifi Çerçevesinde Kişisel ve Hassas Verilerin Korunması

24 Ekim 1995 tarihinde Avrupa Konseyi ve Avrupa Parlamentosu tarafından kabul edilen 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki Direktif, 1998 yılında yürürlüğe girmiştir. 108 sayılı AK sözleşmesi ve OECD'nin hazırlamış olduğu rehber ilkelere bağlı olarak hazırlanan ulusal veri koruma direktifleri arasındaki farklılıkların giderilmesi amacıyla 1990 yılında başlatılan çalışmalar sonucunda 95/46/EC sayılı direktif oluşturulmuştur. AB hukuksal düzenlemelerinin genelinde olduğu gibi, 95/46/EC sayılı direktifte de asıl amacın verilerin değil kişilerin başta kişisel mahremiyet hakkı olmak üzere temel hak ve

özgürlüklerinin korunması olduğuna vurgu yapılmaktadır (Avrupa Konseyi, 1995). 95/46/EC sayılı direktif, üye ülkeler arasındaki veri korumaya yönelik farklılıkların ortadan kaldırılarak, kişisel verilere yönelik muhtemel saldırı ve yetkisiz erişimler için sistemli olarak önleyici tedbirlerin alınmasını öngörmektedir. Bununla birlikte, üye ülkeler arasında güvenli olarak kişisel verilerin akışının sağlanması ve ortak pazarın tamamlanması da direktifin ana hedefleri arasında yer almaktadır. Bu hedeflere ulaşılabilmesi için, 108 sayılı sözleşmeyi tamamlayıcı nitelikte olan bu direktifte yer alan temel ilkelerin, (sözleşmenin 4. Maddesinde de belirtildiği gibi) taraf ülkeler tarafından iç hukukun parçası haline getirilmesi gerekmektedir. Farklı bir ifadeyle, 95/46/EC sayılı direktif, üye ülkelerin iç hukuk sistemlerini hedef almakta, AB kurum ve organlarını kapsamın dışında tutmaktadır. 95/46/EC sayılı direktifin oluşmasında da rol oynayan başlıca gerekçeler ve ortaya konulan prensiplere de direktifler içinde detaylı olarak yer verilmiştir (Avrupa Konseyi, 1995);

Direktifin genel yapısı göz önüne alındığında, ortak pazarın geliştirilmesi amacıyla üye ülkeler arasında kişisel veri akışının sağlanması ile kişilerin temel haklarının korunması arasında denge oluşturulduğu görülmektedir. Bu denge kurulurken, başta AİHS ve AB Antlaşması olmak üzere direktiften önce yürürlüğe giren diğer hukuksal düzenlemeler de dikkate alınmıştır.

Direktifin 3. Maddesinde de belirtildiği gibi, bir dosyalama sisteminin[27] parçasını oluşturan ya da oluşturması istenen kişisel verilerin, otomatik ya da otomatik olmayan araçlarla işlenmesi direktif kapsamında yer almaktadır. Ancak bu direktif, AB Antlaşmasının 5. ve 6. başlıklarında da belirtilen AB hukuku kapsamı dışında kalan faaliyetler, ceza hukuku alanındaki devlet faaliyetleri, savunma, kamu güvenliği ve bir gerçek kişinin tamamen kişisel veya ev içi faaliyetlerini içeren verilere yönelik olarak uygulanmamaktadır (Avrupa Konseyi, 1995). Direktifte kişisel veya ev içi faaliyetlerin kapsam dışında olduğu ifade edilse de, bu bilgilerin internet üzerinde erişime açık olarak bulundurulmasının nasıl değerlendirileceği konusunda somut olaya bağlı olarak belirsizlikler oluşabilmektedir. Bu konuyla ilgili Avrupa Adalet Divanı'nın vermiş

[27] **Kişisel Veri Dosyalama Sistemi:** Merkezi ya da merkezi olmayan, özel kriterlere göre erişilebilir olan herhangi bir yapılandırılmış kişisel veri dizisidir (Avrupa Konseyi, 1995).

olduğu kararlar incelendiğinde, kişisel verilerin internet ortamında belirsiz sayıda kişinin erişimine açık hale getirilmesi halinde, direktifin 3/2. Maddesinde[28] yer alan istisnaların kapsamının dışında kalacağı anlaşılmaktadır (Avrupa Adalet Divanı, 2003). Özellikle sosyal paylaşım ağları üzerinde bulunan bilgiler için hizmet sağlayıcılar tarafından uygulanan koruma düzeyinin değişken olması ve hizmet sağlayıcı politikalarına bağlı olarak kullanıcıya gerekli bildirimler yapılmaksızın kişisel verilerin açık hale getirilmesi (Stutzman, Gross ve Acquisti, 2012) gibi durumların direktif kapsamında nasıl değerlendirileceği tartışmaların odağında yer almakta ve belirsizliğini korumaktadır. Ayrıca direktif kapsamında yer alan kişisel verilerin, özel kriterlere göre erişilebilir ve yapılandırılmış olması gerekmektedir. Elektronik ortamda bulunan verilere erişim konusunda direktifin bu kriteri açısından bir engel bulunmamaktadır. Ancak elden işlenen kişisel verilerin yapılandırılmış ve özel kriterlere göre erişilebilir olması önem taşımaktadır.

Direktifin 6. Maddesinde veri kalitesine ilişkin prensiplere yer verilmiştir. Bu prensipler; kişisel verilerin adil ve yasal olarak işlenmesi, meşru amaçlar için toplanmış olması, toplanma amacıyla ilgisiz ve gereğinden fazla bilgi toplanmaması, doğru ve güncel olması, toplanma amacına uygun süre boyunca tutulması ve üye ülkelerin bu şartların yerine getirilmesi için gerekli önlemleri almalarıdır. Gerekli önlemlerin alınması halinde; tarihsel, istatistiksel ya da bilimsel amaçlar için kişisel verilerin detaylı olarak işlenmesi veya daha uzun süre depolanmasının veri koruma direktifine aykırı olmayacağı ayrıca belirtilmektedir (Avrupa Konseyi, 1995). Üye ülkelerin kişisel verilerin işlenmesini sağlamaları için gerekli koşullara ise direktifin 7. Maddesinde[29] yer verilmiştir. Bu koşullar içinde dikkati çeken noktalar; veri sahibinin açık ve kesin olarak rızasının alınması, bir sözleşmenin yerine getirilmesi, yasal yükümlülüğün yerine getirilmesi, veri sahibinin hayati menfaatlerinin korunması ve kamu menfaati için gerekli görevin yerine getirilmesidir.

Ulusal ve uluslararası birçok hukuksal düzenlemede, sağlık durumu, cinsel yaşama ilişkin veriler, dini ve felsefi inançlar, ırk veya etnik kökeni açıklayan kişisel veriler, siyasi görüş

[28] Bkz. (Avrupa Konseyi, 1995)
[29] Bkz. (Avrupa Konseyi, 1995)

ve sendika üyeliği, daha üst seviyede korumayı gerektiren hassas veriler olarak tanımlanmaktadır. Bu tür verilerin üst seviyede koruma gerektiren hassas veriler olarak tanımlanmasının nedeni, toplum içinde ayrımcılığa ve kişilerin mağduriyetine yol açabilme riskinin yüksek olmasıdır. 95/46/EC sayılı direktifin 8/1. Maddesinde[30] de bu kapsamda yer alan kişisel verilerin işlenmesinin üye devletler tarafından yasaklanması öngörülmektedir. Bu yasakların uygulanmayacağı veri sahibinin açık rızasının olması gibi istisnai durumlar ise 8. Maddenin 2. Fıkrasında belirtilmektedir (Avrupa Konseyi, 1995).

Direktife göre kişisel verilerin işlenmesinden sorumlu olan kişiler, bu verilerin işlenmesine ilişkin araç, amaç ve yöntemler hakkında karar verme yetkisine sahip olan ve denetleyici[31] olarak tanımlanan kişi ya da kurumlardır. Direktifin 16. Maddesi[32] gereğince, kişisel verilere erişim hakkı bulunan işleyici ve işleyici ya da denetleyicinin yetkisi altındaki kişiler, kanun tarafından istenmediği sürece denetleyicinin talimatı haricinde verileri işlememelidirler (Avrupa Konseyi, 1995). Direktifin 17. Maddesinde ise, kişisel verilerin ağ üzerinden iletimi, yetkisiz erişim, değiştirme ve kazara ya da yasa dışı yöntemlerle yapılacak tahribe karşı gerekli teknik ve kurumsal önlemlerin denetleyici tarafından uygulanması ve üye ülke tarafından bunun sağlanması öngörülmektedir.

Üye ülkelerde bulunan AB vatandaşları, direktifin iç hukuka uygulanıp uygulanmadığına bakmaksızın direktifte bireylere doğrudan tanınan haklardan (mahremiyet, veri işleme, veri erişim vd.) yararlanabilmekte ve direktife dayanarak yargı yoluna başvurabilmektedirler. Bu önemli korumanın dayanağı, üye ülkelerin kendi iç hukuklarını direktif ile uyumlu hale getirirken, direktifte belirtilen temel ilkelerden daha düşük seviyede koruma sağlayan düzenlemeler yapmalarının sınırlandırılmış olmasıdır. Ancak Almanya örneğinde olduğu gibi (Reding, 2013), daha yüksek seviyede koruma önlemleri içeren düzenlemelerin yapılması, üye ülkelerin inisiyatifine bırakılmıştır. Bununla birlikte, Direktifinin oluşturulması esnasında görülen az sayıda üye ülkenin katkı

[30] **95/46/EC, Article 8:** 1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

[31] **Denetleyici:** Kişisel verilerin işlenme araç ve amaçlarını belirleyen, gerçek veya tüzel kişiyi, kamu makamı, devlet dairesi ya da başka bir kuruluştur (Avrupa Konseyi, 1995).

[32] Bkz. (Avrupa Konseyi, 1995)

sağlaması ve aralarında görüş farklılıkları (Simitis, 1995; White, 1997) bulunması gibi sorunların, bu Direktifin iç hukuk ile uyumlu hale getirilmesi esnasında da bulunduğu belirgin olarak görülmektedir. Genel olarak bakıldığında, AB üyesi ülkelerin veri koruma direktifini iç hukuka uyarlama konusunda yeterli düzeyde çalışma yapmamış oldukları görülmektedir (Schartum, 2008). Bu durum, ulusal veri koruma direktifleri ile birlikte 95/46/EC sayılı veri koruma direktifinin de kişisel verilerin korunması konusunda tek başına yetersiz kalmasına neden olmaktadır. Bu nedenle, kişisel verilerin her üye ülkede eşit seviyede korunabilmesi ve bireylerin çevrimiçi ticarete olan güveninin sağlanarak AB pazarının canlandırılabilmesi için veri koruma direktifi üzerinde yapılan reform çalışmaları önem taşımaktadır.

95/46/EC sayılı veri koruma direktifinin düzenlemiş olduğu temel alanlardan biri de kişisel verilerin üçüncü ülkelere aktarılması konusudur. 1990'lı yıllardan itibaren bilgi ve iletişim teknolojilerinde yaşanan gelişmeler, AB'de kişisel verilerin korunması konusunda veri aktarımına yönelik olarak daha yoğun çalışmaların yapılmasına neden olmuştur. Direktifte kişisel verilerin üçüncü ülkelere aktarımına ilişkin düzenlemeler, 25. ve 26. Maddelerde[33] yapılmaktadır. Direktifin 25. Maddesinde, üçüncü ülkelere kişisel verilerin transferinin yapılabilmesi için, yeterli koruma seviyesinin bulunması koşulu bulunmaktadır. Komisyonun yeterlilik konusunda onay verdiği Kanada[34], İsviçre[35] ve Arjantin[36], bu konuda verilebilecek örnekler arasında yer almaktadır. AB'nin yeterlilik konusunda onay vermediği ABD ile ticari ilişkilerin ve kişisel bilgi akışının devam edebilmesi için ise, AB ile ABD Ticaret Bakanlığı arasında imzalanan "Safe Harbour Antlaşması" uygulamaya geçirilerek çözüm üretilmeye çalışılmıştır. Ancak bu antlaşmanın uygulanmasına yönelik eksikliklerin bulunduğu konusunda tartışma ve eleştiriler de yürürlüğe girdiği tarihten itibaren devam etmektedir (Avrupa Komisyonu, 2004a). Bununla birlikte üye ülkelerin ve Komisyonun, yapılan incelemelerde yeterli korumayı sağlamadığı görülen üçüncü ülkeler hakkında birbirlerini bilgilendirme yükümlülüğü bulunmaktadır. Bu hükümler, 95/46/EC sayılı veri koruma direktifini Avrupa sınırları dışında da etkin ve bağlayıcı hale getirmektedir. Direktifin 26.

[33] Bkz. (Avrupa Konseyi, 1995)
[34] Bkz. (Avrupa Komisyonu, 2002)
[35] Bkz. (Avrupa Komisyonu, 2000)
[36] Bkz. (Avrupa Komisyonu, 2003)

Maddesinde ise, verilerin aktarılacağı ülkede yeterli seviyede koruma olmaması halinde aktarmanın yapılabilmesi için geçerli olabilecek istisnalar yer almaktadır.

Direktifin 26. Maddesinde yer alan istisnalar dâhilinde kişisel verilerin üçüncü ülkelere aktarımı yapılırken, temel hak ve özgürlükler ile kişisel mahremiyetin korunması göz önünde bulundurulacak en önemli koşullardır. Bununla birlikte veri aktarımı konusunda genel anlamda dikkati çeken nokta, direktifte veri aktarımına ilişkin olarak bir tanımın yapılmamış olmasıdır. Sadece direktif göz önüne alındığında, özellikle internet ortamında yayınlanan kişisel verilerin üçüncü ülkelere veri aktarımı kapsamında değerlendirilip değerlendirilmeyeceği açık değildir. Ancak Avrupa Adalet Divanının bu konuda vermiş olduğu kararlar (Avrupa Adalet Divanı, 2003) incelendiğinde, herkesin erişimine açık olmayan kişisel verilerin internet ortamı kullanılarak AB üyesi olmayan bir ülkedeki sunucu üzerinden gönderilmesi dışında, bu kapsamda değerlendirilemeyeceği görülmektedir.

95/46/EC sayılı veri koruma direktifinin önleyici koruma sağlamasına ilişkin en önemli unsurlardan biri de etkin denetim sisteminin kurulmuş olmasıdır. Direktifin 28. Maddesi[37] gereğince, her üye devlet direktifte yer alan hükümlerin kendi ülkesindeki uygulamasını izlemekten ve bu konuda en az bir kamu kurumunun görevli olmasından sorumludur. Bu kurumun görevlerini yerine getirirken bağımsız olarak hareket edeceği de direktifte ayrıca vurgulanmaktadır. Ayrıca üye ülkelerin, kişisel verilerin işlenmesi ve bireysel hakların korunması konusunda yönetmelik hazırlanırken ya da idari tedbir alırken, denetim makamına danışılmasını sağlama yükümlülüğü bulunmaktadır. Direktifte denetleme makamlarına, denetim görevini yerine getirmesi için gerekli tüm bilgilere erişim, silinmesini ya da yok edilmesini isteme, ihtar verme ve ulusal hükümlerin ihlal edilmesi halinde bu ihlalleri yargıya sunmak üzere kovuşturmaya başlama yetkisinin verilmesi de öngörülmektedir. Denetleme makamı bu yetkileri kendi ulusal kanunlarına bağlı olmaksızın kullanabilecek ve diğer denetleme makamlarıyla da bilgi alışverişinde bulunabilecektir. Denetleme makamlarının kararlarına karşı mahkemelerde temyiz yoluna gidilebilmektedir (Avrupa Konseyi, 1995).

[37] Bkz. (Avrupa Konseyi, 1995)

Direktifin kişisel verilerin işlenmesine dair bireylerin korunması konusunda sunmuş olduğu yeniliklerden biri de, danışma statüsünde olacak ve bağımsız hareket edecek bir çalışma grubu kurulmasını öngörmesidir. Direktifin 29. Maddesinde tanımlanan çalışma grubu, üye ülkelerin denetleme makamlarından, AB kurum ve kuruluşlarından ve AB Komisyonundan birer temsilcinin katılımıyla oluşmaktadır. Direktifin 30. Maddesinde yer verilen çalışma grubunun öne çıkan bazı görev ve sorumlulukları şunlardır (Avrupa Konseyi, 1995);

- AB üyesi ya da üçüncü ülkelerdeki koruma seviyesi hakkında Komisyon'a görüş bildirme,
- Direktifte yapılacak değişikliklere ilişkin Komisyon'a tavsiyede bulunma,
- Üye ülkelerin uygulama ya da kanunlarından kaynaklanan uyuşmazlıklar hakkında Komisyon'u bilgilendirme ve
- Kişisel verilerin işlenmesine dair kişilerin korunmasına ilişkin tüm konularda tavsiyelerde bulunma.

2.3.5. AB'nin Hazırlamış Olduğu Diğer Hukuksal Düzenlemeler ve Sözleşmeler Çerçevesinde Kişisel ve Hassas Verilerin Korunması

AB hukuk mevzuatında kişisel verilerin korunmasına ilişkin olarak yapılan düzenlemelerde, bireysel hakların korunması ve böylece bireylerin çevrimiçi ticarete olan güveninin kazanılması amacı öne çıkmaktadır (Reding, 2013). Bu amaca bağlı olarak, temel veri koruma direktifinin yanı sıra AB hukuk mevzuatında farklı alanlara yönelik yayınlanmış direktif ve tavsiye kararları da bulunmaktadır. AB hukukunda, direktif ve sözleşmelerin yürürlüğe girmesinden sonra meydana gelen yenilikler ve farklı alanlarda gelişen yeni koşullar dikkate alınmakta ve hukuksal eksikliklerin giderilerek uygulamaya dönüştürülmesinde ağırlıklı olarak tavsiye kararları kullanılmaktadır. Bu konuda öne çıkan başlıca AB direktifleri ve tavsiye kararları şunlardır;

- Bilgi Güvenliği Alanındaki 92/242/EEC[38] Sayılı Karar

[38] Bkz. (Avrupa Konseyi, 1992b)

- 97/66/EC[39] Sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi
- 2000/520/EC[40] Sayılı Güvenli Liman Anlaşmasına ilişkin Avrupa Komisyonu kararı
- 2001/497/EC[41] Sayılı Üçüncü Ülkelere 95/46/EC Sayılı Direktif Kapsamında Yer Alan Kişisel Verilerin Transferi İçin Standart Sözleşme Kuralları kararı
- 45/2001/EC[42] Sayılı AB Organlarının Kişisel Verilerin Korunmasıyla İlgili Yükümlülükleri hakkında tüzük
- 2002/58/EC[43] Sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Direktifi
- Avrupa Konseyinin "Ağ ve Bilgi Güvenliği Kültürü Oluşturulması"[44] konusundaki 18 Şubat 2003 tarihli kararı
- 2004/915/EC[45] Sayılı Kişisel Verilerin Üçüncü Ülkelere Transferine İlişkin Alternatif Standart kararı
- 2004/0023 (COD)[46] Sayılı İnternet ve Yeni Çevrimiçi Teknolojilerin Güvenli Kullanımı kararı
- 460/2004[47] Sayılı Avrupa Ağ ve Bilgi Güvenliği Ajansını (ENISA) kuran tüzük.
- 854/2005/EC[48] Sayılı Güvenli İnternet Kullanımına Geçiş Kararı
- 2006/24/EC[49] Sayılı Kamusal Elektronik Haberleşme Hizmetlerinin Sunumu Sırasında Veya Kamusal Haberleşme Şebekeleri Üzerinden Elde Edilen Verilerin Muhafazasına İlişkin Direktif
- 2008/49/EC[50] Sayılı İç Pazar Bilgi Sistemlerinin Kişisel Verilerin Korunmasına Yönelik Olarak Kullanımı Kararı

[39] Bkz. (Avrupa Konseyi, 1997)
[40] Bkz. (Avrupa Komisyonu, 2000)
[41] Bkz. (Avrupa Komisyonu, 2001a)
[42] Bkz. (Avrupa Konseyi, 2001b)
[43] Bkz. (Avrupa Konseyi, 2002)
[44] Bkz. (Avrupa Konseyi, 2003)
[45] Bkz. (Avrupa Komisyonu, 2004a)
[46] Bkz. (Avrupa Konseyi, 2004a)
[47] Bkz. (Avrupa Konseyi, 2004b)
[48] Bkz. (Avrupa Konseyi, 2005)
[49] Bkz. (Avrupa Konseyi, 2006)
[50] Bkz. (Avrupa Komisyonu, 2008)

- 2010/87/EU[51] Sayılı "95/46/EC Sayılı Direktif Kapsamında Üçüncü Ülkelere Kişisel Verilerin Transferine İlişkin Standart Sözleşme Hükümleri" Kararı
- 2011/136/EU[52] Sayılı Tüketici Koruma İşbirliği Sistemi İçinde Veri Koruma Kurallarının Uygulanması tavsiye kararı
- 526/2013[53] Sayılı Avrupa Ağ ve Bilgi Güvenliği Ajansı'na İlişkin tüzük

AB hukukunda kişisel verilerin korunmasına ilişkin düzenlemeler içeren diğer direktifler ve tavsiye kararları, kişisel verilerin korunması konusunda temel veri koruma direktifi olan 95/46/EC sayılı direktifin tamamlayıcısı niteliğindedir. Diğer taraftan, Avrupa Konseyinin "Ağ ve Bilgi Güvenliği Kültürü Oluşturulması" konusunda 18 Şubat 2003 tarihinde almış olduğu kararda (Avrupa Konseyi, 2003), kamunun oluşturacağı güvenlik kültürüne bireylerin de katılımının sağlanmasının hedeflendiği görülmektedir. Kararda ağ ve bilgi güvenliğinin sağlanması için "güvenlik kültürü" oluşturulmasının gerekçelerine yer verilerek, bu konuda kapsamlı bir Avrupa stratejisinin oluşturulması gerektiği ve bunun için OECD'nin "Bilgi Sistemleri ve Ağ Güvenliği" (OECD, 2002) konusunda belirlemiş olduğu ilkelerin önemli bir model olabileceği vurgulanmaktadır.

97/66/EC sayılı direktif, 95/46/EC sayılı direktifin yetersiz olduğu düşünülen telekomünikasyon alanında tamamlarken; 2002/58/EC sayılı direktif, elektronik haberleşme alanında kapsamlı çerçeveyi oluşturmuş ve 97/66/EC sayılı direktifi kaldırarak yürürlüğe girmiştir. 2006/24/EC sayılı direktif ile birlikte verilerin saklanmasına ilişkin hükümlere yer verilmiş ve 95/46/EC sayılı veri koruma direktifinde belirtilen temel hak ve özgürlüğün korunmasına ilişkin ilkelere bağlı kalarak, 2002/58/EC sayılı direktif üzerinde değişiklikler yapılmıştır. 2006/24/EC sayılı direktifte; adli olaylar, elektronik haberleşme altyapısı, trafik bilgilerine ilişkin verilerin takibi ve internet hizmetleri gibi konulara kapsamlı olarak yer verilerek, 2002/58/EC sayılı direktiften daha detaylı bir direktif olması sağlanmıştır. Ancak Avusturya ve İrlanda'nın Temel Haklar Sözleşmesi'ne uygunluğunun değerlendirilmesi istediği bu direktifin, AB Adalet Divanı tarafından 08.04.2014 tarihinde geçersiz olduğuna karar verilmiştir (AB Adalet Divanı,

[51] Bkz. (Avrupa Komisyonu, 2010a)
[52] Bkz. (Avrupa Komisyonu, 2011a)
[53] Bkz. (Avrupa Konseyi, 2013c)

2014b). İptalin gerekçeleri olarak; direktifin özel hayatın ve kişisel verilerin korunması gibi temel hakları ihlal etmesi, verilerin 6-24 ay süre ile saklanmasının gerekçelerinin açık olmaması, kişiye ait verilerin bilgisi dışında kullanılmasının "özel hayatın gözetim altında olduğu" hissini uyandırması ve tutulan bilgilere ulusal makamların ulaşmasının mahremiyeti ihlal etmesi gösterilmiştir.

2008/49/EC sayılı kararda, üye ülkelerin elektronik bilgi alış verişinde 45/2001/EC sayılı tüzük ve 95/46/EC sayılı veri koruma direktifinde yer alan verilerin serbest dolaşımına ilişkin ilkelere uymaları gerektiği belirtilmiş ve ayrıca bu verilerin ne kadar süre saklanabileceği konusuna açıklık getirilmiştir. 2011/136/EU Sayılı kararda ise, özellikle sınır ötesinde yaptırım eksikliği bulunduğu zaman kişisel verilerin korunması konusunda hayati önem taşıyan, ulusal tüketici koruma yetkilileri arasındaki işbirliğinin sağlanması amaçlanmaktadır. Bu karar, AB içindeki tüketicinin kişisel verilerini hedef alan olası ihlallerin ve illegal ticari faaliyetlerin incelenmesi ve durdurulması için, iki ülkenin kamu otoritelerinin 95/46/EC sayılı veri koruma direktifi çerçevesinde işbirliğinin sağlanmasını öngören düzenlemeler içermektedir.

95/46/EC sayılı veri koruma direktifi ile üye ülkelerin iç hukuk sistemlerinde veri korumaya ilişkin ortak temellere dayanan bir düzenleme yapılması amaçlanmaktadır. Bu nedenle, AB kurum ve organları bu direktifin dışında tutulmuştur. AB kurum ve kuruluşlarının kişisel verilerin korunması konusundaki yükümlülükleri, 45/2001/EC sayılı tüzük ile belirlenmiştir (Avrupa Konseyi, 2001b). Bu tüzük ile AB organlarının kendi içindeki veri akışını engellemeyecek şekilde kişisel verileri koruması öngörülmektedir. Tüzüğün birçok bölümünde 95/46/EC sayılı veri koruma direktifine atıf yapılmasına rağmen, AB organları tarafından işlenen verilere ilişkin yükümlülükler üzerinde durulurken temel ilkelerin tekrar edildiği görülmektedir. OECD rehber ilkelerine paralel olarak hazırlanan bu tüzükte dikkat çeken noktalardan biri, AB organlarının kişisel verilerin işlenmesiyle ilgili yükümlülüklerinin kontrol ve denetiminin, bağımsız AB veri koruma denetçisi tarafından yapılacağının belirtilmesidir. Tüzüğün 24/1. maddesine göre AB kurum ve kuruluşlarında en az bir veri koruma görevlisinin bulunması ve uygulamalar hakkında AB Veri Koruma Kurumu'nu bilgilendirmesi öngörülmektedir (Avrupa

Konseyi, 2001b). AB Veri Koruma Kurumu, bu uygulama ile AB kurum ve kuruluşlarını kişisel verilerin korunmasına ilişkin olarak denetlemektedir.

2001/497/EC ve 2004/915/EC sayılı Avrupa Komisyonu kararları, AB içinde yer alan bir veri denetleyicisinin AB dışındaki bir veri denetleyicisine veri transfer ederken uyması gereken sözleşme hükümlerini içermektedir. Her iki kararda 95/46/EC sayılı veri koruma direktifinin 26/2. Maddesine[54] uygun olarak hazırlanmıştır. AB içinde bulunan bir veri denetleyicisinin 95/46/EC sayılı veri koruma direktifinin 26/2. Maddesi kapsamında alması gereken güvenlik önlemlerine ilişkin olarak ise, 2010/87/EU sayılı Avrupa Komisyonu kararı uygulanmaktadır. Kişisel verilerin üçüncü ülkelere transferine ilişkin standart sözleşme kurallarını belirleyen 2001/497/EC ve 2004/915/EC sayılı Avrupa Komisyonu kararlarıyla birlikte, iki farklı sözleşme hükümleri modeli sunulmaktadır (Schwartz, 2012). 2004/915/EC sayılı Avrupa Komisyonu kararı, 2001/497/EC sayılı karar üzerinde yapılmış düzeltmeler ve eklentiler içermektedir. Genel olarak değerlendirildiğinde, 2004/915/EC sayılı kararda yer alan ifadeler daha özenli ve bilgi transferi yapanların sorumluluklarını arttırıcı niteliktedir. Her iki sözleşme modeli de kullanılabilir durumdadır. Ancak kullanılacak olan modelin kendine özgü avantajlarından tam olarak yararlanılabilmesi için şirketler bu iki modeli birleştirmeden kullanmalıdırlar (Data Protection Unit of the Directorate-General for Justice, t.y.).

26 Temmuz 2000 tarih ve 2000/520/EC sayılı Avrupa Komisyonu kararı ile Avrupa Ekonomik Alanı'ndan ABD'ye bilgi transferi yapacak olan ABD ticari şirketlerinin Güvenli Liman Anlaşması (Safe Harbour Aggrement) üyesi olma zorunluluğu getirilmiştir. Bu zorunluluk aynı zamanda veri koruma direktifinin sınır ötesi veri transferini yasaklayan hükmüne karşı bir istisna anlamına da gelmektedir (Avrupa Komisyonu, 2004b). Güvenli Liman Anlaşması, ABD Ticaret Bakanlığı ile AB arasında 2000 yılında yapılan ve AB sınırları içindeki ülke vatandaşlarının kişisel bilgilerinin ABD şirketleri tarafından transferini belirli şartlara bağlayan bir anlaşmadır. Bu anlaşmanın üyesi olabilmek için, şirketler gerekli şartları sağladıktan sonra AB üyesi ülkelerden onay

[54] **95/46/EC, Article 26/2:** Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

almak zorundadırlar. Anlaşma gereğince, bilgileri taşıyacak olan üye şirketin, veri sahibini verilerin işlenmesine (hangi amaçla, ne kadar süreyle vd.) ilişkin olarak bilgilendirmek ve gerekli tüm bilgi güvenliği önlemlerini almak zorundadır. Bu anlaşma kişisel verilerin korunmasına ilişkin önlemlerin hem teknik hem de hukuksal boyutuyla bütün olarak ele alınmış olması nedeniyle konumuz açısından dikkat çekicidir.

Kişisel verilerin korunmasına ilişkin olarak bazı temel ilkelerin, direktiflerin dışında da birçok resmi kaynakta farklı zamanlarda yer aldığı görülmektedir[55]. Bu kaynaklarda yer alan temel ilkeler; bireylerin kendisine ait kişisel verilerin korunmasını isteme hakkı, bu verilerin belirlenen amaçların dışında bireyin rızası olmaksızın kullanılmaması, bireyin kendisine ait verilere erişim ve düzeltme hakkının sağlanması ve bu kuralların uygulanmasının bağımsız bir kuruluş tarafından kontrolünün sağlanmasıdır.

2.3.6. AB'de Kişisel Verilerin Korunmasına Yönelik Reform Çalışmaları

AB içinde yer alan ülkelerin ulusal veri koruma kanunlarında farklılıkların bulunması, bu kanunların yeterince anlaşılır olmaması ve mevcut veri koruma direktifinin kullanıcılarda çevrimiçi alışverişe karşı oluşan kaygıları gideremmemesi nedeniyle, 95/46/EC sayılı veri koruma direktifinin gözden geçirilmesine ilişkin çalışmalar başlatılmıştır (Avrupa Komisyonu, 2013).

Kişisel verilerin korunması konusunda hukuksal düzenlemelerin, bilgi depolama yöntemleri, sosyal medya ve bilgi sistemlerindeki gelişimin ve toplumsal ihtiyaçların gerisinde kalması, 2010 yılından itibaren AB'yi yeni bir veri koruma direktifi üzerinde çalışmaya zorlamaktadır (Filippi ve Belli, 2012). AB veri koruma kanununun güncellenmesi konusu, 4 Kasım 2010 tarihinde yayınlanan IP/10/1462 referans numaralı "Kişisel Verilerin Nasıl Korunacağına İlişkin Strateji" belgesi (Avrupa Komisyonu, 2010b) ve MEMO/10/542 referans numaralı bildirilerle (Avrupa Komisyonu, 2010c) birlikte gündeme taşınmıştır. Bu çerçevede belirlenen güncelleme ihtiyacına bağlı olarak,

[55] Bkz. http://ec.europa.eu/justice/data-protection/law/index_en.htm
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:en:HTML

25 Ocak 2012'de 2012/0011 (COD)[56] referans numaralı yeni kişisel verilerin korunması direktifi önerisi hazırlanmış ve AB Konseyi ve Parlamentosu'nun onayına sunulmuştur (Avrupa Komisyonu, 2012a).

95/46/EC sayılı AB veri koruma direktifinin güncellenmesiyle gerçekleştirilecek olan veri koruma reformuyla; kişisel hakların genişletilmesi (Avrupa Komisyonu, 2012b), iç pazarın canlandırılması (Avrupa Komisyonu, 2011g), uluslararası işbirliğinin kolaylaştırılması (Avrupa Komisyonu, 2011e), mevcut kuralların daha basit ve anlaşılır hale getirilmesi (Avrupa Komisyonu, 2011f), iş dünyasına fayda sağlaması (Avrupa Komisyonu, 2011d) ve veri korumaya ilişkin hukuksal düzenlemelerin yeni bilgi teknolojilerine uyumlu hale getirilmesi (Avrupa Komisyonu, 2011h) hedeflenmektedir. Bu hedeflere ulaşmak için bir dizi yeniliğin yapılması öngörülmektedir (Avrupa Komisyonu, 2011i);

Üniversitelerde kişisel verilerin korunması kapsamında geliştirilecek olan bilgi güvenliği politikaları için, bilgi teknolojilerindeki gelişmelere bağlı olarak gerekli olduğu düşünülen AB veri koruma reform çalışmalarının dikkate alınması büyük önem taşımaktadır. Zira AB vatandaşlarının kişisel verilerinin korunması konusunda kaygılarını gidermede yeterli olmayan 95/46/EC sayılı veri koruma direktifinin önemli eksiklerinin olduğu bilinmektedir. Veri koruma reformuna ilişkin muhalif yaklaşım ve tartışmalar, ağırlıklı olarak önerilen yeni düzenlemenin içeriği üzerinde yoğunlaşmaktadır.

2.3.7. AB'de Kişisel Verilerin Korunmasına Yönelik Kontrol ve Koordinasyon Mekanizması

AB Hukuk Mevzuatında ve bilgi güvenliği politikalarında, kişisel verilerin korunması amacıyla kurumsal yapının ve bu kapsamda kişisel veri koruma otoritelerinin oluşturulmasına önem verildiği görülmektedir. Bu otoritelere yüklenen sorumluluklar; ulusal bilgi güvenliğinin sağlanmasına yönelik strateji, politika ve standartların

[56] Bkz. (Avrupa Konseyi, 2012)

geliştirilmesi, kurumlar arasındaki koordinasyonun ve işbirliğinin gelişmesine katkı sağlaması, ulusal bilgi güvenliği risklerinin tespit edilmesi, kurum ve kuruluşlara güvenlik testlerinin uygulanması ve farkındalığın oluşması amacıyla çalışmalar yapılmasıdır. Bu tür kuruluşların, temel ilkeler çerçevesinde yapmış oldukları durum tespiti sonucunda oluşturdukları raporlar, dolaylı olarak denetimlere önemli katkılar sağlamaktadır.

AB'de bu düşüncenin ilk olarak yer aldığı belgelerden biri olan AK'nin 31 Mart 1992 tarihli ve 92/242/EEC sayılı kararında, üye ülkelerin bilgi sistemleri kullanım güvenliğinin sağlanması ve bir politika geliştirilmesine ilişkin amacı ortaya konulmaktadır (Avrupa Konseyi, 1992a). Bu kararda, bir eylem planı oluşturacak ve komisyona danışmanlık yapacak birimin kurulması da öngörülmektedir. 460/2004[57] sayılı tüzük ile 10 Mart 2004 tarihinde kurulan Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA-European Network and Information Security Agency), 92/242/EEC sayılı kararla ilişkili olarak kurulmuştur. 460/2004 sayılı düzenlemeyi yürürlükten kaldıran 18 Haziran 2013 tarih ve 526/2013[58] sayılı düzenlemeyle, ENISA'nın görev kapsamında değişiklikler yapılmıştır. 526/2013 sayılı düzenlemede 95/46/EC ve 2002/58/EC sayılı direktiflerin öngörülerine atıfta bulunularak; ENISA'nın çalışmalarıyla geliştirilecek ağ ve bilgi güvenliği kültürünün, kişisel verilerin korunmasına daha fazla katkı sağlanacağı belirtilmektedir (Avrupa Konseyi, 2013c). ENISA, AB ekonomik alanı içinde üst düzeyde ağ ve bilgi güvenliğinin sağlanması için, AB çatısı altında bulunan tüm kurum ve kuruluşların bilgi güvenliği konusunda bilgi alışverişinde bulunduğu bir danışma ve koordinasyon merkezi konumdadır (ENISA, 2009, 2012). Üye ülkelerle de işbirliği yaparak AB içindeki tüm özel ve kamu kuruluşlarına vermiş olduğu rehberlik hizmetinin yanı sıra, kullanıcılara uyguladığı anketler sonrasında hazırlamış olduğu raporlar ve yapmış olduğu bilinçlendirme çalışmalarıyla da ENISA ulusal risk yönetimi ve bilgi güvenliği politikalarının geliştirilmesine katkı sağlamaktadır.

ENISA'nın özellikle bulut bilişim hizmetlerine ilişkin artan kaygıların giderilmesine yönelik olarak yapmış olduğu çalışma ve raporlarda, kişisel verilerin korunması ve

[57] Bkz. (Avrupa Konseyi, 2004b)
[58] Bkz. (Avrupa Konseyi, 2013c)

kapsamlı bilgi güvenliği politikalarını da içeren önerilere yer verilmektedir (ENISA, 2011). Kişisel verilerin korunmasına ilişkin denetimlerde ENISA'nın rolü, daha çok AB içinde bilgi güvenliği kültürü oluşturmaya yöneliktir. Bu nedenle, AB içinde bilgi güvenliği politikalarının geliştirilmesi ve gerekli önlemlerin alınması konusunda en büyük sorumluluğu ENISA üstlenmektedir (Avrupa Komisyonu, 2011b). McCumber bilgi güvenliği modelinde yer alan güvenlik önlemlerine ilişkin sorumlulukların AB içindeki sahibi ve uygulayıcısı ENISA'dır. ENISA bu sorumlulukları, AB ülkelerinde oluşturulan "bilgisayar olaylarına müdahale ekipleri"[59] ile yürütmekte olduğu ortak çalışmalarla yerine getirmektedir. Yetki ve sınırları açık olarak çizilmiş olan ENISA, Türkiye için de kurulması öngörülen "Ulusal Bilgi Güvenliği Teşkilatı" için örnek bir model niteliği taşımaktadır (BMD, 2007).

2.4. TÜRK HUKUK MEVZUATINDA KİŞİSEL VE HASSAS VERİLERİN KORUNMASI

Bilgi teknolojileri ve internet kullanım oranlarının artışına bağlı olarak Türkiye'de her geçen gün kişisel verilerin bulunduğu ortamların ve bu ortamlara bilgilerini sunan kullanıcıların sayıları artmaktadır. Devlet kurumlarının internet altyapısı üzerinden kişisel veri toplandıkları uygulamaların yanı sıra, çevrimiçi ticaret amacıyla kişisel verileri elde ederek sistemleri üzerinde bulunduran yüzlerce şirket, bankalar ve sosyal paylaşım siteleri bu konudaki risklerin artmasına neden olmaktadır. Dolaylı olarak kişisel verilerin korunması konusu; hukukun farklı alanlarına yayılarak Anayasa Hukuku, Ceza Hukuku, Özel Hukuk ve İdare Hukukunun konusu haline gelmiştir. Ancak bu konudaki sorunların çözümüne bir kişisel verileri koruma kanunu yerine farklı hukuksal düzenlemeler içinde farklı gerekçelerle yer verilmesi, alınacak önlemlerin dayanağı olma açısından konuyu karmaşık hale getirmektedir. Üniversitelerde kişisel verilerin korunması konusunu ele alan bu çalışmada, hukuksal düzenlemeler içinde yer alan ve üniversitelerle ilişkili olan kısımlar irdelenmiştir.

[59] **Bilgisayar Olaylarına Müdahale Ekipleri, BOME (Computer Emergency Response Team, CERT):** Kurum ve kuruluşlar arasında koordinasyonu sağlayarak bilgi sistem güvenliğine yönelik önleyici ve düzeltici servis sunan ekiptir.

2.4.1. Anayasa Çerçevesinde Kişisel ve Hassas Verilerin Korunması

Kişisel verilerin korunmasına yönelik hukuksal düzenlemeleri bulunan birçok AB ülkesinin anayasalarında, kişisel verilerin korunmasına yönelik maddelere, özel yaşamın gizliliği ya da kişilik haklarını içeren bölümlerde yer verildiği görülmektedir (Constitution.eu, 2013). Bu anayasaların birçoğu, kişisel verilerin korunması konusundaki endişelerin ve tartışmaların başlamasından daha önce kabul edilmiştir. Hollanda ve İspanya gibi yeni anayasalara sahip ülkelerde ise kişisel verilere erişim haklarının düzenlendiği görülmektedir (Netherlands Constitution, 2008). Kişisel verilerin korunmasına yönelik çalışmalar, bu alanda ülkelerin anayasaya yapmış oldukları eklemelerin yeterli olmadığını ve ayrı bir veri koruma kanunu yapılmasının zorunlu hale geldiğini göstermiştir. T.C. Anayasası'nda da kişisel verilerin ve özel hayatın gizliliğinin korunmasına yönelik anayasal temeller yer almaktadır. AB ülkeleri genelinde olduğu gibi, Anayasa'da kişisel verilerin korunmasına yönelik düzenleme "özel hayatın gizliliği" isimli bölüm altında yapılmıştır (T.C. Anayasası, 1982). Bu bakımdan anayasal hak olarak kişisel verilerin korunması, özel yaşamın gizliliği hakkı içinde değerlendirilmektedir. Ancak yeni anayasa çalışmaları kapsamında hazırlanan taslak metinlerde (STA, 2007), yeni anayasalara sahip AB ülkelerinde olduğu gibi, kişisel bilgilerin korunmasına dair maddelerin ayrı bir başlık altında yer aldığı görülmektedir.

Kişisel verilerin korunması konusunun anayasal dayanağı, 2010 yılı öncesinde temel hak ve özgürlüğe ilişkin maddelerdi (md.20, m.5, m.17, m.22 ve m.25). Ancak bu konuda açık ifadelerin yer almaması, konuya mesafeli yaklaşılmasına neden olmuştur. Bireylere kendisiyle ilgili kişisel verilerin korunmasını isteme, kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, silinmesini veya düzeltilmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkı, 12.09.2010 tarihinde yürürlüğe giren 5982 sayılı Kanunun 2/3. maddesi ile Anayasa'nın 20. Maddesine eklenerek sağlanmıştır[60]. Aynı fıkrada, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği de belirtilmiştir (T.C. Anayasası, 1982). Burada

[60] **T.C. Anayasası, 20. Madde:** (Ek fıkra: 12/9/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

işaret edilen kişisel verilerin korunmasına ilişkin usul ve esasları düzenleyen kanunun olmaması ise bu konudaki önemli eksikliklerden biridir. 2008 yılında hazırlanan kişisel verilerin korunması kanun tasarısı, araya seçim girmesi nedeniyle hükümsüz kalmıştır[61]. Bu tasarının yenilenmesine ilişkin çalışmalar 2011 yılından itibaren yeniden başlamış ve 2014 yılında yeni bir tasarı hazırlanmıştır. Bununla beraber, Anayasanın 20. Maddesinde kişisel verilerin işlenebileceği hallerin kanunda açıkça yer alması zorunluluğu bulunmasına karşın, "herhangi bir belirleme ve sınırlama yapılmaksızın doğrudan kişisel verilerin temin edilmesi ve işlenmesi" Anayasa Mahkemesi tarafından Anayasanın 20. Maddesine aykırı bulunmaktadır (Anayasa Mahkemesi, 2014). Anayasa Mahkemesinin vermiş olduğu bu kararın gerekçesinde; Anayasanın 13. ve 20. Maddelerinde yer alan güvencelere rağmen, bilgi toplama, saklama, işleme ve değiştirme yetkisi olan idareye karşı ilgili kişilerin korumasız bırakıldığı belirtilmektedir.

Anayasa'nın 20. Maddesi kişisel verilerin korunmasını öngörmekte ve kanunda öngörülen hallerde veya kişinin açık rızası ile kişisel verilerin işlenebileceğini söylemektedir. Bu madde ile birlikte, kişisel veriler üzerinde veri sahipleri mutlak hak sahibi olmaktadırlar. Kişisel verilerin korunmasına yönelik temel hak ve hürriyetin sadece kanunla sınırlandırılabileceği ise Anayasa'nın 13. Maddesinde ifade edilmektedir[62]. Buna göre, kişisin açık rızası olmaksızın kişisel verilerin işlenmesinin ancak kanun ile yapılması ve çıkarılan kanunun anayasaya uygun olması gerekmektedir. Ayrıca kişisel verilerin işlenmesi ve transferine ilişkin uygulamalarda görev alan personelin, Anayasa'nın 137. Maddesinde[63] "kanunsuz emir" başlığı altında ifade edilen hükümlere uygun olarak hareket etmeleri önem taşımaktadır.

---

[61] **Türkiye Büyük Millet Meclisi İç Tüzüğü'nün 77. Maddesi:** Bir yasama döneminde sonuçlandırılamamış olan kanun tasarı ve teklifleri hükümsüz sayılır. Ancak, Hükümet veya Türkiye Büyük Millet Meclisi üyeleri bu tasarı veya teklifleri yenileyebilirler.

[62] **T.C. Anayasası, 13. Madde**: Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.

[63] **T.C. Anayasası, 137. Madde**: Kamu hizmetlerinde herhangi bir sıfat ve suretle çalışmakta olan kimse, üstünden aldığı emri, yönetmelik, tüzük, kanun veya Anayasa hükümlerine aykırı görürse, yerine getirmez ve bu aykırılığı o emri verene bildirir. Ancak, üstü emrinde ısrar eder ve bu emrini yazı ile yenilerse, emir yerine getirilir; bu halde, emri yerine getiren sorumlu olmaz.

Konusu suç teşkil eden emir, hiçbir suretle yerine getirilmez; yerine getiren kimse sorumluluktan kurtulamaz.

Askerî hizmetlerin görülmesi ve acele hallerde kamu düzeni ve kamu güvenliğinin korunması için kanunla gösterilen istisnalar saklıdır.

Doğrudan kişisel verilerin korunmasını hedef almadığı halde, kişisel verilerin korunmasının farklı anayasal temelleri de bulunmaktadır. Anayasa'nın 25[64]. ve 26. Maddesinde ifade edilen "düşünceyi açıklama ve yayma hürriyeti" bu kapsamda değerlendirilebilir. Kişisel verilerin korunması ile özel yaşamın ve düşünce özgürlüğünün korunması arasındaki ilişki, Anayasa Mahkemesi tarafından verilen kararların içeriğinde açık olarak görülebilmektedir (Anayasa Mahkemesi, 2008). Bu ve benzeri durumlarda hak ve hürriyetleri ihlâl edilen veri sahibinin yetkili makamlara başvuru hakkı ise Anayasa'nın 40. Maddesinde[65] ifade edilerek sağlanmıştır.

Kişisel verilerin korunmasına ilişkin olarak anayasada yer alan düzenlemeler içinde Anayasası'nın 90. Maddesi[66] de önemli bir yere sahiptir. Anayasanın 90. Maddesinde, imzalanan milletlerarası antlaşmaların yasa hükmünde olduğu, aykırılığı nedeniyle Anayasa Mahkemesine başvurulamayacağı ve milletlerarası antlaşmaların aynı konu üzerinde kanunlar ile farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası antlaşmaların hükümlerinin esas alınacağı ifade edilmektedir. Bu madde, Türkiye'nin de taraf olduğu AİHS'nin 8. Maddesinde[67] yer alan kişisel verilerin korunmasına ilişkin hükümlere ve sözleşmenin yargı organı olan AİHM kararlarına uyulması açısından önem taşımaktadır. AİHS'de kişisel verilerin korunması konusu ayrı bir hak alanı olarak yer almamaktadır. Ancak AİHM'nin konuya ilişkin olarak verdiği kararlar ve yorumu, kişisel verilerin AİHS'nin 8. Maddesi kapsamında değerlendirildiğini göstermektedir (Küzeci, 2011). Kişisel verilerin korunmasına yönelik olarak geliştirilecek bilgi güvenliği politikaları ve yapılacak hukuksal düzenlemeler,

---

[64] **T.C. Anayasası, 25. Madde:** Herkes, düşünce ve kanaat hürriyetine sahiptir.

Her ne sebep ve amaçla olursa olsun kimse, düşünce ve kanaatlerini açıklamaya zorlanamaz; düşünce ve kanaatleri sebebiyle kınanamaz ve suçlanamaz.

[65] **T.C. Anayasası, 40. Madde**: Anayasa ile tanınmış hak ve hürriyetleri ihlâl edilen herkes, yetkili makama geciktirilmeden başvurma imkânının sağlanmasını isteme hakkına sahiptir.

(Ek fıkra: 3/10/2001-4709/16 md.) Devlet, işlemlerinde, ilgili kişilerin hangi kanun yolları ve mercilere başvuracağını ve sürelerini belirtmek zorundadır.

Kişinin, resmî görevliler tarafından vâki haksız işlemler sonucu uğradığı zarar da, kanuna göre, Devletçe tazmin edilir. Devletin sorumlu olan ilgili görevliye rücu hakkı saklıdır.

[66] **T.C. Anayasası, 90. Madde**: … Usulüne göre yürürlüğe konulmuş milletlerarası andlaşmalar kanun hükmündedir. Bunlar hakkında Anayasaya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz. (Ek cümle: 7/5/2004-5170/7 md.) Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası andlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası andlaşma hükümleri esas alınır.

[67] **AİHS, 8. Madde:** 1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.

Anayasa'nın 90. Maddesi ve buna bağlı olarak milletlerarası antlaşmalar da dikkate alınarak yapılmalıdır.

2.4.2. Türk Ceza Kanunu'nda Kişisel ve Hassas Verilerin Korunmasına İlişkin Düzenlemeler

Kişisel verilerin (yazılı-basılı ya da elektronik ortamda) kaydedilmesi, hukuka aykırı olarak dağıtılması ya da ele geçirilmesi konuları 5237 sayılı Türk Ceza Kanunu'nun (TCK) 135. ve 136. Maddelerinde düzenlenmiş ve kişisel verilerin korunmasına ilişkin suç ve yaptırımlar belirlemiştir. Ancak kişisel verilerin korunmasına yönelik temel ilkelerin tanımlandığı bir hukuksal düzenlemenin bulunmaması, TCK açısından önemli bir eksiklik olarak değerlendirilebilir. Bu eksiklik göz önüne alınarak, TCK'da kişisel verilerin korunmasına ilişkin maddeler değerlendirilirken, Kişisel Verilerin Korunması Kanunu Tasarısı'nın da uyumlu olduğu AB veri koruma kanununda ve milletlerarası sözleşmelerde yer alan kişisel veri tanımı[68] dikkate alınmaktadır. TCK'nın gerekçesinde de benzer şekilde "gerçek kişilerle ilgili her türlü bilgi kişisel veri olarak kabul edilmelidir" ifadesine yer verilmiştir (Hafızoğulları ve Özen, 2009).

TCK'nın 135. Maddesinde[69] kişisel verilerin hukuka aykırı olarak kaydedilmesi suç olarak düzenlenmiştir. 135. Maddenin 1. Fıkrasında ve 2. Fıkranın bir bölümünde kaydedilen bilgilerin "hukuka aykırı" olma şartı yer almaktadır. Kişilerin siyasi, felsefi veya dini görüşleri ve ırki kökenlerini gösteren bilgilerin kişinin rızası dışında kaydedilmesinin ise tamamen hukuka aykırı olduğu değerlendirilmektedir. Kanunun gerekçesinde ve hazırlık çalışmalarında bu ayrımın nedenine ilişkin bir açıklama yer almamaktadır (Hafızoğulları ve Özen, 2009). Kaydedilen bilginin bilgisayar ya da kâğıt ortamında olmasına ilişkin ayrım gözetilmemiştir. Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçun oluşması için yeterlidir. Üniversiteler açısından bu maddeye ilişkin olarak dikkat edilmesi gereken nokta, kişilerin siyasi, felsefi veya dini görüşleri ve ırki

[68] **Kişisel Veri**: Belirli ya da kimliği belirlenebilir gerçek kişi ile ilgili her türlü bilgi

[69] **TCK, 135. Madde:** (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.
(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.

kökenlerini gösteren bilgilerin herhangi bir gerekçeyle kaydedilmemesi, diğer kişisel bilgilerin ise hukuka aykırı[70] olarak kaydedilmemesidir. Kamu kurumlarının sunmuş olduğu kamu hizmetlerine ilişkin olarak kanun hükümleri kapsamında kaydedilen bilgiler bu maddede tanımlanan suçu oluşturmamaktadır. 135. Madde kapsamında düzenlenen suçun gerçekleşmesi için, zararın oluşması şartı aranmamakla birlikte sadece bilginin ilgili kişinin rızası olmaksızın hukuka aykırı olarak kaydedilmiş olması yeterli görülmektedir. Bu madde kapsamında, kişisel verilerin elde edilmesi, işlenmesi/kullanılması ve depolanması gibi bilginin durumunu nitelendiren ve kişisel verilerin korunması açısından çok önemli olan diğer unsurlara yer verilmemiştir. Bu açıdan değerlendirildiğinde, bilginin hukuka aykırı olarak elde edilmesi ve kullanımından kaynaklanan kişisel hakların ihlâli karşısında 135. Madde yetersiz kalmaktadır (Ketizmen, 2008).

TCK'nın 136. Maddesinde[71] verileri hukuka aykırı olarak verme veya ele geçirme suç olarak düzenlenmiştir. Kişisel verilerin erişim yetkisi bulunmayan üçüncü kişilere verilmesi ya da hukuka uygun olarak kaydedilmiş verilerin üçüncü kişiler tarafından ele geçirilmesi 136. Madde kapsamındaki suçun oluşması için yeterlidir. Verilerin nasıl verildiğine ilişkin detayların önemi bulunmamaktadır. Ancak internet ortamında "verme" ve "ele geçirme" fiillerinin hukuka aykırı olma şartının nasıl değerlendirileceği konusu açık değildir (Doğan, 2005). İnternet ortamında çoğu zaman bu fiillerin kesin delillerle ortaya konulabilmesi teknik yöntemlerle mümkün olamamaktadır. Verinin daha önce hukuka aykırı ya da hukuka uygun olarak elde edilmiş olmasının bu madde açısından bir önemi yoktur. Asıl önemli olan, kişisel verilerin hukuka aykırı olarak üçüncü kişilere verilmesi, yayılması ya da ele geçirilmesidir. Suçun bir kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmesi ise suçun nitelikli halini oluşturmaktadır[72].

---

[70] **Hukuka Aykırılık:** Kanun hükmünün uygulanması, hakkın kullanılması ya da kişinin rızasının olması durumu haricindeki nedenlerdir. Hukuka uygunluğun sebepleri, TCK 24/1, 25/1 ve 26/1-2 maddelerinde yer almaktadır.

[71] **TCK, 136. Madde:** Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.

[72] **TCK, 137. Madde:** (1) Yukarıdaki maddelerde tanımlanan suçların;
a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,
b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.

TCK'nın 138. Maddesinde[73] verileri yok etmeme suçu düzenlenmiştir. Kullanım süresi sona eren bilginin uygun yöntemlerle yok edilmesi, kişisel verilerin korunması konusundaki temel ilkelerden biridir. Ancak bu madde kapsamında süreye odaklanıldığı ve verinin kullanımı sona ermiş olsa dahi kanunların belirlediği sürenin sonuna kadar saklanabileceği anlaşılmaktadır. Genel itibariyle önemli bir eksikliği giderecek şekilde düzenlenen 138. Maddeyle, kullanım amacı ortadan kalkan bilgilerin kullanım süresi sonuna kadar tutulmasına izin verilerek yeni risklerin oluşumu göz ardı edilmiştir. 138. Maddede yer alan verilerin "sistem içinde yok edilmesi" ifadesi, kapsamının elektronik ortamda işlenen verilerle sınırlı olduğunu düşündürmektedir (Ketizmen, 2008). Bununla beraber, verinin geri dönüşü olmayacak biçimde yok edilmesi uygun teknik yöntemlerin kullanılması ile mümkün olabilmektedir (Henkoğlu, 2011). Bu maddede verilerin yok edilmesinden tam olarak hangi seviyede yok etme işleminin kast edildiği, uygun teknik yöntemlerle yok edilmeyen verilerin geri dönüşümünün sağlanması halinde kimin sorumlu olacağı ya da bunun bir ihmâl olarak değerlendirilip değerlendirilmeyeceği açık değildir.

TCK'da doğrudan kişisel verilerin korunmasına yönelik olarak düzenlenmeyen, ancak üniversitelerde kişisel verilerin korunmasına yönelik sonuçlarla ilişkili maddeler de bulunmaktadır. 132. Maddenin 3. Fıkrasında[74] yer alan haberleşmenin ifşa edilmesine ilişkin düzenleme, özellikle bilgi merkezlerinin danışma hizmetlerini ve bu hizmetin verilmesi aşamasındaki kayıtların korunması ile yakından ilgilidir. 132. Maddede ihlalin nasıl gerçekleşeceği ve haberleşme aracının (e-posta, anlık mesajlaşma, telefon vd.) belirtilmemiş olması, gelişen teknolojiye uyumlu ve güncel olması açısından önemlidir. 132. Maddenin genelinde haberleşme hürriyeti güvence altına alınmıştır. Haberleşme hürriyetinin hâkim kararına ya da kanunla yetkili kılınan merciin yazılı emrine bağlı olarak engellenmesi ve gizliliğine dokunulmasını gerektirebilecek sebepler Anayasanın 22. Maddesinde belirtilmektedir[75]. 132. Maddenin 3. Fıkrasında dikkati çeken diğer nokta

---

[73] **TCK, 138. Madde:** Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir.

[74] **TCK, 132/3. Madde:** (3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. (Ek cümle: 2/7/2012-6352/79 md.) İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

[75] **T.C. Anayasası, 22. Madde**: Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili

ise, haberleşmede diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa edilen haberleşme içeriğinin, mağdur üzerinde herhangi bir zarara neden olması şartının aranmamasıdır.

TCK'da kişisel verileri koruma sorumluluğunu içeren düzenleme 258. Madde[76] ile yapılmıştır. Kişisel verileri işleyen personelin görevi nedeniyle edindiği bilgilerin gizli kalmasını ve yetkisiz kişilere verilmemesini öngören bu madde ile kişisel veriler için dolaylı olarak koruma sağlanmaktadır.

TCK'da bilişim alanında suçlar başlığı altında düzenlenmiş 243. ve 244. Maddeler[77] de üniversitelerde veri güvenliğinin sağlanmasına ve dolaylı olarak kişisel verilerin korunmasına katkı sağlamaktadır. Bilişim sistemine izinsiz girme, sistemi engelleme bozma, verileri yok etme veya değiştirme ile ilgili suçlar hakkındaki düzenlemeleri içeren 243 ve 244. Maddeler, kişisel verilerin korunması açısından da dikkate alınmalıdır. Üniversitelerde kişisel verileri işleyen birimler, bilişim alanındaki suçlarla karşılaşmaları ve kişisel verilerin ihlali halinde yetkili makamlara bildirimde bulunmakla yükümlüdürler. Bildirimde ihmal ya da gecikme olması halinde, TCK'nın 279. Maddesi[78] gereğince cezai yaptırım uygulanması öngörülmüştür.

---

kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir.

[76] **TCK, 258. Madde:** (1) Görevi nedeniyle kendisine verilen veya aynı nedenle bilgi edindiği ve gizli kalması gereken belgeleri, kararları ve emirleri ve diğer tebligatı açıklayan veya yayınlayan veya ne suretle olursa olsun başkalarının bilgi edinmesini kolaylaştıran kamu görevlisine, bir yıldan dört yıla kadar hapis cezası verilir.

(2) Kamu görevlisi sıfatı sona erdikten sonra, birinci fıkrada yazılı fiilleri işleyen kimseye de aynı ceza verilir.

[77] **TCK, 243. Madde:** (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

TCK, 244. Madde: (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

[78] **TCK, 279. Madde:** (1) Kamu adına soruşturma ve kovuşturmayı gerektiren bir suçun işlendiğini göreviyle bağlantılı olarak öğrenip de yetkili makamlara bildirimde bulunmayı ihmal eden veya bu hususta gecikme gösteren kamu görevlisi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır.

2.4.3. Türk Medeni Kanunu Çerçevesinde Kişisel ve Hassas Verilerin Korunması

Özel hukukta kişisel verilerin korunması, kişilik haklarının korunması ile ilişkili olarak değerlendirilmektedir. Hukuksal düzenlemelerde kişilik hakkının tanımı yapılmadığı ve içeriğinin ortaya konulmadığı görülmektedir. Ancak literatürde kişisel veriler ve özgürlükler gibi kişisel değerler üzerindeki hakların kişilik hakkını ifade ettiği görüşünün hâkim olduğu görülmektedir (Kaya, 2010). Kişilik hakkı, özel yaşam alanı ve mahremiyeti de içeren bir kavramdır. Özel yaşam alanının kişisel bir değer ve varlık olarak korunması, bireylerin kendi yaşam biçimlerini ve kişiliklerini geliştirmelerine olanak sağlamaktadır (Yüksel, 2003). Medeni kanun ve özel hukuk alanındaki diğer kanunlarda (Borçlar Kanunu, Türk Ticaret Kanunu, Hukuk Usulü Muhakemeleri Kanunu, Fikir ve Sanat Eserleri Kanunu) kişilik haklarının korunmasına yönelik hukuksal düzenlemeler bulunmaktadır. Kişisel verilerin kişilik hakkının bir parçası olduğu görüşü (Kılıçoğlu, 2013) dikkate alındığında, gizli ve özel yaşam alanlarının[79] korunmasına yönelik hukuksal düzenlemelerin kişisel verilerin korunmasında da etkin olduğu söylenebilir.

Medeni Kanun'un 24.[80] ve 25. Maddesinde gizli ve özel yaşam alanına yönelik saldırılara karşı bireyin korunmakta olduğu ve kişilik hakkının benimsenmiş olduğu görülmektedir. Kişiliğin bütün olarak korunduğu bu maddelerle, kişiyi oluşturan değerlerin de korunacağı değerlendirilmektedir (Zevkliler, Gökyayla ve Acabey, 2000). Medeni Kanun ile sağlanan bu koruma, Borçlar Kanununun 49. Maddesi[81] ile tamamlanmaktadır. Ancak kişisel verilerin korunmasına yönelik temel ilkelerin açıklandığı bir veri koruma kanununun bulunmaması, Medeni Kanunda kişisel hakların korunmasına ilişkin genel

(2) Suçun, adlî kolluk görevini yapan kişi tarafından işlenmesi halinde, yukarıdaki fıkraya göre verilecek ceza yarı oranında artırılır.

[79] **Gizli Yaşam Alanı:** Bireyin sadece kendisi için saklı tuttuğu ve diğer insanların erişmesini istemediği gizlilik alanıdır.

Özel Yaşam Alanı: Bireyin sadece kendisine yakın kişilerle (aile ve arkadaş çevresi gibi) paylaştığı gizlilik alanıdır.

[80] **Türk Medeni Kanunu, 24. Madde:** Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.

[81] **Türk Borçlar Kanunu, 49. Madde:** Kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür.

Zarar verici fiili yasaklayan bir hukuk kuralı bulunmasa bile, ahlaka aykırı bir fiille başkasına kasten zarar veren de, bu zararı gidermekle yükümlüdür.

hükümlerin bu açıdan yorumlanmasını zorlaştırmakta ve yetersiz kalmaktadır. Ayrıca, özel hukuk ve kamu hukukunun aynı anda ilgi alanına giren saldırılara ilişkin belirsizliklerin giderilmesi için de veri koruma kanununa ihtiyaç duyulmaktadır.

Medeni Kanunun 25. Maddesinde[82] saldırı tehlikesinin önlenmesi ve sürmekte olan saldırıya son verilmesine ilişkin olarak izlenecek yöntem belirtilmiştir. Ancak bu maddede yer alan saldırı tehlikesinin önlenebilmesi için, önceden ihlalin gerçekleşeceğine yönelik açık bir tehdidin (örneğin, kişisel verilerin bir ilanda yer alacağı bilgisinin verilmesi gibi) ortaya çıkmış olması gerekmektedir. Bu nedenle, Medeni Kanunda yer alan düzenlemenin uygulamada önleyici olmaktan uzak olduğu ve saldırıya son verilmesinde daha etkin olabileceği değerlendirilmektedir (Akipek, Akıntürk ve Karaman, 2012).

Özel yaşamın tanımlanmasına ilişkin belirsizlikler, kişinin başkalarıyla ilişki kurduğu kamusal ve özel alanda kişisel verilerin korunması konusunda da tartışmalara neden olmaktadır. Ancak AİHM'nin kararları incelendiğinde, kişinin başkalarıyla ilişki kurduğu tüm alanların özel yaşamın sınırları içinde olduğu anlaşılmaktadır (Küzeci, 2011). Bu yönüyle değerlendirildiğinde, kamusal alanda yapılan görüntü kayıtları, internet üzerinden kurulan iletişim ve e-posta kayıtları, özel yaşamın sınırları içinde güvence altına alındığı değerlendirilmektedir. Ancak özel yaşam alanı ihlal edilen kişinin rızasının bulunması kamu yararının bulunması ya da kanunun verdiği yetkinin kullanılması halinde, kişilik hakkına yapılan müdahale medeni hukuk çerçevesinde hukuka uygun olarak değerlendirilmektedir.

[82] **Türk Medeni Kanunu, 25. Madde:** Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.
Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir.

2.4.4. Kişisel Verilerin Korunması Kanun Tasarısı

2.4.4.1. Türkiye'de Kişisel Verilerin Korunması Kanunu Süreci, Amacı ve Önemi

Türkiye, 108 sayılı Kişisel Verilerin Elektronik Ortamda İşlenmesi Bağlamında Bireylerin Korunmasına Dair Avrupa Konseyi Sözleşmesini ilk imzalayan ülkelerden olmasına rağmen, sözleşmenin 4. maddesi gereğince yapılması zorunlu olan veri koruma yasasının 30 yılı aşan bir süre içinde yapılamaması nedeniyle 108 sayılı sözleşme onaylanmamıştır (Avrupa Konseyi, 2013b)[83]. Ancak 11 Aralık 1999 tarihinde gerçekleşen AB Helsinki zirvesi sonrasında Türkiye'nin tam üye adayı olarak kabul edilmesiyle birlikte, tam üyelik sürecine ilişkin çalışmalarla beraber mevzuat uyumu için de çalışmalar başlatılmıştır. Bu kapsamda, 95/46/EC sayılı veri koruma direktifi ile uyumlu bir hukuksal düzenlemenin yapılması öngörülmüş ve 2003 Ulusal Programı içinde yer alan öncelikler listesinde bu konuya yer verilmiştir (T.C. AB Bakanlığı, 2003). 2003-2013 yılları arasında kişisel verilerin korunmasına ilişkin olarak ulusal mevzuatın AB müktesebatı ile uyumlu hale getirilememesi, Avrupa Komisyonu tarafından hazırlanan düzenli ilerleme raporlarının içeriğinde de eleştirilen noktalar arasında yer almıştır. En son hazırlanan 2012 yılına ait ilerleme raporunda, ulusal mevzuatın AB müktesebatı ile uyumlu hale getirilmesi, bağımsız bir veri koruma ve denetleme biriminin kurulması, 108 sayılı Avrupa Konseyi Sözleşmesi'nin ve 181 nolu ek protokolün onaylanmasının gerektiğine vurgu yapılmış ve veri korumaya ilişkin mevzuatın olmamasının polis ve yargı organları arasındaki işbirliğini engellediği ifade edilmiştir (Avrupa Komisyonu, 2012d). Kişisel Verilerin Korunması Kanunu (KVKK), Türkiye'nin AB müktesebatına uyum programı (2007-2013) içerisinde yer alan "yargı ve temel haklar" başlığı altında, yeni çıkarılacak yasal düzenlemeler arasında da bulunmaktadır. Bu belgede KVKK'nın amaçlarının, "kişisel verilerin korunması suretiyle, kişinin dokunulmazlığı, maddi ve manevi varlığı ile temel hak ve özgürlüğünü korumak ve kişisel verilerin toplanması, işlenmesi ve muhafazası konularında temel ilkeleri tayin etmek" olduğu belirtilmektedir (T.C. AB Bakanlığı, 2010). KVKK'nın uyum sağlaması öngörülen AB mevzuatı içerisinde 108 sayılı Avrupa Konseyi Sözleşmesi ve 95/46/EC

[83] Türkiye, 108 sayılı sözleşmede imzası bulunan ancak Avrupa Konseyi üyesi 47 ülke içinde bu sözleşmeyi Kasım 2014 itibariyle onaylamayan tek ülkedir.

sayılı veri koruma direktifinin bulunması, Kişisel Verilerin Korunması Kanunu Tasarısının (KVKKT) hedefi ve içeriği hakkında genel olarak fikir vermektedir. AB uyum süreci ile paralel olarak hazırlanan diğer belgelerin (adalet, özgürlük ve güvenlik, bilgi toplumu ve medya vd.) içeriğinde de kişisel verilerin korunmasına ilişkin hukuksal düzenlemelerin yapılacağı ifade edilmiştir.

Uluslararası bilişim suçlarıyla ilişkili olarak Avrupa Konseyi tarafından hazırlanan en önemli düzenlemelerden biri olan 185 Sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesini, Türkiye de 2011 yılında imzalamıştır. Sözleşmeyi imzalayan ülkelerin bu sözleşmenin yaptırım gücünden yararlanabilmesi için, Meclis onayından geçmesi ve iç hukuka uyarlanması gerekmektedir. Sözleşmenin 22 Nisan 2014 tarihinde 6533 Sayılı Kanun ile TBMM tarafından "çekince ve beyanlarla" onaylanması uygun bulunmuş ve 2 Mayıs 2014 tarihinde yürürlüğe girmiştir (6533 Sayılı Kanun, 2014). Sözleşmenin iç hukuka uyarlanması konusundaki en önemli eksikliklerden biri ise, kişisel verilerin korunması kanununun bulunmamasıdır. Sözleşme, emniyet teşkilatları arasında bilgi değişimi ve paylaşımına da imkân sağlamaktadır. Ancak kişisel verilerin korunmasına ilişkin olarak iç hukukta gerekli düzenlemenin bulunmaması, bu sözleşmeyi imzalayan ülkelerle kişisel verilerin kontrolsüz ya da tek taraflı olarak paylaşılmasına olanak sağlayabilecektir. Nitekim adli bilgi paylaşımı ve gümrük idareleri arasındaki bilgi paylaşımı konusunda benzer olumsuzlukların yaşandığı görülmektedir. Avrupa Konseyi'ne üye diğer devletler, 108 sayılı sözleşmenin onaylanmamış olmasını (ya da bunun nedeni olan Türkiye'de kişisel verilerin korunmasına ilişkin eşdeğer bir hukuksal düzenleme olmamasını) gerekçe göstererek, Türk mahkemelerinin adli yardım istemlerini geri çevirmektedirler (T.C. Başbakanlık, 2014a). KVKK'nın yürürlüğe girmesi Avrupa Konseyi üyesi devletlerle bilgi paylaşımının önünü açmakla birlikte, uluslararası boyutta siber suçlarla mücadele edilmesi ve bilgi güvenliği önlemlerinin daha etkin olarak alınabilmesine de önemli katkılar sağlayacağı düşünülmektedir.

Günümüzde kişisel verilerin elektronik ortamda işlenmesi ve ilgililerin bu verilerden yararlanmasını kolaylaştırmak kaçınılmaz hale gelmiştir. Ancak bu verileri işlerken kişiliğin ve temel hak ve hürriyetlerin korunması da geleneksel yöntemlere nazaran daha büyük bir sorun olarak ortaya çıkmıştır. Bu çalışmada da üniversiteler açısından

incelendiği ve görüldüğü gibi Türk Hukuk Mevzuatı içerisinde yer alan birçok hukuksal düzenlemede doğrudan ya da dolaylı olarak kişisel verilerin korunması konusuna yer verilmiştir. Ancak KVKKT'nın gerekçesinde de açıkça belirtildiği gibi, kişisel verilerin korunmasına ilişkin alanı bütüncül olarak düzenleyen bir kanun bulunmamaktadır. Örneğin TCK'nın 135 ve devamı maddelerinde yer alan fiillerin ne zaman hukuka aykırı, ne zaman hukuka uygun olduğunun belirlenmesinde sorunlar yaşanmaktadır (T.C. Başbakanlık, 2014a). Mevcut düzenlemeler kişisel verilerin korunması amacıyla değil, ilgili olduğu sahalarda zamanın ihtiyaçlarına cevap vermesi amacıyla hazırlanmıştır (T.C. Başbakanlık, 2008b). Bu nedenle, modern hukuk sistemlerinde olduğu gibi, Türkiye'de de kişisel verilerin korunmasına yönelik genel bir çerçeve oluşturacak kanunun yürürlüğe girmesi ve kamu kurum ve kuruluşları ile farklı sektörlerin bu kanuna uyum sağlayacak düzenlemeleri yapmaları zorunlu hale gelmiştir. Devletlerin kişisel verilerin korunmasına yönelik olarak hukuksal düzenlemelere öncelik vermelerinin farklı gerekçeleri olabilmektedir. 30 yıldan daha fazla süreden beri kişisel verilerin korunması amacıyla çalışmaların ve hukuksal düzenlemelerin yapıldığı AB'de yeni düzenlemelerin gerekçesi olarak ekonomi ve çevrimiçi ticaretin geleceğine ilişkin kaygılar yer almaktadır (Henkoğlu ve Yılmaz, 2013). Türkiye'nin de veri koruma kanunu için gerekçeleri temelde AB ile benzer yönler taşımakla birlikte, AB'ye uyum sağlama sürecinin de önemli bir parçası olarak görülmektedir. Uluslararası ticari rekabet, bilişim suçlarına yönelik uluslararası işbirliğinin geliştirilmesi ve adli bilgilerin paylaşımına ilişkin etkenler, Türkiye'yi kişisel verilerin korunması konusunda AB ile paralel düşüncede olmaya zorlamaktadır. Bu açıdan bakıldığında, temel hak ve özgürlüklerin korunması amacı, KVKK'ya duyulan gereksinimler içinde ikinci öncelikli sırayı almaktadır.

Tasarının gerekçesinde kişisel verilerin işlenmesinin disiplin altına alınması ve Anayasa'da öngörülen temel hak ve özgürlüklerin korunmasının amaçlandığı belirtilmiştir. KVKKT'de kanunun amacının yer aldığı 1. Maddeye[84] de bu düşünce yansıtılmıştır.

[84] **KVKKT, 1. Madde:** (1) Bu Kanunun amacı; kişisel verilerin işlenmesinde kişinin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usulleri düzenlemektir.

2.4.4.2. KVKKT'de Dikkate Alınan Rehber İlkeler

Rehber ilkeler, dünyanın farklı bölgelerinde yer alan ülkelerin ulusal veri koruma kanunlarında dikkate alınan ve dört uluslararası kuruluşun da (AB, Avrupa Konseyi, OECD ve APEC[85]) benimsemiş olduğu ortak ilkelerdir (Greenleaf, 2012). KVKKT'de de kabul edilen ve gerekçede açıklanan rehber ilkeler, OECD tarafından kabul edilen rehber ilkeler dikkate alınarak oluşturulmuştur. Bu ilkelerin büyük bölümünün, 95/46/EC sayılı AK veri koruma direktifinde yer alan ilkelerle de uyumlu olduğu görülmektedir. KVKKT'de dikkate alınan rehber ilkelerin içeriğinde üniversitelerde kişisel verilerin işlenmesiyle de ilişkili birçok nokta bulunmaktadır[86].

KVKKT'de olduğu gibi, üniversitelerde ve diğer kurum/kuruluşlarda da bilgi güvenliği politikaları içinde kişisel verilerin korunmasına yönelik önlemlere yer verilirken çalışmaların bu rehber ilkelerin ışığında yapılması önem taşımaktadır. Tasarının kanunlaşması halinde, bu ilkelere aykırı olarak alınacak güvenlik önlemleri kanuna aykırı olacaktır. Ancak tasarı kanunlaşmasa dahi, bu ilkeleri dikkate almaksızın hazırlanan bilgi güvenliği önlemlerinin ya da hazırlanan politikaların kişisel hakları göz ardı etmiş olacağı değerlendirilmektedir.

2.4.4.3. KVKKT Çerçevesinde Üniversitelerde Kişisel ve Hassas Verilerin Korunması

Uluslararası belgeler ve 95/46/EC sayılı veri koruma direktifi dikkate alınarak hazırlanan KVKKT[87], dokuz bölümden oluşmaktadır. Kişisel verilerin işlenmesine ilişkin hususların yer aldığı ikinci bölüm ve verisi işlenen kişinin haklarının düzenlendiği üçüncü bölümde, rehber ilkelerin dikkate alındığı görülmektedir. Çerçeve niteliğindeki bu ilkelere bağlı kalarak, kurum ve kuruluşların da kendi kurallarını belirlemeleri gerekmektedir. Tasarıda hukuksal ya da bilgi teknolojilerine ağırlık veren detaylar yer almamaktadır. Bu nedenle, üniversitelerin farklı birimlerinin kişisel verilerle çalışma şartlarını değerlendirerek,

---

[85] **APEC (Asia-Pacific Economic Cooperation / Asya Pasifik Ekonomik İşbirliği):** 21 ülkenin katılımıyla oluşan ve dünya ekonomisinin %60'ını temsil eden uluslararası bir örgüttür.

[86] Bu çalışma sonunda geliştirilen bilgi güvenliği politikası içinde, KVKKT'te yer alan rehber ilkeler de dikkate alınmıştır.

[87] Tasarı için bkz. (http://web.tbmm.gov.tr/gelenkagitlar/metinler/362939.pdf)

teknoloji ve hukuksal tabanlı bir koruma politikasını KVKKT'da belirtilen temel ilkeler çerçevesinde oluşturmaları gerekmektedir. KVKKT'nin genel çerçeve ile sınırlı kalan bu yaklaşımının, diğer kurum ve kuruluşlar içinde de özel şartların ve teknolojik değişimlerin dikkate alındığı daha etkin bilgi güvenliği önlemlerinin alınmasına yardımcı olacağı değerlendirilmektedir.

KVKKT'nın 1. ve 2. Maddelerinde[88] kanunun amacı ve kapsamı ifade edilmiştir. Diğer hukuksal düzenlemelerde (Anayasa, TCK vd.) özel hayatın gizliliği ya da kişi haklarına vurgu yapılırken, KVKKT'da temel hak ve özgürlüğün korunmasına vurgu yapılmaktadır. Bu duruma ilişkin olarak AB'deki hukuksal düzenlemeler ışığında değerlendirme yapıldığında herhangi bir çelişki bulunmadığı söylenebilir. Zira literatürde ve AB yayın organlarında da bu üç kavramın iç içe geçmiş ve kişisel verilerin korunması açısından aynı anlamı ifade edecek şekilde farklı alanlarda kullanılmışlardır (Greenleaf, 2012). Tasarının 2. Maddesinde kişisel verilerin bulunduğu ortamın kısıtlanmamış olması, üniversitelerde işlenen tüm kişisel verileri kapsaması ve teknolojik gelişmeler karşısında güncelliğini kaybetmemesi açısından önemlidir. Bu konuya ilişkin olarak KVKKT'nın 24/1-a Maddesinde kanun hükümlerinin uygulanmayacağı ifade edilen istisnai durumun ise, 95/46/EC sayılı direktifin 3/2. Maddesiyle[89] uyumlu olduğu görülmektedir.

KVKKT'nın 4. Maddesinde kişisel verilerin bu ve diğer kanunlarda öngörülen hallerde işlenebileceği ifade edilmiştir. Ancak bu önemli nokta, 2010 yılında Anayasa'nın 20. Maddesine eklenen ek fıkrası ile birlikte değerlendirildiğinde, Anayasa'da yer alan ifadenin bir bölümünün tekrar edilmiş olduğu söylenebilir. Tasarının 5. Maddesinde de kişisel verilerin ancak kişinin açık rızası ile işlenebileceği ve bunun istisnaları belirtilerek Anayasa'da yer alan ifade genişletilmiştir. KVKKT'nin gerekçesinde, bu rızanın

---

[88] **KVKKT, 1. Madde:** (1) Bu Kanunun amacı; kişisel verilerin işlenmesinde kişinin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usulleri düzenlemektir.
KVKKT, 2. Madde: (1) Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen, otomatik olan veya olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.

[89] **AK 95/46/EC Direktifi, Madde 3/2:** This Directive shall not apply to the processing of personal data:
- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
- by a natural person in the course of a purely personal or household activity.

tereddüte yer bırakmayacak şekilde olması gerektiği vurgulanmıştır (T.C. Başbakanlık, 2014a). Daha önce de belirtildiği gibi, üniversitelerde toplanan ve işlenen kişisel veriler üzerinde veri sahiplerinin mutlak hak sahibi olduğu ve kişisin açık rızası olmaksızın kişisel verilerin işlenmesinin ancak kanun ile yapılabileceği bu maddelerle tekrar vurgulanmış ve verilerin işlenmesinde keyfiliğin önüne geçilerek bireylerin özel hayatlarının korunması amaçlanmıştır. 95/46/EC sayılı AK direktifi ile uyumlu olarak hazırlanan KVKKT'nin 5. Maddesinde[90] yer alan hukuka uygunluk sebepleri üniversitelerin bilgi güvenliği politikalarına yansıtılarak, kişisel verilerin işlendiği birimlerin bu şartları göz önünde bulundurmaları sağlanmalıdır. Veri sahibinin itirazları değerlendirilirken, tasarının 10. Maddesinde "ilgili kişinin hakları" başlığı altında düzenlenen hakların korunması da sağlanmalıdır. Bu madde ile veri sahibine tanınan hakların sınırlandırılmasına yönelik istisnalara ise 24. Maddede yer verilmiştir.

Kişisel verilerin elde edilmesinden imhasına kadar olan sürece ilişkin temel ilkelere tasarının 4. Maddesinde yer verilmiştir. Tasarının 4. Maddesiyle, AK'nin 108 sayılı sözleşmesinde belirtilen "temel ilkelerin iç hukukta yaşama geçirilmesi" yükümlülüğü, 95/46/EC sayılı AK direktifinin 6. Maddesiyle de uyumlu olarak yerine getirilmiştir. Veri sahibinin verilerin işlenmesine itirazı olmasa dahi üniversite birimlerinin bu ilkelere uyma yükümlülüğü bulunmaktadır. Kişisel verilerin işlenmesine ilişkin olarak tasarının 24/1-b Maddesinde belirtilen istisna ise, özellikle üniversite bilgi merkezleri açısından önem taşımaktadır. Üniversite bilgi merkezlerinde 24/1-b ve 7/1 Maddesine uygun olarak istatistik ya da bilimsel amaçla tutulan kişisel veriler, 4/2-d Maddesi gereğince işlendiği amaç için gerekli olan süre kadar saklanabilecektir. Bu istatistiksel bilgilerin kişi ile ilişkili olarak kullanılmaması (örneğin en çok erişilen veri tabanları listesi) ve tasarının 7. Maddesinin[91] dikkate alınarak anonim hale getirilmesi önem taşımaktadır. İhtiyaç

[90] **KVKKT, 5. Madde:** (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(3) Aşağıdaki şartlardan en az birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi, b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, c) Bir sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, d) İlgili kişinin kendisi tarafından alenileştirilmiş olması, e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

[91] **KVKKT, 7. Madde:** (1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir.

duyulmayan verilerin yok edilmesine ilişkin düzenleme de tasarının 7. Maddesi ile yapılmıştır. Ancak verinin imhasına ilişkin ifadenin, "geri dönüşümü mümkün olmayacak şekilde uygun teknik yöntemler kullanılarak" gibi bir tanımlama ile kuvvetlendirilmesinin yerinde olacağı değerlendirilmektedir. Her ne kadar bu konuya ilişkin usul ve esasların yönetmelikte gösterileceği belirtilse de, genel çerçevenin oluştuğu ifadenin kanunda yer alması yazılı bilgi güvenliği politikalarında ve yönetmeliklerde konunun eksiksiz olarak ele alınmasına katkı sağlayacaktır. Aksi halde, verinin uygun teknik yöntemler ve veri silme standartları kullanılmaksızın kalıcı olarak silinmemesi, kanunda yer alan "verinin yok edilmesi" ifadesini karşılamak için yeterli olmayacaktır[92].

KVKKT'nin 6/1. Maddesinde[93], TCK'nın 135/2. Maddesine ve 95/46/EC sayılı AK direktifinin 8. Maddesine paralel olarak özel niteliği olan verilerin genel kural olarak işlenemeyeceği düzenlenmiştir. Bu maddenin 2. Fıkrasında ise, yeterli önlemlerin alınması şartıyla özel niteliği olan kişisel verilerin işlenmesinin istisnai şartları verilmiştir. Üniversitelerin kişisel verileri işleyen birimlerinde, TCK'nın 135/2. Maddesine ilişkin olarak daha önce yapmış olduğumuz değerlendirmenin ve KVKKT'nın 6/2. Maddesinde düzenlenen yazılı rızanın alınması gibi istisnaların göz önüne alınmasının ve yazılı bilgi güvenliği politikaları belirlenirken bu iki düzenlemeden (TCK:135/2 ve KVKKT:6/2) birlikte yararlanılmasının daha uygun olacağı değerlendirilmektedir.

KVKKT'nın 8. Maddesinde kişisel verilerin (95/46/EC sayılı direktifin 25. ve 26. maddelerine uygun olarak) üçüncü kişilere ve yurtdışına aktarılmasına ilişkin düzenlemeler yer almaktadır. 8. Maddede kişisel verilerin kural olarak ilgili kişinin rızası olmaksızın üçüncü kişilere aktarılamayacağı belirtilse de, bu maddenin 2. Fıkrasında bazı

(2) Kişisel verilerin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir.

(3) Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanun hükümleri saklıdır.

[92] KVKKT'nin 7. Maddesine ilişkin gerekçede verilerin "silinmesi" ile kayıt ortamındaki verinin kalıcı olarak silinmesinin, "yok edilmesi" ifadesi ile verilerin kaydedildiği ortamın geri dönüşümü mümkün olmayacak şekilde imha edilmesinin kast edildiği belirtilmektedir. Ancak kanaatimizce bu kullanım teknik ifade açısından uygun olmadığı gibi, kanun maddesinden bu ifadenin doğru anlaşılmasında da sorunlar yaşanabilecektir.

[93] **KVKKT, 6/1. Madde:** (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, dernek, vakıf ya da sendika üyeliği, sağlığı veya cinsel hayatıyla ilgili verileri, özel nitelikli kişisel veriler olup bunların işlenmesi yasaktır.

istisnalara yer verilmiştir. Üniversitelerde kişisel verileri işleyen birimlerin, kişisel verilerin üçüncü kişilere ya da yurtdışına aktarılmasına ilişkin önemli sorumlulukları bulunmaktadır. Kişisel verilerin kaydedildiği üniversite birimlerinin veri transferi için gerekli şartların oluştuğunu kontrol etmeleri ve Tasarının 8. Maddesinde belirtilen koşullara bağlı olarak kişisel verileri aktarmaları önem taşımaktadır.

Kişisel verilerin hukuka aykırı olarak işlenmesinin ve bu verilere hukuka aykırı olarak erişilmesinin önlenmesi ile muhafazasının sağlanmasına ilişkin sorumluluklar 95/46/EC sayılı AK direktifinin 17. Maddesiyle uyumlu olarak tasarının 11. Maddesinde[94] düzenlenmiştir. Ancak 95/46/EC sayılı direktifin 17. Maddesi ile karşılaştırıldığında, veri sorumlusunun yükümlülüklerinin daraltıldığı ve bir önceki KVKKT'nin 15. Maddesinde (T.C. Başbakanlık, 2008b) belirtilen unsurların bazılarına yer verilmediği görülmektedir. Tasarıda gerekli tedbirleri alarak bu yükümlülüğü yerine getirme görevi veri sorumlusuna verilmiştir. Ancak veri güvenliğinin sağlanmasına yönelik olarak "gerekli tedbirlerin alınması" ifadesiyle veri sorumlusuna çok geniş inisiyatif kullanma alanı tanıyan ve yoruma açık bir alan bırakılmıştır. Veri sorumlusunun gerekliliği hangi alanlara (teknik, hukuksal, idari vd.) yönelik olarak sağlayacağı ve bunun nasıl belirleneceği açık değildir. 95/46/EC sayılı direktifin 17. Maddesi ve bir önceki KVKKT'nin 15. Maddesinde (T.C. Başbakanlık, 2008b) gerekli uygun teknik ve idari önlemlerin alınacağı belirtilerek, bilgi güvenliği önlemlerinin bütün boyutlarının dikkate alınması sağlanmıştır. Buna bağlı olarak maddenin gerekçesinde, risklere yönelik en üst düzey teknik önlemlerin alınması ve uygun idari personelin istihdam edilmesinin de bu kapsamda olduğu belirtilmektedir (T.C. Başbakanlık, 2008b). Üniversitelerde özellikle BİDB'nin sorumlulukları KVKKT'nin 11. Maddesi (T.C. Başbakanlık, 2014a) çerçevesinde değerlendirilmektedir. Genellikle üniversite BİDB'nin öncülüğünde geliştirilen bilgi güvenliği politikaları içinde bu sorumlulukların paylaştırılması, korunan verinin niteliğine bağlı olarak alınacak bilgi güvenliği önlemlerinin belirlenmesi ve ilgili personelin hukuksal sorumluluğunun hatırlatılması açısından bu madde önem taşımaktadır.

[94] **KVKKT, 11. Madde:** (1) Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini sağlamaya yönelik gerekli tedbirleri almak zorundadır.

KVKKT'nin 9. Maddesinde[95] 95/46/EC sayılı AK direktifinin 10. maddesiyle uyumlu olarak veri sorumlusunun aydınlatma yükümlülüğü düzenlenmiştir. Bu madde ile veri sorumlusu, verilerin işlenmesine ve daha sonra kullanımına ilişkin tüm bilgileri veri sahibine bildirmekle ve farklı bir amaç için kullanılacaksa veri sahibinin rızasını almakla yükümlüdür (T.C. Başbakanlık, 2014a). Kişisel verilerin veri sahibi dışındaki bir kaynaktan elde edilmesi halinde de (uygulanabilir ve mümkün olması halinde) veri sahibinin bilgilendirilmesi gerekmektedir. Ancak 95/46/EC sayılı AK direktifinin 11. Maddesinde ve bir önceki KVKKT'nin 11. Maddesinde (T.C. Başbakanlık, 2008b) ilgili kişi için tanımlanan bu hakkın KVKKT'nin 9. ve 10. Maddelerinde yer almadığı görülmektedir. Bu durumda ilgili kişinin tam olarak nerelerde kişisel verilerinin bulunduğunu bilmesinin ve tasarıda belirtilen haklarını kullanabilmesinin mümkün olamayacağı değerlendirilmektedir. Tasarının 10. Maddesinde[96] de ilgili kişinin hakları düzenlenmiştir. Bu maddede yer alan yükümlülüklerin veri sorumlusu olarak üniversitelerde kişisel verileri işleyen birimler tarafından yerine getirilmesi gerekmektedir. KVKKT'nin 24. Maddesinde istisnalar düzenlenmiştir. Kapsamının geniş ve sınırlarının belirsiz olması, genel olarak değerlendirildiğinde bu istisnaların uygulanmasını kolaylaştırmakta ve kanunun kişisel hakların korunması amacından uzaklaşmasına neden olmaktadır.

KVKKT'nın 18. Maddesinde, kişisel verilere ilişkin verilen görevleri yerine getirmek üzere Kişisel Verileri Koruma Kurulu'nun oluşturulması öngörülmektedir. 95/46/EC sayılı AK direktifinin 28. Maddesi ile uyumlu olarak hazırlanan bu maddede öngörülen bağımsız kurulun görevleri, oluşum biçimi ve çalışma esasları, tasarının 19., 20. ve 21.

---

[95] **KVKKT, 9. Madde:** (1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu, ilgili kişilere;
a) Kendisinin ve varsa temsilcisinin kimliği,
b) Kişisel verilerin hangi amaçla işleneceği,
c) İşlenen verilerin kimlere ve hangi amaçla aktarılabileceği,
ç) Kişisel veri toplamanın yöntemi ve hukukî sebebi,
d) 10 uncu maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür.
(2) Kişisel verilerin silinmesi, yok edilmesi ya da anonim hale getirilmesi halinde veri sorumlusu, ilgili kişiyi ayrıca bilgilendirmekle yükümlüdür.

[96] **KVKKT, 10. Madde:** (1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; a) Kişisel veri işleyip işlemediğini öğrenmek, b) Kişisel verileri işlemişse buna ilişkin bilgi talep etmek, c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenmek, ç) Yurtiçinde veya yurtdışında kişisel verilerin aktarıldığı üçüncü kişileri bilmek, d) Kişisel verilerin eksik veya yanlış olması halinde bunların düzeltilmesini istemek, e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini istemek, f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini istemek, g) İşlenen kişisel verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etmek, ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etmek, haklarına sahiptir.

Maddelerinde düzenlenmiştir. Ancak geniş yetkilerle donatılan bu kurulun, tasarının 20. Maddesi gereğince Bakanlar Kurulu tarafından seçilecek olmasının, kurulun tarafsızlığı ve bağımsızlığına gölge düşüreceği kanaati oluşmaktadır.

108 sayılı AK sözleşmesinin 10. Maddesi ve 95/46/EC sayılı AK direktifinin 24. Maddesi gereğince, KVKKT'de yer alan hükümlerin uygulanmasını sağlamak ve ihlali durumunda uygulanacak yaptırımları belirlemek amacıyla 16. ve 17. Maddelerle düzenlemeler yapılmıştır. Buna göre, tasarıda yer alan hükümlere aykırı olarak kişisel verileri depolayan, muhafaza eden, değiştiren, yeniden düzenleyen, açıklayan, elde edilebilir hale getiren, sınıflandıran ya da kullanılmasını engelleyen veya üçüncü kişilere aktaranların TCK'nın 135. Maddesine göre cezalandırılması öngörülmektedir (T.C. Başbakanlık, 2014a). Ancak TCK'nın 135. Maddesinin sadece hukuka aykırı olarak kişisel ve hassas verileri kaydeden kimselere ilişkin olarak düzenlendiği görülmektedir. Bu nedenle, KVKKT'nin 16/2. Maddesi ile TCK'nın 135. Maddesinin uygulama alanı genişletilmektedir. KVKKT'nin 16/3. Maddesinde ise, 7. Maddede belirtilen kişisel verilerin "işlenmesini gerektiren sebeplerin ortadan kalkması" halinde silinmemesi ya da anonim hale getirilmemesine ilişkin olarak TCK'nın 138. Maddesinin dikkate alınmasının tartışmaya açık olduğu görülmektedir. Çünkü kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkmış olması, bu verilerin saklama sürelerinin de sona erdiği anlamına gelmemektedir. TCK'nın 138. Maddesinde verinin toplanma amacı ile bağlantı kurulmadığı için, veri sorumlularının kullanım amacı sona eren verileri saklama süresi sonuna kadar saklayabilmesine imkân tanınmaktadır (Ketizmen, 2008). Ayrıca tasarının 9., 11., 14. ve 15. Maddelerinde öngörülen yükümlülüklere aykırı hareket edenler için 17. Maddede yapılan düzenleme ile idari para cezası öngörülmüştür.

2.4.5. Kişisel Verilerin ve Bilgi Güvenliğinin Sağlanmasına İlişkin Denetim ve Koordinasyon Sisteminin Geliştirilmesi

Kişisel verilerin korunması için öncelikle hukuksal düzenlemelerin yapılması ve her kurum ya da kuruluş için geliştirilen bilgi güvenliği politikaları çerçevesinde teknik önlemlerin alınması gerekmektedir. Ancak hukuksal düzenlemeler ve alınan teknik önlemler uygulamaya dönüşmediği sürece, kişisel verilerin korunması söz konusu

olamamaktadır. Kişisel verilerin ihlali sonrasında gerekli idari ya da hukuksal işlemlerin yapılması, mevcut hukuksal düzenlemeler çerçevesinde yapılabilmektedir. Ancak kişisel verilerin korunmasına ilişkin bireysel hakların korunabilmesi için, önleyici tedbirlerin alınması ve hukuksal düzenlemelerin de önleyici nitelikte olması gerekmektedir. Alınan hukuksal ya da teknik önlemlerin önleyiciliğinin belirlenebilmesi için ise başvurulabilecek yöntem, denetim sistemlerinin geliştirilmesi ve belirli standartlar çerçevesinde aralıklı olarak iç ve dış denetimlerin yapılmasıdır.

Türkiye'de kişisel verilerin korunmasına ilişkin olarak kurum ve kuruluşlara yönelik yapılmış denetim örneklerinin nadiren görüldüğü söylenebilir. Ancak Cumhurbaşkanlığı Devlet Denetleme Kurulu (DDK) tarafından bu konu kapsamında 2013 yılında gerçekleştirilmiş olan denetimler, mevcut durumun ortaya konulması, bu tür denetimlerin gerekliliğinin anlaşılması ve çözüm önerileriyle, konuya ilişkin önemli bir aşama ve gelişme olarak görülmektedir. DDK tarafından altı kuruluşa (Adalet Bakanlığı, Sağlık Bakanlığı, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, Gelir İdaresi Başkanlığı, Sosyal Güvenlik Kurumu ile Tapu ve Kadastro Genel Müdürlüğü) yönelik olarak yapılan "Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları" sonucunda hazırlanan rapor, Türkiye'de kişisel verilerin korunmasına ilişkin önlemlerin ve dolaylı olarak hukuksal düzenlemelerin yetersizliğini ortaya koymaktadır (DDK, 2013). Raporda ayrıca, belirli bir standarda bağlı olmaksızın yapılan güvenlik testlerinin güvenilir olmadığı ifade edilerek, ulusal düzeyde "Kamu Kurumları Güvenlik Testleri Standardı" dokümanının oluşturulması ve uygulanmasının önemine vurgu yapılmıştır. DDK'nın hazırlamış olduğu raporda ortaya konulan eksikliklerin büyük bölümünün, üniversiteler de dâhil olmak üzere birçok kurum ve kuruluşta görülmesi muhtemeldir. Bu raporda dikkat çekilen noktalar, üniversitelerde kişisel verilerin korunması, bilgi güvenliği politikalarına ilişkin olarak yapılan araştırmalarda eksikliklerin tam olarak tespit edilmesi ve uygulanabilir bilgi güvenliği politikalarının geliştirilmesine katkı sağlayabilecek nitelikte olması nedeniyle önem taşımaktadır.

Denetimler sonucunda hazırlanan raporda dikkati çeken önemli noktalar şunlardır (DDK, 2013);

- Bilgi güvenliği ve kişisel verilerin korunması konusunda, bilgi işlem personeli ve kurum çalışanlarının farkındalığının arzulanan seviyede olmadığı görülmüştür.
- Kurumların çoğunun bilgi güvenliği politikasına sahip olmadığı, bilgi güvenliği politika belgesi olanlarda ise kurum çalışanlarının bu belgeden yeterince haberdar olmadığı tespit edilmiştir.
- Denetimlerde yazılı yedekleme politikası bulunmayan ya da politika belgesi ile uygulama arasında uyumsuzluk bulunan kurumlar olduğu görülmüştür.
- Denetim kapsamındaki kurumlardan sadece birinde kullanım dışı kalan elektronik bilgi depolama ortamlarının güvenli imhasına ilişkin yazılı politikanın bulunduğu, ancak bu kurumda da ilgili personelin politikadan habersiz olduğu ve uygulamadığı tespit edilmiştir.
- Kurumlarda ve Türkiye genelinde kişisel ve hassas verilerin neler olduğuna dair herhangi bir envanter çalışmasının yapılmadığı ve buna yönelik güvenlik önlemlerinin belirlenmediği tespit edilmiştir.
- Sistem tasarımı aşamasında güvenliğin temel tasarım prensibi olarak ele alınmadığı, günlük işlerin yürütülmesine odaklanıldığı görülmüştür.
- Denetimlerde iki kurum dışındaki diğer kurumlarda merkezi kayıt ve izleme sisteminin bulunmadığı görülmüştür.
- Çoğu kurumun iş sürekliliği ve felaket kurtarma politika ve senaryolarına sahip olmadığı tespit edilmiştir.
- Kurumlara dışarıdan bilişim hizmeti sunan şirketlerle gizlilik sözleşmesinin ve personeline yönelik güvenlik araştırmasının yapılmadığı tespit edilmiştir.
- Bilgi sistemlerinin fiziksel güvenliğinin dahi sağlanmamış olduğu ve bu sistemler üzerinde yapılan saldırı girişimleri sonucunda 5 dakikalık süre içinde verilere ulaşılabildiği görülmüştür.
- Sistem odalarının fiziksel güvenliğinin zayıf olduğu ve ayrıca bilgisayar ağ kablolarının dışarıdan müdahaleye açık olduğu görülmüştür.
- Bilgi sistemleri üzerinde yapılan işlemlere dair kayıt altına alma politikasının bulunmadığı ve kayıtların tutulmasında eksikliklerin olduğu görülmüştür.

- Hassas veriler içeren sistemlere erişim için, 1111 ve 1234 gibi kolay tahmin edilebilir şifreler kullanıldığı ve güçlü şifrelerin kullanılmasını sağlayacak teknik önlemlerin alınmamış olduğu görülmüştür.
- Bazı kurumların çağrı merkezlerinden sadece isim ya da kimlik numarası ile doktor ve ilaç bilgileri gibi birçok kişisel bilgiye ulaşılabilmektedir.
- Kurumların çoğunda iç denetimlerin düzenli olarak yapılmadığı, yapılan bazı testlerin ise kalitesinde farklılıklar bulunduğu ve bu testler sonucunda tespit edilen kritik güvenlik açıklarının kapatılmadığı tespit edilmiştir.

DDK tarafından hazırlanan raporda bu çalışma açısından önem taşıyan diğer nokta, kişisel verilerin korunmasına ilişkin denetim işlemlerinde kullanılan yöntemler ve referans gösterilen kaynaklardır. Raporun isminden de anlaşılacağı üzere, kişisel verilerin korunmasına ilişkin durum değerlendirmesi yapılırken ulusal ve uluslararası durum birlikte ele alınmış ve kişisel verilerin korunmasına ilişkin denetim, bilgi güvenliği denetimi ile birlikte yapılmıştır. Raporda, uluslararası belgelerde kabul görmüş kişisel verilerin işlenmesine ilişkin genel ilkelerin dikkate alındığının, uluslararası antlaşmalar ve Türk Hukuk Mevzuatı'nda kişisel verilerin korunmasına ilişkin düzenlemelerin göz önünde bulundurulduğunun ve ISO 27001 gibi uluslararası standartların dikkate alınarak denetimin yapıldığının vurgulanması önemli ve dikkat çekicidir. Bilgi teknolojileri ve bilgi güvenliği konusunda yapılan denetimlerin bilgi kriterleri çerçevesinde ve uluslararası standartlara referans verilerek yapılması, elde edilen bulgu ve önerileri içeren raporların kabul edilebilirliğine de katkı sağlamaktadır (Kayrak, 2012).

DDK tarafından yapılan denetimler sonucunda elde edilen bulgular, üniversitelerde bilgi güvenliğinin sağlanmasına ilişkin olarak yapılacak araştırmalar için de önem taşımaktadır. Kurum ve kuruluşlarda uluslararası bilgi güvenliği standartları kapsamında birçok eksikliğin bulunması, üniversitelerde de benzer eksikliklerin görülebileceğini işaret etmektedir. Bu nedenle çalışma kapsamında yapılan araştırmada, DDK raporunda yer alan uygulama hataları ve eksiklikler de dikkate alınmıştır. Araştırmadan elde edilen bulgulara bağlı olarak, üniversiteler için geliştirilen bilgi güvenliği politikasında benzer eksiklikleri giderecek ve/veya önleyici nitelikte önerilere yer verilmiştir. DDK raporunda

yer alan eksiklikler, üniversitelerde bilgi güvenliğine ilişkin denetim faaliyetlerinin neden gerekli olduğu sorusuna da cevap vermektedir.

2.4.6. Üniversitelerde Kişisel ve Hassas Verilerin Korunmasına İlişkin Dikkate Alınması Gereken Diğer Hukuksal Düzenlemeler

Türk Hukuk Mevzuatında kişisel verilerin korunmasına ilişkin olarak hazırlanmayan, ancak kişisel verilerin elde edilmesi ve işlenmesi ile ilişkili olarak üniversitelerde dikkate alınması gereken önemli hukuksal düzenlemeler bulunmaktadır. Bu düzenlemelerin özellikle kişisel verileri işleyen birimlerin çalışanlarına yüklediği sorumluluklar, göz ardı edilmesi halinde maddi ve manevi kayıplara neden olabilmektedir.

2.4.6.1. Bilgi Edinme Hakkı Kanununda Kişilik Haklarının Korunmasına İlişkin Düzenlemeler

4982 sayılı Bilgi Edinme Hakkı Kanunu (BEHK), kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetleriyle ilgili, eşitlik, tarafsızlık ve açıklık ilkelerine uygun olarak kişilerin bilgi edinme hakkını kullanmalarına ilişkin esas ve usulleri düzenlemektedir (BEHK, 2003). Ancak BEHK çerçevesinde elde edilebilecek bilgiler, kanunun 4. Bölümünde yer alan ve bu hakkın sınırlarını belirten maddelerin içeriğine uygun olmalıdır. Kanunun 4. Bölümünde, hangi bilgi ve belgelerin kanun kapsamı dışında tutulacağına ayrıntılı olarak yer verilmiştir.

BEHK'da kişisel verilerin korunmasına ilişkin düzenleme, 4. Bölümde (Bilgi edinme hakkının sınırları) yer alan "özel hayatın gizliliği" başlığı altında 21. Madde[97] ile yapılmıştır. Bu madde ile yapılan düzenleme, özel hayatın gizliliği kapsamında değerlendirilen kişisel verileri bilgi edinme hakkı kapsamının dışında tutarak korunmasını sağlamaktadır. BEHK'da yer alan bu düzenlemeye göre kişisel bilgi veya

[97] **BEHK, 21. Madde:** Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır.

Kamu yararının gerektirdiği hâllerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir.

belgelerin açıklanabilmesi için, kamu yararının bulunması, en az yedi gün önce ilgiliye haber verilmesi ve veri sahibinin yazılı izninin alınmış olması şartı getirilmiştir. BEHK'nın 21. Maddesinde yer alan bu ifade; PDB, BİDB ve bilgi merkezi gibi belge işlemleri yöneten üniversite birimlerini doğrudan ilgilendirmektedir. Yazılı bilgi güvenliği politikaları içinde, BEHK'nın kapsamı dışında kalan bilgi ve belgelerin neler olduğunun açık ifadelerle belirtilmesi ve farkındalığın arttırılması, özel hayata ilişkin değerlere haksız müdahalenin ve oluşabilecek kayıpların önlenmesi açısından önem taşımaktadır. BEHK'da yer alan düzenlemelerin uygulanmasında ihmâli, kusuru veya kastı bulunan kamu görevlileri hakkında uygulanacak cezai yaptırımlar, kanunun 29. Maddesinde[98] düzenlenmiştir.

2.4.6.2. Elektronik İmza Kanununda Kişilik Haklarının Korunmasına İlişkin Düzenlemeler

15 Ocak 2004 tarihli ve 5070 sayılı Elektronik İmza Kanununa (EİK) göre elektronik imza, kimlik doğrulama amacı ile kullanılan ve başka bir elektronik veriye eklenen ya da mantıksal bağlantısı bulunan elektronik veridir (Elektronik İmza Kanunu, 2004). Elektronik imza, elle atılan imza ile aynı hukuksal sonucu doğurmaktadır[99]. EİK'ya uygun güvenli elektronik imzanın oluşturulabilmesi için, nitelikli elektronik sertifikanın oluşturulması gerekmektedir. Elektronik sertifika, imza sahibinin kimlik bilgileri ile imza doğrulama verisini birbirine bağlayan elektronik kayıttır (Elektronik İmza Kanunu, 2004). EİK'nın 9. Maddesinde[100] de belirtildiği gibi; bir elektronik sertifikanın nitelikli

---

[98] **BEHK, 29. Madde:** Bu Kanunun uygulanmasında ihmâli, kusuru veya kastı bulunan memurlar ve diğer kamu görevlileri hakkında, işledikleri fiillerin genel hükümler çerçevesinde ceza kovuşturması gerektirmesi hususu saklı kalmak kaydıyla, tâbi oldukları mevzuatta yer alan disiplin cezaları uygulanır.

[99] **EİK, 5. Madde:** Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur.

Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez.

[100] **EİK, 9. Madde:** Nitelikli elektronik sertifikada;

a) Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibarenin,
b) Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının,
c) İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,
d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin,
e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,
f) Sertifikanın seri numarasının,
g) Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin,
h) Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgilerinin,
ı) Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddî sınırlamalara ilişkin bilgilerin,
j) Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının, bulunması zorunludur.

olabilmesi için üzerinde taşıması gereken bilgiler arasında, imza sahibinin teşhis edilebileceği kimlik bilgileri de bulunmaktadır. Bu kişisel verilerin korunmasına yönelik sorumluluk ise EİK'nın 12. Maddesinde[101] yer alan düzenleme ile elektronik sertifika hizmet sağlayıcısına verilmiştir. Elektronik imzanın Türkiye'de uygulanmasına ilişkin hukuksal dayanağı olan ve Telekomünikasyon Kurumu tarafından 6 Ocak 2005 yılında yayınlanan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul Ve Esaslar Hakkında Yönetmeliğin" 9. Maddesinde de, gereğinden fazla bilgi toplanmaması, sertifika sahibinin onayı olmaksızın bu bilgilerin üçüncü kişilere iletilmemesi ve başka amaçlarla kullanılmamasına ilişkin ifadeler yer almaktadır (BTK, 2005).

Elektronik belge yönetim sistemlerinin (EBYS) kullanılmasıyla birlikte yazışmaların dijital ortama taşınması ve üniversitelerde elektronik imza kullanımı hızla artmaktadır (Uludağ Üniversitesi, 2013). 15 Kasım 2013 tarihi itibariyle Kamu Sertifikasyon Merkezi tarafından üretilen toplam 313236 adet kullanılabilir sertifikanın 5502 adedi (%1,75) üniversiteler için üretilmiş iken, 15 Kasım 2014 tarihi itibariyle üretilen toplam 393659 adet kullanılabilir sertifikanın 21060 adedi (%5,34) üniversiteler için üretilmiştir (TÜBİTAK UEKAE, 2014). Elektronik imzanın kullanımı, EBYS uygulamalarının kullanımının ön şartı niteliğindedir. Ancak elektronik imzanın kullanımı konusundaki bilgi eksikliği ve duyulan endişeler, üniversitelerde EBYS'nin yaygınlaşmasının önünde bir engel olarak durmaktadır (Özdemirci, 2012). Nitelikli elektronik sertifika başvurusu ve elektronik imza kullanımına ilişkin problemlerin çözümünde üniversite BİDB'nin de rehberlik görevini üstlendiği ve sorumluluklar aldığı görülmektedir (HÜ. BİDB, 2013). Elektronik İmza Kanununda kişisel verilerin korunmasına ilişkin sorumluluğun elektronik sertifika hizmet sağlayıcısına verilmesine karşın, bu sertifikanın elde edilme süreci ve kullanımına yönelik olarak sağladığı hizmetler nedeniyle, bilgi güvenliğinin sağlanması açısından önemsenen bilinçli kullanımın arttırılmasına üniversite BİDB de önemli katkılar sağlamaktadır.

[101] **EİK, 12. Madde:** Elektronik sertifika hizmet sağlayıcısı;

a) Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,

b) Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,

c) Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

2.4.6.3. 5651 Sayılı Kanun Gereğince Toplanan Kişisel ve Hassas Verilerin Korunması

Türkiye'de internet ortamında yapılan yayın ve bilgi paylaşımına ilişkin konular 5651 sayılı kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) ile düzenlenmiştir. 4 Mayıs 2007 tarihinde kabul edilen 5651 sayılı kanun; internet ortamındaki hizmet sağlayıcıların yükümlülüklerini ve internet ortamında işlenen suçlarla bu servis sağlayıcılar üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektedir[102]. Bütün kurum ve kuruluşlarda olduğu gibi, üniversitelerin de 5651 sayılı kanun gereğince uymak zorunda oldukları yükümlülükler bulunmaktadır (ODTÜ BİDB, 2008).

Üniversite bilgi merkezleri ya da bilgi işlem merkezi üzerinden veri tabanlarına erişim esnasında kullanılan erişim bilgilerini saklama ve bu erişim sağlayıcı trafik bilgileri[103] içinde yer alan kişisel verilerin güvenliğini sağlama yükümlülüğü, 6. Maddenin 1. Fıkrasında[104] ifade edilen düzenleme ile "erişim sağlayıcı"[105] rolünü üstlenen üniversite bilgi merkezlerine (ya da bilgi işlem merkezine) verilmiştir (Henkoğlu ve Özenç Uçak, 2012). Kanun kapsamında elde edilmesi ve belirli bir süre saklanması zorunlu kılınan (kişisel verileri de içeren) trafik bilgilerinin nasıl korunacağına ilişkin bilgilere ilişkin hukuksal düzenleme ise, 26716 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmeliğin" 8/1. Maddesi[106] ile

---

[102] **5651 Sayılı Kanun, 1. Madde:** Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektir.

[103] **Erişim sağlayıcı trafik bilgisi:** İnternet ortamında yapılan her türlü erişime ilişkin olarak abonenin adı, kimlik bilgileri, adı ve soyadı, adresi, telefon numarası, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileridir.

[104] **5651 Sayılı Kanun, 6. Madde:** (1) Erişim sağlayıcı;

a) Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun hükümlerine uygun olarak haberdar edilmesi halinde erişimi engellemekle,

b) Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla,

c) Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla,

ç) (Ek: 6/2/2014-6518/89 md.) Erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla,

d) (Ek: 6/2/2014-6518/89 md.) Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla yükümlüdür.

[105] **Erişim sağlayıcı:** Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişilerdir.

[106] **26716 Sayılı Yönetmelik, 8. Madde:** b) Sağladığı hizmetlere ilişkin olarak, Başkanlığın Kanunla ve ilgili diğer mevzuatla verilen görevlerini yerine getirebilmesi için; erişim sağlayıcı trafik bilgisini bir yıl saklamakla, bu bilgilerin

yapılmıştır. Ancak veri koruma kanunu ve denetim sistemi olmaksızın erişim sağlayıcılar tarafından trafik bilgilerinin saklanmasının istenmesinin kişisel verilerin korunması açısından risk oluşturduğu düşünülmektedir. Üniversitelerde erişim sağlayıcı olarak hizmet sunan birimler, kullanıcılarına ait hukuka aykırı içeriğe, haberdar edilmesi halinde erişimi engellemekle de 5651 sayılı kanunun 6. Maddenin gereği olarak yükümlüdürler. Ancak kendisi aracılığıyla erişilen bilgilerin içeriğinin hukuka uygunluğunu kontrol etmekle yükümlü değildirler (5651 Sayılı Kanun, 2007).

Üniversitelerde kişisel verilerin işlendiği birimler, web sayfaları aracılığıyla sundukları içerikten "içerik sağlayıcı"[107] olarak sorumludurlar. Bu nedenle, özellikle ilan süreçlerinde şeffaflık ilkesi göz önünde bulundurulurken, kişisel bilgilerin korunmasına da özen gösterilmelidir. Üniversite içindeki her birim ya da personelin, denetim yetkisinin bulunduğu ve içerik üzerinde düzenleme yapabildiği kendi web sayfası üzerinde içerik sağlayıcı olarak sorumluluğu bulunmaktadır. Ancak bu içeriğin içerik sahibinin bilgisi ve onayı dışında değiştirilmesi amacıyla gerçekleştirilen girişimlere karşı korunması ve gerekli önlemlerin alınması, sitenin bulunduğu teknik altyapıyı işleten servis sağlayıcının yükümlülüğüdür. Zira gerekli teknik önlemlerin veri sahibi ya da başka bir otorite tarafından sağlanması mümkün değildir.

Üniversitelerde sunucu bilgisayarların işletilmesinden sorumlu bilgi işlem merkezlerinin, 5651 sayılı kanun kapsamında "yer sağlayıcı"[108] olarak da sorumlulukları bulunmaktadır. Yer sağlayıcılar, hukuka aykırı içeriği, haberdar edilmeleri halinde, kanunun 5. Maddesi[109] gereğince yayından kaldırmakla yükümlüdürler. Kişisel verilerle ilişkili olarak içeriğin yayından kaldırılması, içerik nedeniyle haklarının ihlal edildiğini iddia eden kişinin içerik sağlayıcısına ulaşamayarak yer sağlayıcısına başvurması halinde,

---

doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle, internet trafik izlemesinde Başkanlığa gerekli yardım ve desteği sağlamakla, faaliyet belgesinde yer alan Başkanlığın uygun gördüğü bilgileri talep edildiğinde bildirmekle ve ticari amaçla internet toplu kullanım sağlayıcılar için belirli bir IP bloğundan sabit IP adres planlaması yapmakla ve bu bloktan IP adresi vermekle yükümlüdür.

[107] **İçerik sağlayıcı:** İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilerdir.

[108] **Yer sağlayıcı:** Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir.

[109] **5651 Sayılı Kanun, 5. Madde:** (1) Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.

(2) Yer sağlayıcı, yer sağladığı hukuka aykırı içeriği bu Kanunun 8 inci ve 9 uncu maddelerine göre haberdar edilmesi hâlinde yayından çıkarmakla yükümlüdür.

Kanunun 9. Maddesinde belirtilen hususlara uygun olarak yer sağlayıcı tarafından yerine getirilir (5651 Sayılı Kanun, 2007). 19 Şubat 2014 tarihinde yürürlüğe giren 6518 sayılı torba kanun ile 5651 sayılı kanun üzerinde de değişiklikler yapılmıştır (6518 Sayılı Kanun, 2014). Bu kapsamda, 26716 sayılı yönetmeliğin 7/1-c Maddesinde[110] yer sağlayıcı için tanımlanan trafik bilgisi saklama yükümlülüğü, 5651 sayılı kanunun 5. Maddesinde de süresi arttırılarak ek fıkralar[111] ile tanımlanmıştır. Ancak yeni düzenlemeler kapsamında trafik bilgilerinin yer sağlayıcılar tarafından da daha uzun bir süre boyunca tutulmasının doğruluğu tartışma konusudur. Maliyetleri de arttıracağı düşünülen bu kayıtların korunma standartlarının belirlenmemiş olmasının, bu konudaki risklerin artmasına sebep olacağı değerlendirilmektedir.

AB Adalet Divanı tarafından geçersiz olduğuna karar verilen 2006/24/EC Sayılı Direktife ilişkin olarak sunulan gerekçeler, 5651 Sayılı Kanun açısından düşündürücüdür. 2006/24/EC Sayılı Direktif, organize ve terör suçları gibi önemli suçların önlenmesi, soruşturulması ve konuşturmasını amaçlayarak; bu kapsamda servis sağlayıcıların trafik ve yer bilgisi gibi kullanıcı kimliğini ya da teşhisini sağlayan iletişim bilgilerin servis sağlayıcılar tarafından tutulmasını istemekteydi. Ancak AB Adalet Divanı kararın gerekçesinde; en az 6 en fazla 24 ay süre ile her birey için istisnasız iletişim bilgilerinin tutulması, özel hayatın gizliliğine orantısız olarak müdahale edildiğini, bireylerin kendi veri ve trafik bilgilerinin tutulduğundan haberdar olmadığını ve bu verilere ulusal makamların gerekçe göstermeksizin ulaşabilmesinin mahremiyeti ihlal ettiğini açıklamıştır. 2006/24/EC Sayılı Direktif ile 5651 Sayılı Kanun arasında uygulama açısından büyük benzerlik bulunmaktadır. 5651 Sayılı Kanun'da erişim sağlayıcı ile birlikte yer sağlayıcılara da en az bir yıl süreyle trafik bilgilerini saklama yükümlülüğü getirilmiştir. Ancak bu bilgilerin doğruluğunun, gizliliğinin ve bütünlüğünün nasıl saklanacağı yeterince açık değildir. Bu açıdan bakıldığında; 5651 Sayılı Kanun kapsamındaki uygulamaların da temel hak ve özgürlüklere müdahale niteliğinde olduğu değerlendirilmektedir.

---

[110] **26716 Sayılı Yönetmelik, 7. Madde:** c) Yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle yükümlüdür.

[111] **5651 Sayılı Kanun, 5. Madde:** (3) Yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür.

5651 sayılı kanunun 5. Maddesine eklenen 3. Fıkra ile, yer sağlayıcıların saklamak zorunda oldukları ve kişisel veriler olarak da nitelendirilebilecek trafik bilgilerinin doğruluğunu, bütünlüğünü ve gizliliğini sağlama yükümlülükleri de bulunmaktadır. Bu yükümlülükleri nasıl yerine getirecekleri ya da yerine getirdiklerinin nasıl denetleneceği açık olmadığı gibi, yerine getirememeleri halinde uygulanacak yaptırımın da sadece idari para cezası[112] olacağı belirtilmektedir. Bu haliyle trafik bilgileri ile elde edilebilecek kişisel verilere bir maddi değer biçilmiş olduğu ve bu değerin üst limitinin belirlenmiş olduğu düşüncesi oluşmaktadır.

5651 sayılı kanunun 9. Maddesinde yapılan değişiklik ile kişilik haklarının ihlaline yönelik taleplerin içerik ve/veya yer sağlayıcısı tarafından cevaplanma süresi 24 saate indirilmiştir. Bu değişiklik kişilik haklarının korunmasına yönelik olarak olumlu bir düzenleme olarak görülmekle birlikte, bu kısa süre içinde talebin haklılığının nasıl değerlendirileceği konusunda şüpheler bulunmaktadır. Ayrıca özel hayatın gizliliğinin korunmasına yönelik olarak 5651 sayılı kanuna eklenen 9/A maddesi ile (6518 Sayılı Kanun, 2014) Telekomünikasyon İletişim Başkanlığı'nın (TİB) erişim engellemeye ilişkin yetkileri arttırılmış ve öncelikli duruma getirilmiştir.

[112] **5651 Sayılı Kanun, 5. Madde:** (6) Yer sağlayıcılık bildiriminde bulunmayan veya bu Kanundaki yükümlülüklerini yerine getirmeyen yer sağlayıcı hakkında Başkanlık tarafından on bin Türk Lirasından yüz bin Türk Lirasına kadar idari para cezası verilir.

2.5. KİŞİSEL VE HASSAS VERİLERİN KORUNMASINA İLİŞKİN HUKUKSAL DÜZENLEMELERİN BİLGİ GÜVENLİĞİ MODELİ ÇERÇEVESİNDE DEĞERLENDİRİLMESİ

2.5.1. AB Hukuku ve Türk Hukuk Mevzuatında Kişisel ve Hassas Verilerin Korunmasına İlişkin Farklılıklar

2.5.1.1. Temel Haklar ve Kişisel Verilerin Korunması Hakkı

AB'de kişisel verilerin korunması konusunun "özel hayatın gizliliği" ilkesine bağlı olarak değerlendirildiği ve AİHM'nin vermiş olduğu kararlarda kişisel verilerin korunmasıyla ilgili olarak genel kişilik hakları ve insan onurunun korunmasına ilişkin ilkelerin dikkate alındığı görülmektedir. Bunun başlıca nedeni, AB hukuk sisteminin temel insan hak ve hürriyetleri üzerine kurulu olmasıdır. Türkiye'de de Anayasa Mahkemesi tarafından bu yaklaşıma bağlı olarak alınan kararlar bulunmaktadır. Ancak mevcut haliyle Türk Hukuk Sisteminde, genel kişilik haklarının ve özel hayatın gizliliği haklarının kişisel verilerin korunmasına ilişkin olarak kullanıldığı sınırlı sayıda örnek[113] bulunmaktadır.

AB hukukunda farklı alanlara ilişkin (haberleşme vd.) hukuksal düzenlemeler içinde kişisel verilerin korunmasına yönelik önlemler yer almakla birlikte, konunun merkezinde önleyici tedbirleri detaylı olarak düzenleyen veri koruma direktifinin yer aldığı görülmektedir. Türk Hukuk Mevzuatı'nda ise birçok hukuksal düzenleme içinde temel bir hak olarak kişisel verilerin korunmasına yönelik düzenlemeler bulunmaktadır. Ancak verilerin korunmasına ilişkin AB veri koruma direktifi benzeri yeterli ve açık bir hukuksal düzenleme bulunmamaktadır. Katılım ortaklığı belgesi, ilerleme raporları ve 23. fasıl tarama sonu raporunda, Türkiye'de KVKK'nın olmaması önemli bir eksiklik olarak değerlendirilmektedir. Ayrıca Türkiye'de henüz KVKK'nın bulunmaması nedeniyle, 108 sayılı sözleşmenin 4. Maddesinde belirtilen yükümlülük yerine getirilememiş ve bu nedenle 108 sayılı sözleşme ve 108 sayılı sözleşmenin onaylanmasının ön şart olarak kabul edildiği 181 sayılı protokol onaylanmamıştır. AB alanı içinde kişisel verilerin

[113] Bkz. (Anayasa Mahkemesi, 2008)

korunmasına ilişkin uluslararası anlaşmaları imzaladığı halde bunu iç hukukuna uyarlamayan ve bu nedenle onaylamayan tek ülke olarak Türkiye, kişisel verileri korumadığı gerekçesiyle AB ülkeleri ile bilgi paylaşımı (özellikle adalet ve polis teşkilatına ilişkin olarak) ve güvenlik işbirliği anlaşmaları yapamamaktadır. Hukuksal düzenlemeler açısından gerekli adımların atılmamış olması, kişisel verilerin korunması konusunda Türkiye'nin "güvensiz ülke" olarak nitelendirilmesine ve tüm alanlarda bu eksikliğin hissedilmesine neden olmaktadır.

2006/24/EC sayılı AB veri saklama direktifi kapsamında tutulan bilgiler (iletişim süresi, gerçekleştiği yer, sıklığı ve kişilerin kimliği) ve tutulma gerekçeleri ile 5651 sayılı kanun kapsamında tutulan kayıtlar benzer niteliktedir. Bu açıdan bakıldığında, AB Adalet Divanı tarafından 08.04.2014 tarihinde geçersiz olduğuna karar verilen 2006/24/EC sayılı veri saklama direktifinin iptal edilmesi için sunulan gerekçeler (AB Adalet Divanı, 2014b), 5651 sayılı kanun için de öne sürülebilecek niteliktedir.

2.5.1.2. Kişisel Verilerin İşlenmesi

Türk Hukuk Mevzuatında kişisel verilerin toplanması konusunda kurumların yetkili olduğunu belirten hükümler bulunmaktadır[114]. Ancak bu verilerin hangi ilkelere bağlı olarak toplanacağı, hangi kurumlarla paylaşılabileceği, nasıl korunacağı ve nasıl silineceği konusunda açıklık bulunmamaktadır. Bu soruların cevabının KVKK'nın içinde yer alacağı düşünülmektedir. Oysa AB Hukuk Mevzuatında bu konunun hiçbir aşamasında belirsizliğin bulunmadığı görülmektedir.

KVKKT'de öngörülen istisnaların kapsam ve sınırlarının belirsiz olduğu ve bu istisnaların verinin işlenmesinde uyulması gereken temel ilkelere uyma zorunluluğunu da ortadan kaldırdığı değerlendirilmektedir. AB veri koruma direktifinde yer alan istisnaların ise sınırlarının tam olarak belirlendiği ve denetlenebilir nitelikte olduğu görülmektedir.

[114] Detaylı bilgi için "2.4.2. Türk Ceza Kanunu'nda Kişisel ve Hassas Verilerin Korunmasına İlişkin Düzenlemeler" isimli konuya bkz.

AB veri koruma direktifi, elektronik ortamda olma şartı aranmaksızın bütün kişisel verilere uygulanabilecek kapsamda hazırlanmıştır. Bu nedenle, henüz elektronik ortama aktarılmamış arşiv dosyaları üzerinde de koruma sağlamaktadır. Türkiye'de arşiv dosyaları üzerindeki kişisel verilerin korunmasına ve bu konudaki sorumlulukların belirlenmesine yönelik bir yasa bulunmamaktadır. Arşiv hizmetlerinin yürütülmesinde 16.05.1988 tarihli ve 19816 sayılı Resmî Gazete'de yayımlanan Devlet Arşiv Hizmetleri Hakkında Yönetmelik kullanılmaktadır. Bu yönetmelik üzerinde 08.08.2001 yılında yapılan değişiklik ile (Ek Madde 1)[115], elektronik ortamda bulunan arşiv malzemesinin kaybını önlemek için alınacak önlemler belirtilmiştir. Ancak yönetmeliğin 4. Maddesinde (T.C. Başbakanlık, 1988) tanımlanan koruma yükümlülüğünün, elektronik ortama kaydedilen arşiv malzemelerini koruma konusunda sadece fiziksel önlemlerle sınırlı bırakıldığı görülmektedir.

2.5.1.3. Veri İhlallerine Karşı Müdahale Yapıları

95/46/EC sayılı AB veri koruma direktifinde, kişisel verilerin korunması konusuna ilişkin kişilerin hak ve özgürlüğünün sağlanması için, verilerin işlendiği sistemlerin tasarımı esnasında ve verilerin işlenmesi sırasında teknik ve kurumsal önlemlerin alınması gerektiği belirtilmektedir. Cumhurbaşkanlığı DDK'nın kurumlara yönelik olarak yapmış olduğu denetimlerde de bu konuya dikkat çekilerek, eksikliklerin giderilmesi için önerilerde bulunulmuştur. Ancak Türk Hukuk Mevzuatında kişisel verilerin korunmasına yönelik önleyici kurumsal ve teknik önlemlerin alınmasıyla ilgili düzenlemeler bulunmamaktadır.

AB hukukunda 1995 yılından itibaren yapılan kişisel verilerin korunmasına ilişkin düzenlemeler önleyici niteliktedir. Kişisel verilerin ihlalini önlemek için kurulan bu yapı "önleyici müdahale yapısı" olarak da ifade edilebilir. Ancak Türk Hukuk Mevzuatında yer alan düzenlemeler kendi içindeki ihtiyaca cevap veren ve kişisel verilerin ihlalinden

[115] **Devlet Arşiv Hizmetleri Hakkındaki Yönetmelik. Ek Madde 1:** Elektronik ortamlarda teşekkül eden bilgi ve belgelerden arşiv malzemesi özelliği taşıyanların kaybını önlemek ve devamlılığını sağlamak amacıyla bir kopyası cd, disket veya benzeri kayıt ortamlarına aktarılmak suretiyle muhafaza edilir.

Bu tür malzemelerin muhafaza, tasnif, devir vb. arşiv işlemlerinde diğer tür malzemeler için uygulanan hükümler uygulanır.

sonraki sürece yönelik olarak "durdurucu müdahale yapısı" benimsenerek hazırlanmıştır. Diğer bir ifadeyle, kişisel verileri ihlal eden kişinin TCK gereğince hapis cezası alması, özel hukuk çerçevesinde tazminat ödemesi ya da devam etmekte olan tehdidin sonlandırılması sağlanabilir. Nitekim Anayasa Mahkemesi'nin kararlarında da, idarenin Anayasada belirtilen temel hakların ihlal edilmediği konularda bilgi isteminde bulunabileceği, kişisel verilerin ihlal edilmesi halinde bireylerin yargı makamları önünde haklarını arayabilecekleri ifade edilmektedir (Anayasa Mahkemesi, 2011). Bu yaklaşımla, idarenin hatalı uygulamalarından doğabilecek zararı dikkate almaksızın bireye bu konuda hak arama sorumluluğu (dava açma, harç ödeme ve avukat tutma gibi) yüklenmesi, Anayasanın 2. Maddesinde belirtilen hukuk devleti ilkesi açısından da düşündürücüdür. Türk hukuk mevzuatında kişisel verilerin korunmasına ilişkin önleyici tedbirleri içeren bir düzenlemenin bulunmaması nedeniyle, ihlal sonrasına yönelik olarak düzenlemelerle kişisel verilerin korunduğunu söylemenin mümkün olmayacağı kanaatindeyiz. Mevcut hukuk sistemindeki uygulamaya etkisi olmamakla birlikte, KVKKT'de bilgi sistemleri güvenliğinin sağlanmasına yönelik genel ilkelere yer verilmiştir.

AB Hukuk Mevzuatında kişisel verilerin korunmasına yönelik olarak kamu idaresi ve özel sektör arasında ayrım yapılmamıştır. Kişisel verilerin ihlali her kim tarafından gerçekleştirilirse, aynı hukuk kuralları ve yaptırımlara tabi olması öngörülmüştür. Ancak veri sahibinin onayı alınmaksızın verinin işlenmesinde hukuka uygunluk sebepleri ve istisnalar açıklanırken, kamu menfaati gözetilmiştir. Türk Hukuk Mevzuatında da kamu menfaatlerinin ön planda olduğu görülmektedir.

2.5.1.4. Kişisel Verilerin Korumasına İlişkin Kurumsal Yaklaşım

AB'de kişisel verilerin korunmasına ilişkin en önemli hukuksal düzenlemeler olan 95/46/EC sayılı direktif ve 108 sayılı sözleşme, taraf ya da üye ülkenin iç hukuku ile bu düzenlemeleri uyumlu hale getirmesini öngörmektedir. Bununla birlikte, özel bir veri koruma kanunu çerçevesinde bağımsız bir denetim kurumunun kurulması da AB'nin kişisel verilerin korunması için gerekli gördüğü temel unsurlardan biridir. AB'nin kişisel verilerin korunması konusunda benimsemiş olduğu temel prensiplere ilişkin Türkiye'de

çalışmalar yapılmakla birlikte, uygulamaya yönelik somut bir adımın atılamadığı söylenebilir. Türkiye'de bilgi güvenliğinin sağlanmasına yönelik olarak kamu kurum ve kuruluşlarına yol gösteren, standartları belirleyen, denetleyen ya da uygulamalarında bağlayıcı olan bir kurum veya kuruluş bulunmamaktadır. Mevcut hukuksal düzenlemelerde de bu görevi üstlenecek kurum ya da kuruluş tanımlanmamıştır. Ancak KVKKT içerisinde Adalet Bakanlığına bağlı "Bilgi Güvenliği Kurumu" kurulmasına ilişkin ifadelere yer verilmiştir. Türkiye'de de veri koruma kanunu ile birlikte bağımsız kurumsal denetim mekanizmasının kurulması ve bireylerin bu organlara başvuru yapabilmesi sağlanmalıdır.

Kişisel verilerin korunmasında dolaylı olarak etkisi bulunan bilişim suçlarına yönelik hukuksal düzenlemeler (TCK'nın 243., 244. ve 245. Maddeleri gibi) Türk Hukuk Mevzuatında yer almaktadır. Ancak Ulusal Bilgi Güvenliği Kanunu ve bu kanunun uygulanmasında etkin görev alacak bir Ulusal Bilgi Güvenliği Teşkilatı'nın olmaması, önleyici tedbirlerin alınmasında eksikliklere neden olmaktadır. Bu konuya ilişkin çalışmaların, "Bilgi Toplumu Stratejisi Eylem Planı"[116] ve "Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı"[117] hazırlanmasının ötesine gidememiş ve kamuoyunda yeterince tartışılmamış olduğu görülmektedir.

2.5.1.5. Kişisel Verileri Koruma Önlemlerinde Süreklilik ve Unutulma Hakkı

AB Hukuk Mevzuatında kişisel verilerin korunmasına ilişkin farklı alanlara yönelik birçok direktif ve karar bulunduğu halde, bu direktif ve kararlar 95/46/EC sayılı temel veri koruma direktifini odak noktası olarak almakta ve birbiri ile çelişen hükümler içermemektedir. Ayrıca 95/46/EC sayılı veri koruma direktifi ve 108 sayılı sözleşme gibi veri korumaya ilişkin en önemli hukuksal düzenlemelerin, gelişen bilgi ve iletişim teknolojileri karşısında yetersiz kaldığı noktalarının güncelleme çalışmaları aralıksız olarak devam etmektedir. Türkiye'de ise kişisel verilerin korunmasına yönelik temel veri koruma direktifi olmadığı gibi, mevcut hukuksal düzenlemelerin içinde yer alan

[116] İçerik için bkz. http://www.dpt.gov.tr/DocObjects/Download/2227/Eylem_Plani.pdf
[117] İçerik için bkz. http://bt-stk.org.tr/bilgi-guvenligi.html

hükümler arasında herhangi bir ilişki bulunmamakta ve yetersiz olduğu düşünülen hükümlerin güncellenmesine yönelik çalışmalar da gündemde yer almamaktadır.

AB veri koruma direktifi üzerinden yapılan reform çalışmaları bireylere unutulma hakkını sunmakta ve veri sahibi olma koşuluyla bireylere internet üzerindeki rahatsız edici kişisel verilerin silinmesini isteyerek yayılmasını engelleme olanağı sağlamaktadır (Henkoğlu ve Yılmaz, 2013). "Unutulma hakkı" olarak tanımlanan bu hak, her türlü eksik ve yanlış bilginin düzeltilmesi ve sosyal paylaşım ağları üzerinde kişinin kendi hak sahibi olduğu internet alanında yayınlanmasını istemediği bilgileri kapsamaktadır. Unutulma hakkı ile üçüncü kişiler tarafından oluşturulan içerikler de dâhil olmak üzere, tüm içerikler üzerinde bireyler kendi kişisel verilerini kontrol edebilme yetkisine sahip olmaktadır. AB Adalet Divanının "İspanya ile Agencia Española de Protección de Datos (AEPD) ve Mario Costeja González" arasında görülen davada 95/46/EC sayılı direktife de atıfta bulunarak 13 Mayıs 2014 tarihinde almış olduğu karar sonrasında (AB Adalet Divanı, 2014a), AB vatandaşlarının unutulma hakkını kullanabilmesine imkân tanınmıştır. Dünyanın önde gelen arama motorlarından biri olan Google, AB Adalet Divanının kararını uygulayarak 29 Mayıs 2014 tarihinden itibaren AB vatandaşlarının internet üzerindeki ilgisiz ve geçersiz linklerini taleplere bağlı olarak değerlendirmeye ve kaldırmaya başlamıştır (Google, 2014). Türkiye'de unutulma hakkını düzenleyen bir kanun bulunmamaktadır. Mevcut kanunlar (TCK, 5651 sayılı kanun, TTK, FSEK) çerçevesinde mahkeme kararıyla içeriklerin kaldırılması ya da erişimin engellenmesi mümkün olabilmektedir. Ancak bu düzenlemeler AB Hukukunda tanımlanan unutulma hakkını tam olarak karşılayamamaktadır. AB Hukukunda tanımlanan unutulma hakkına uygun olarak Anayasa'nın 20. Maddesine 2010 yılında ek yapılmıştır. Ancak bu düzenlemenin uygulanabilmesi için veri koruma kanununun da yapılması gerekmektedir. Türkiye'de mevcut yasal düzenlemeler çerçevesinde içeriğin yayından kaldırılabilmesi, bir ihlalin gerçekleşmesine bağlıdır.

2.5.2. Hukuk Mevzuatlarının Kişisel ve Hassas Verilerin Korunmasına İlişkin Temel İlkeleri Işığında Bilgi Güvenliğinin Sağlanmasına Yönelik İlkelerin Değerlendirilmesi

2.5.2.1. McCumber Bilgi Güvenliği Modeli ve Kişisel Verilerin Korunması Hakkı

Bir bilginin değeri, "CIA[118] üçgeni" olarak da ifade edilen ve üç temel prensibe dayanan bilginin karakteristik özelliklerinin değeri ile ölçülmektedir. Bilginin karakteristik özelliğinin değişmesi, bilginin değerinin artmasına ya da çoğu zaman azalmasına neden olmaktadır. Ancak sadece CIA prensibine dayanan modeller, bilgi güvenliğine ilişkin gelişmeleri ve artan unsurları tam olarak adreslemede yetersiz kalmaktadır. Bilginin çok daha karmaşık yöntemler ve amaçlarla değişebilir hale gelmesi, daha kapsamlı bilgi güvenliği modellerinin kullanımını gerektirmektedir (Whitman ve Mattord, 2011).

McCumber bilgi güvenliği modelinde öngörülen önleyici güvenlik önlemleri, AB hukuk sisteminde verilerin korunmasına ilişkin yaklaşım ile örtüşmektedir. AB hukuk sistemi, kişisel verilerin ihlaline neden olabilecek uygulamalara ilişkin olarak proaktif düzenlemelerin yapılması ve üye ülkeler tarafından bu düzenlemelerin uygulanmasının takibini öngörmektedir. Türk Hukuk Mevzuatı ise meydana gelen ihlaller sonrasında uygulanacak olan yaptırımlar ile sınırlı kalmakta ve McCumber bilgi güvenliğinde öngörülen kapsamlı güvenlik önlemlerinin uygulanmasını destekleme ve dayanak noktası olmaktan uzaktır.

Kişisel verilerin korunması hakkı, bireylerin kendisine ait verilerin işlenmesi nedeniyle oluşan risk ve tehditler karşısında temel hak ve özgürlüğünün korunması ve bu verilerin geleceğini belirleneme hakkının sunulması amacını taşımaktadır. Buna ilişkin olarak 2010 yılında Anayasa'nın 20. Maddesine yapılan ek ile kişisel verilerin korunmasını isteme hakkı oluşturulmuştur. Ancak bilgi güvenliği modellerinde doğrudan kişisel verilerin korunması hakkına değinmek yerine, hukuksal düzenlemeler adres gösterilerek daha geniş bir çerçeve çizilmiştir. Böylece ülkeden ülkeye değişen hukuksal koşullar ve

[118] **CIA**: **C**onfidentiality - Gizlilik, **I**ntegrity - Bütünlük, **A**vailability - Kullanılabilirlik

kişisel verilerin tanımına yönelik farklılıkların da geliştirilen ilkelerle çatışmasının önüne geçilmiştir.

Çalışmada örnek model olarak seçilen McCumber bilgi güvenliği modeli, tüm üniversitelerde temel alınabilecek genel bilgi güvenliği politikasının yapılmasına imkân sağladığı gibi, her üniversitenin kişisel verilerin korunmasına yönelik detayları içeren bir bilgi güvenliği stratejisi belirlemesine de katkı sağlamaktadır. Mevcut hukuksal koşullar içinde kişisel verilerin korunması için alınacak bilgi güvenliği önlemleri, üniversitenin özel şartlarına bağlı olarak bilgi güvenliği politikaları içinde daha açık şekilde ifade edilebilmektedir.

2.5.2.2. Veri Gizliliğinin İhlali ve Bilgi Güvenliği Önlemleri

Gizlilik, bilginin yetkisiz kişi ve sistemlerin erişimine kapatılarak içeriğinin açığa çıkmasının engellenmesidir. Yetkisiz kişiler tarafından bilgilere erişimin engellenmesi ve gizlilik ihlallerinin önlenmesi için, bilginin sınıflandırılması, güvenlik politikalarının belirlenmesi, veri depolama üniteleri üzerinde teknik önlemlerin alınması ve bilgiyi işleyen kullanıcıların eğitilmesi gerekmektedir. Bilginin korunması gereken karakteristik özelliği olarak gizlilik, kişisel verilerin korunmasına ilişkin olarak kullanılan mahremiyet ile yakından ilişkilidir. Gizliliği söz konusu olan bilginin hassas ve kişisel bilgi varlıkları olması halinde değeri artmaktadır. Kişisel verileri alınan birey, bu verilerin ilgili kurum, kuruluş ya da şirket tarafından gizliliğinin korunmasını isteme hakkına sahiptir. Bu verilerin amaçlı ya da yanlışlıkla veri sahibinin bilgisi dışında transfer edilmesi, dışarıdan yapılan yetkisiz erişimlere karşı gerekli teknik önlemlerin alınmamış olması veya kullanım süresi sonunda uygun yöntemlerle imha edilmemesi, gizlilik ihlalinin oluşmasına neden olmaktadır.

Kişisel verilerin korunmasını da kapsayan teknik yöntemlerle uygulanan güvenlik sınırlı seviyede kalmaktadır. Bu nedenle önleyici güvenlik önlemlerini içeren hukuksal düzenlemelerin yapılması, denetim kurumlarının oluşturularak düzenli denetimlerin gerçekleştirilmesi, tüm kullanıcıların veri koruma sürecinin katılımının sağlanması, farkındalığın arttırılmasına yönelik eğitsel programlara ağırlık verilmesi ve risk yönetiminin yapılarak etkin bilgi güvenliği politikalarının oluşturulması gerekmektedir.

Hukuk mevzuatlarında yer alan KVKKT haricindeki hukuksal düzenlemelerde, risk ve tehditlere karşı kişisel verilerin korunması için gereken güvenlik önlemlerinin alınması ilkesine uygun bir düzenleme bulunmamaktadır. Bu eksiklik, özellikle teknik önlemleri içeren bilgi güvenliği politikaları içinde sorumluluğun ilgili birimlere verilmemesi ve bu nedenle uygulama da önleyici tedbirlerin yetersiz kalmasına neden olabilmektedir.

2.5.2.3. Uluslararası Standartlar

Bilgi güvenliği politikalarının geliştirilmesinde faydalanılan ve referans gösterilen öncelikli kaynaklar arasında yer alan uluslararası standartlar, kurum ve kuruluşun kendi özel yönetim/denetim sistemine ve hukuksal koşullara bağlı olarak uygulandığında bilgi güvenliğine önemli katkı sağlamaktadır. Kişisel verilerin korunmasına ilişkin olarak uluslararası bilgi güvenliği standartlarından kurum ya da kuruluş yapısıyla örtüşen bilgi güvenliği politikalarını tamamlayacak şekilde faydalanılmalıdır.

ISO 27002 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında, kişisel bilginin mahremiyetinin korunmasının kurumun kanuni yükümlülükleri açısından önemli olduğu vurgulanmaktadır. Bu açıdan bakıldığında, bilgi güvenliğinin sağlanmasına ilişkin uluslararası standartlarda, kişisel verilerin korunması ile bilgi güvenliğine ilişkin temel ilkelerin ve hukuksal koşulların birbiri ile bütünleştiği ve bilgi güvenliği politikalarında da bu ilişkinin birlikte ele alınması gerektiği değerlendirilmektedir.

2.5.2.4. Hukuksal Düzenlemeler ve Bilgi Güvenliği Politikaları

Yasal düzenlemeler kişisel verilerin korunması ya da ihlal edilen özel hayatın gizliliğinin tekrar kazanılması için tek başına yeterli görünmemektedir. Ancak alınacak olan teknik önlemlerin hukuksal bir dayanağının bulunması önemlidir. Ayrıca, yasal düzenlemelerin varlığı, teknik önlemlerin yetersizliği nedeniyle açığa çıkan kişisel verilerin daha hızlı yayılmasını caydırıcılık özelliği ile önleyici etkenlerden biridir.

Bilgi güvenliği politikaları belirlenirken; genel olarak mevcut bilgi değerlerinin ve risk durumunun analizi yapılarak, önleyici tedbirlerin alınması hedeflenmektedir. AB

hukukunda yer alan kişisel verilerin korunmasına ilişkin düzenlemeler de önleyici niteliğiyle bilgi güvenliği politikalarının geliştirilmesine kaynak ve rehber olabilecek ilkeler içermektedir. Ancak Türk hukuk mevzuatında yer alan düzenlemeler için aynı şekilde düşünülmesi ya da bilgi güvenliği politikalarına yansıtılması mümkün değildir. Çünkü kişisel verilerin ihlali sonrasında yapılacak olan işlemler, bilgi güvenliği politikaları ile tam olarak örtüşmemektedir. Bilgi güvenliği politikalarında öncelikli amaç, verinin korunmasını "önleyici" yöntemlerle sağlamaktır. İhlalin gerçekleşmesi durumunda ise, verinin mümkün olan en güncel halinin en kısa zamanda tekrar kullanılabilirliğinin sağlaması hedeflenmektedir. İhlal sonrasında açığa çıkan kişisel bilgilerin internet ortamındaki transferinin engellenemeyeceği de düşünüldüğünde, önleyici tedbirlerin kişisel veriler açısından önemi daha iyi anlaşılmaktadır. Bilgi güvenliği politikaları ve alınan bilgi güvenliği önlemleri, Türk Hukuk Mevzuatındaki önleyici tedbirlerin eksikliği nedeniyle oluşabilecek zafiyet ve zararların azaltılması açısından da önem taşımaktadır.

AB Hukuk Sisteminin öngördüğü veri erişim yetkilendirmeleri, bilgi güvenliği sistem tasarımları esnasında sistem yöneticileri tarafından alınması gereken teknik önlemlerdir. 95/46/EC sayılı veri koruma direktifinde bu sorumluluk, verilerin işlendiği birimlere ve dolaylı olarak bu verilerin depolandığı ve yedeklendiği ortamların sorumluluğunu üstlenen bilgi işlem sorumlularına verilmiştir. Üniversitelerde de benzer şekilde BİDB'lığının bu sorumluluk ile karşı karşıya olduğu görülmektedir.

Veri ihlalleri, veri koruma düzenlemelerinin bir parçası olarak düşünülmektedir. AB'nin 2012 yılında hazırlamış olduğu yeni veri koruma direktifi tasarısında, veri ihlali olması halinde veri koruma otoritesinin 24 saat içerisinde bilgilendirilmesine ilişkin düzenleme yapılarak bu konudaki eksiklikler giderilmeye çalışılmıştır. Ancak bu sürenin gerekli inceleme yapılarak sağlıklı bilginin verilmesi için yeterli olmadığı konusunda tartışmalar bulunmaktadır (Danagher, 2012). Verilerin hangi durumlarda ihlal edilmiş olacağı ise, AB'nin 2012 yılında hazırlamış olduğu yeni veri koruma direktifi tasarısının 4. Maddesinde[119] yer alan geniş tanımdan çıkarılabilmektedir. Veri ihlaline yönelik tanım

[119] **Personal Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

ve sonrasında uygulanacak yöntemlerin yeni hukuksal düzenlemeler içerisinde yer alması, bu konuda sadece bilgi güvenliği kapsamında önlemler alınmaya çalışılmasından kaynaklanan kişisel hak kayıplarının önlenmesine katkı sağlayacaktır. Bununla birlikte, bilgi güvenliği politikaları belirlenirken, veri ihlallerine yönelik olarak uygulanacak yöntem ve adımların hukuksal düzenlemeler içerisinde yer alan tanım ve düzenlemeler ile uyumlu olması önem taşımaktadır.

2.5.2.5. Koruma Önlemleri Kapsamında Eğitim ve Farkındalık

Bu çalışmada temel alınan McCumber bilgi güvenliği modelini de içeren ve bilgi güvenliğine ilişkin temel kaynak olarak kullanılan "Bilgi Sistemleri Güvenliği Profesyonelleri İçin Ulusal Eğitim Standartları" dokümanı, bilgi güvenliği önlemleri kapsamında nasıl bir eğitim ve farkındalık programı yapılması gerektiği hakkında çerçeveyi oluşturan bir rehber niteliğindedir. Bu dokümanda yer alan farkındalığın oluşturulmasına yönelik ilkelerin, ulusal bilgi güvenliği politikaları ve risk yönetimini, tehditlere karşı kullanılacak teknik önlemlerin önünde tutması dikkat çekicidir. Türkiye'de de bilgi güvenliği önlemlerinin alınmasına ilişkin eğitim programlarının standartlaştırılarak yaygın hale getirilmesi için, hukuksal düzenlemeleri de dikkate alan ulusal ve kurumsal yazılı bilgi güvenliği politikalarının geliştirilmesine ihtiyaç duyulmaktadır. Kişisel verilerin elde edilmesi, işlenmesi, kullanılması, paylaşılması, silinmesi ya da imha edilmesi aşamalarının her birinde bilgi işlem merkezi çalışanlarının ve kurum içinde bu verileri işleyen personelin eğitim yoluyla farkındalığının arttırılması önem taşımaktadır.

Literatürde bilgi güvenliği farkındalığının ölçülmesine ilişkin farklı yaklaşımların bulunduğu ve buna bağlı olarak farklı sonuçlara ulaşılabildiği görülmektedir. Farkındalığın ölçülmesinde dikkate alınması gereken değişkenler çoğu zaman ihmal edilmektedir. Kullanıcıların bilgi varlıklarının korunmasına ilişkin bilgi düzeyleri, sahip oldukları bilgiyi uygulamaya dönüştürme eğilim ya da yetenekleri ve bu dönüşümü gerçekleştirmek için gerekli yetkiye sahip olma durumu, farkındalığın ölçülmesiyle ilgili sonuçların değişmesinde etken unsurlardır. Hukuksal sorumluluklar kapsamında bu unsurların tümünün dikkate alınması halinde farkındalığın doğru bir şekilde ölçülmesi ve

buna ilişkin gerekli önlemlerin alınması ya da strateji geliştirilmesi mümkün olabilmektedir.

TCK'nın 135., 136 ve 138. Maddesinde kişisel verilerin korunmasına yönelik olarak yapılan düzenlemelerin, kişisel verilerin korunması konusunda sınırlı ve yetersiz olduğu görülmektedir. Bunun yanı sıra, TCK kapsamında cezai yaptırım uygulanabilmesi ve uyulacak esasların belirlenmesi için kişisel verilerin korunması kanununun yapılması gerekmektedir. TCK'da doğrudan kişisel verilerin korunmasına yönelik maddelerin (135,136 ve 138) dışındaki özel hayata ve hayatın gizli alanına karşı suçların (132, 133 ve 134. maddeler) soruşturulması ve kovuşturulması şikâyete bağlıdır[120]. Bu nedenle, bilgi güvenliği çerçevesinde kişisel verilerin korunmasında önemli bir yere sahip özel hayata karşı suçlarla ilgili olarak farkındalığın arttırılması ve bilgi güvenliği politikalarında bu konuya yer verilmesi önem taşımaktadır.

[120] **TCK, 139. Madde:** (1) Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikâyete bağlıdır.

3. BÖLÜM

ÜNİVERSİTELERDE BİLGİ GÜVENLİĞİ VE RİSK YÖNETİMİ

Bilgi sistemleri üzerinde bulunan tüm verilerin kriptolama gibi üst seviyede bilgi güvenliği önlemleri ile korunmasının maliyeti yüksek olacağı için, kurum ve kuruluşların bütün veriler için yukarıda söz edilen önlemleri alması beklenmemelidir. Ancak hassas ve kişisel veriler, üst seviyede güvenlik önlemleri ile korunması gereken verilerdir. Bu nedenle, kurum ve kuruluşlarda işlenen verilerin tanımlanması, değerlendirilmesi, sınıflandırılması ve tüm veriler içindeki önceliğinin belirlenmesi, etkin güvenlik önlemlerinin alınması ve risk yönetiminin sağlanması için önemlidir (Whitman ve Mattord, 2011). Risk yönetimi, bir kurum ya da kuruluştaki bilgi varlıklarının karakteristik özelliğinin korunması amacıyla değerlendirmenin yapılması ve eksikliklerin giderilmesine yönelik gerekli adımların atılmasıdır. Kurum ve kuruluşlarda bilgi güvenliğinin sağlanmasına ilişkin risk temelli yaklaşım, bilgi güvenliği politikalarının geliştirilmesi, standartların uygulanması ve hukuksal düzenlemelerin tanımlanması için zorlayıcı etki oluşturmaktadır (NIST, 2009). Üniversitelerde risk yönetimi için bunların sağlanması gerekir.

3.1. ÜNİVERSİTELERDE RİSK YÖNETİMİ

Yeni risk ve tehditlerin her an geliştirilmekte olduğu internet ortamında bilgi güvenliğinin tamamen sağlanması hiçbir zaman mümkün olamamaktadır. Kusursuz bir güvenlik sisteminin geliştirilmesi de mümkün değildir. Ancak kamu kurum ve kuruluşlarında kişisel verilerin bulunduğu sunucu ve çalışma istasyonlarının büyük bölümünün internete bağlı olarak çalıştığı bilinmektedir (DDK, 2013). Kişisel verilerin bulunduğu ortamların teknik imkânlar dâhilinde korunması, uygulanan risk yönetimi ile orantılı olarak sağlanabilmektedir. Bu nedenle kurum ve kuruluşlarda kişisel verilerin korunmasına ilişkin teknik önlemler alınırken, kusursuz bir bilgi güvenliği değil, kurum ya da kuruluşun ihtiyaçlarına uygun bir güvenlik politikasının uygulanması hedeflenmelidir. Belirlenen güvenlik politikalarının ihtiyaçların ötesinde olması, zaman kaybı ve maliyetin artması gibi olumsuzlukların dışında bir katkı sağlamayacaktır. Bunun için, teknoloji,

değişen tehditler, algılanan risk ve gerçek risk arasında denge kuran politikalar benimsenmelidir.

Üniversiteler ve kurumlarda bilgi sistemleri aracılığıyla işlenen veya elektronik ortamlarda bulundurulan kişisel verilere yönelik risk seviyesinin belirlenebilmesi için, öncelikle korunması gereken yazılı-basılı ve elektronik bilgi varlıklarının belirlenmesi ve bu bilgi varlıklarının sınıflandırılması[121] gerekmektedir. Kişisel veriler, hassas veriler ve herkesin erişimine açık olan verilerin yerleri belirlenerek, uygulanacak güvenlik politikaları buna uygun olarak şekillendirilmelidir. Bu aşamada bilgi varlıklarının karakteristik özelliğine[122] uygun olarak derecelendirme (düşük, orta ya da yüksek etki gibi) ve değerlendirme yapılmalıdır. Bu değerlendirme yapılırken, bilginin durumu[123] da göz önüne alınmalıdır (NIST, 2009). Bilgi varlıklarının değerlendirmesini, bilgi varlıklarına yönelik tehditlerin ve kurumsal ihtiyaçların dikkate alındığı risk değerlendirmesi izlemelidir. Risk değerlendirme işlemi, korunması gereken bilgi kaynaklarına karar verilmesi ve bu bilgi kaynaklarının karakteristik özelliklerinin kaybedilmesine neden olabilecek potansiyel risklerin belirlenmesi sürecidir. Kabul edilen ya da kontrol edilmesi (ortadan kaldırma, azaltma ya da devretme) gereken risklere yönelik değerlendirmeler, oluşturulacak bilgi güvenliği politikalarının en önemli kaynaklarıdır. Risk değerlendirmesine bağlı olarak hazırlanan risk işlem planı ya da kapsamlı bilgi güvenliği politikaları, bu tehditlerin nasıl kontrol edileceğini göstermesi nedeniyle risk yönetimi ve bilgi güvenliğinin sağlanması sürecinin en önemli bileşenleridir. Risk yönetimi sürecinde kişisel ve hassas verilerin işlendiği birimlerdeki bilgi sistemlerine yetkisiz erişimlerin engellenmesi için alınabilecek tüm teknik önlemler gözden geçirilirken, bu birimlerde çalışan personelin niteliği ve farkındalığı da aynı kapsamda değerlendirilmelidir. Nispeten daha az güvenlik önlemi alınarak korunan herkesin erişebileceği veriler için ise, gerçekleşme olasılığı bulunan ihlallerin etkilerini en aza indirme ve veri bütünlüğü sağlanarak sistemin en kısa sürede yeniden hizmet verebilecek duruma getirilmesi için atılacak adımlar belirlenmelidir.

---

[121] Üniversitelerde verilerin sınıflandırılmasına ilişkin örnek için bkz. (http://security.harvard.edu/files/it-security-new/files/data_classification_table_abridged_7.23.13_0.pdf)

[122] Detaylı bilgi "2.2.4. McCumber Bilgi Güvenliği Modelinin Unsurları" konusu altında yer almaktadır.

[123] Detaylı bilgi "2.2.4. McCumber Bilgi Güvenliği Modelinin Unsurları" konusu altında yer almaktadır.

Kişisel ve hassas verilerin korunması konusundaki ana hedef bireyin temel hak ve özgürlüğünün korunması olduğu için, bu verilerin yetkisiz erişimlerden korunması öncelik taşımaktadır. Dolayısıyla bu tür verilerin açığa çıkması ve internet üzerinde hızla çoğalmasının önüne geçebilecek önlemler, ihlal sonrasında verinin güncel ve değiştirilmemiş halinin geri yüklenmesi için alınan önlemlerden çok daha önemlidir. Bu noktada kişisel verilerin korunması için alınacak bilgi güvenliği önlemleri ve belirlenecek strateji, diğer veriler için alınacak önlemlerden ayrışmaktadır. Bireyin temel hak ve özgürlüğü kapsamında kişisel verilerin teknik yöntemlerle korunması, bilgi güvenliği açısından bakıldığında öncelikli olarak bilginin gizliliğinin korunması ile sağlanabilmektedir. Risk yönetimi kapsamında risklerin kontrol edilmesi (ortadan kaldırma, azaltma ya da devretme) açısından bakıldığında ise, kişisel verilerin korunmasına yönelik olarak gerçekte seçenek olmadığı söylenebilir. Çünkü kişisel verilerin korunmasına ilişkin riskler, azaltılması ya da başka bir kuruluşa (servis sağlayıcı, sigorta şirketi vd.) devredilmesi mümkün olmayan risk grubu içinde yer almaktadır. Bu nedenle risk yönetim süreci içinde bilgi varlıklarının değerlendirilmesi ve önceliklerinin belirlenmesi aşamaları, kişisel verilerin korunması açısından özel öneme sahiptir.

Kurum ve kuruluşlarda risk yönetiminin amacı; değeri belirlenen bilgi varlıklarının korunması için, olası tehditlere bağlı olarak belirlenen risklerin kabul edilebilir seviyeye indirilmesidir. Tüm kurumlarda olduğu gibi üniversitelerde de risk yönetiminin etkin olarak yapılabilmesi, uluslararası güvenlik standartları, hukuksal koşullar ve kapsamlı bilgi güvenliği modeli çerçevesinde oluşturulan bilgi güvenliği politikaları ile sağlanabilmektedir. Kişisel verilerin korunmasını amaçlayan risk yönetim politikaları, risk yönetimine ilişkin unsurların en önemli ve öncelikli bileşenidir (Crouhy, Galai ve Mark, 2006). Hassas ve kişisel verilere yönelik tehditlerin değişken olması, bilgi güvenliğinin sağlanması sürecinde alınması gereken önlemlerin de değişken olmasına neden olmaktadır. Bu nedenle üniversitelerde bilgi güvenliği ve risk yönetiminde sürekliliği sağlayan koruma önlemleri, sistem yaşam döngüsüyle birlikte değerlendirilmelidir. Bilgi sistemleri üzerindeki güvenlik seviyesinin belirlenmesi ve daha üst seviyeye getirilmesi amacıyla yapılan risk belirleme ve yönetme işlemlerine, bilgi güvenliğine ilişkin yaşam döngüsünün tüm aşamalarında başvurulmaktadır. ISO

27001 ve 27002 standartları çerçevesinde oluşturulan yaşam döngüsü, üniversitelerin büyüklüğü ve yapısına bağlı olarak risk yönetimine ilişkin stratejik kararların alınması, ihtiyaca bağlı olarak bilgi güvenliği politikalarının geliştirilmesi ve bu politikaların uygulamadaki etkinliğinin izlenerek iyileştirmelerinin yapılmasına katkı sağlamaktadır. Risk yönetiminin de bir parçası olduğu ve uluslararası güvenlik standartlarının temelinde var olan yaşam döngüsü; planlama, uygulama, kontrol ve önlem alma süreçlerinden oluşmaktadır (Whitman ve Mattord, 2011). Yaşam döngüsü içinde yer alan unsurlar birbirini izleyecek ve üniversite için yaşayan bir süreci oluşturacak şekilde uygulanmalıdır. Bununla birlikte, ISO 27001 standardına ilişkin denetim listesinin tüm aşamalarında risk yönetimi kapsamında yerine getirilmesi gereken sorumlulukların sorgulandığı görülmektedir. Bir kuruluşun ISO 27001 standardı kapsamında bilgi güvenliği yönetim sistemi kurabilmesi için, öncelikle risk analizi ile belirlenen riskleri kabul edilebilir seviyeye indirmesi gerekmektedir (Ottekin, 2008).

3.1.1. Üniversitelerde Kişisel Veri Algısı

Kişisel ve hassas verilerin hayatın içindeki anlamı, günlük hayatta çoğu zaman bilimsel olarak açıklandığı ya da tanımlandığı şekliyle algılanmamaktadır. Örneğin bir hastanın kan değerleri son derece önemli bir kişisel veri olarak algılanırken, düşük not alan üniversite öğrencilerinin notlarının listelerle ilan edilmesi genellikle tartışma konusu dahi olmamaktadır. Oysa bireyin eksik yönünü ortaya koyması açısından değerlendirildiğinde, her iki bilgi de bireyin toplum içindeki konumunu ya da onun hakkındaki düşünceyi hemen hemen aynı seviyede değiştirme etkisine sahiptir. Kişisel haklara önem veren ülkelerin hukuk mevzuatlarında bu tür detaylara ilişkin hukuksal düzenlemelerin de yapıldığı görülmektedir. Örneğin ABD'de 1974 yılında yürürlüğe giren "Aile Eğitim Hakları ve Gizlilik Yasası" (The Family Educational Rights and Privacy Act - FERPA) isimli federal kanun, eğitimle ilgili olan kayıtlara ilişkin hukuksal düzenlemeler içermekte ve öğrencilerin rızası bulunmadığı sürece öğrencinin notları da dâhil olmak üzere tüm kayıtlarının gizliliğinin korunmasını zorunlu hale getirmektedir (FERPA, 1974). Bu yasaya bağlı olarak üniversitelerin belirlemiş oldukları bilgi politikaları da web

sayfaları üzerinde yer almaktadır[124]. Kişisel verilerin korunması çerçevesinde konuya bu yönü ile bakıldığında, üniversite birimlerinde kayıtlı kişisel verilerin, öğrenci ve personele ait kimlik bilgileri ile sınırlı olmadığı değerlendirilmektedir. Kişilerle ilişkilendirilen öğretim bilgileri de kişisel verilerle aynı düzeyde korunması gereken bilgi varlıkları arasında yer almaktadır.

AB sınırları içinde yer alan bazı üniversitelerde, ağ üzerinde bulunan IP adresi ile bilgisayarın ve buna bağlı olarak bilgisayarın kullanıcısının tanımlanabildiğine dikkat çekilerek, IP adreslerinin de kişisel veriler olarak değerlendirilmesi yapılmış ve veri koruma politikası bu çerçevede geliştirilmiştir (Cambridge University, 2012). Bazı üniversitelerin bilgi merkezleri (Hannover University, 2014) tarafından yapılan istatistik amaçlı çalışmalarda kişilerle ilişkilendirilebilecek IP adres kayıtlarının tutulmamasına özen gösterilmesi, bu konudaki detayların dahi önemsenmekte olduğunu ortaya koymaktadır. Ancak buna karşın, bu konuda herhangi bir bilgiye yer verilmeyen üniversite web siteleri de bulunmaktadır. Türkiye'deki üniversitelerin de kişisel verilerin korunmasına ilişkin yaklaşımlarıyla bu sınıfta yer almaları nedeniyle, Türkiye'deki üniversiteler için bu konu daha önemli bir noktaya taşınmaktadır.

3.1.2. Uluslararası Bilgi Güvenliği Standartlarından Elde Edilebilecek Kazanımlar

Kişisel verilerin korunmasına ilişkin olarak uluslararası standartlarda yer alan koşulların üniversitelerde de sağlanabilmesi amacıyla, üniversite bilgi güvenliği politikaları içerisinde bu konuya ilişkin detayların yer almasının etkili olacağı değerlendirilmektedir. Bilgi güvenliği politikaları belirlenirken, risk yönetimi, farkındalık, tehditler, teknik çözümler ve hukuksal düzenlemeler temel çerçeve içerisinde göz önünde bulundurulmaktadır. Bu çerçeve belirlenirken genel itibariyle uluslararası bilgi güvenliği standartlarından da faydalanılması, üniversiteler için geliştirilecek bilgi güvenliği politikalarında bu temel konularda eksikliklerin bulunmaması açısından önem taşımaktadır. Bilginin bir varlık olarak değer görmesi, riskler konusunda farkındalığın

[124] Bkz. http://www.washington.edu/students/reg/ferpafac.html
http://www.umd.umich.edu/policies_ferpa/
http://www.uky.edu/Legal/files/Posting%20Grades.pdf
http://www.provost.illinois.edu/resources/Faculty/FacultyGrading_FERPA_Provost092809_bkw.pdf
http://kb.iu.edu/data/augs.html

yaratılması ve bilgi akış sürecinin kesintisiz olarak işlemesinde de bilgi güvenliği standardının uygulanması önemli ölçüde katkı sağlamaktadır. Bu yönüyle değerlendirildiğinde, ISO 27001 standardının uygulanması ile elde edilecek kazanımlar şöyle sıralanabilir (ISO/IEC, 2008);

- Bilgi güvenliği ile ilgili olarak ilke ve amaçların belirlenmesi, risk değerlerinin belirlenmesi ve politikaların yapılmasına katkı sağlamaktadır.
- Bilgi varlıkları ve güvenlik gereksinimi hakkında kullanıcılarda farkındalığın oluşmasını ve kullanıcıların sürece aktif katılımını sağlamaktadır.
- Meydana gelebilecek felaketler karşısında sistem çalışma sürekliliğinin oluşmasını sağlamaktadır.
- Standardı uygulayan kurum ya da şirkete karşı güven ve saygınlık kazandırmaktadır.
- Bilgi, bilgi sistemleri ve kullanıcılarını bilişim suç ve saldırılarından bütünüyle korumaktadır.
- Güvenlik risklerinin ve maliyetlerin yönetilebilir olmasını sağlamaktadır.
- Personelin bilgi sistem kaynaklarını kötü amaçlı olarak kullanmasına engel olmaktadır.
- Bilginin doğruluk, gizlilik ve bütünlüğünün bozulmamasına katkı sağlamaktadır.
- Bilgi güvenlik önlemlerinin yasal düzenlemeler ile uyumlu olmasını sağlamaktadır.
- Kurum ya da şirketin bilgi güvenliği politikalarına ne kadar uyumlu olduğunun etkin ölçümünde ve denetiminde kolaylık sağlamaktadır.

Bu kazanımlar üniversitelerde bilgi güvenliğinin oluşturulması açısından önemlidir. Ancak bu şartları dikkate almayan birçok üniversite bulunmaktadır. Bunun başlıca nedenleri arasında; kullanıcılarda farkındalığın oluşmasıyla daha fazla sorumluluk almanın meydana getireceği olumsuzlukların değerlendirilmesi, bilginin teknik imkânlarla gizliliğinin korunmasının kişisel hakların korunmasından daha öncelikli olarak değerlendirilmesi, bilgi güvenliği önlemlerinin yasal düzenlemeler ile uyumlu hale getirmenin zorlukları ve yeterli düzeyde uzman personelin bulunmaması sayılabilir.

3.2. ÜNİVERSİTELERDE BİLGİ GÜVENLİĞİ ÖNLEMLERİ

Üniversitelerde kişisel verilerin korunması amacıyla alınan teknik önlemlerin içinde, öncelikli olarak erişim yetkilerinin düzenlenmesiyle veri gizliliğinin korunması amaçlanmaktadır. Bunun yanı sıra alınabilecek başlıca önlemler; bilginin sınıflandırılması, bilgi depolama alanının korunması, güvenlik politika uygulamalarının kullanılması ve bilgileri işleyen personele eğitim verilmesidir (Whitman ve Mattord, 2011).

Üniversitelerde işlenen ve özellikle arşiv olarak depolanan hassas ve kişisel verilerin bütünlüğünün bozulup bozulmadığının en kısa sürede anlaşılması ve gerekli müdahalenin yapılması, bilgi güvenliği politikaları içinde yer alması gereken önemli noktalardan biridir. Bütünlüğünün korunduğundan emin olunamayan bilginin değeri hakkında da kesinlik bulunmamaktadır. Bunun için alınabilecek en etkili güvenlik önlemlerinin başında verilerin ilk andan itibaren hash değerlerinin[125] periyodik olarak hesaplanması ve hash değerinde herhangi bir değişiklik olması halinde gerekli müdahalenin yapılması gelmektedir (Whitman ve Mattord, 2011).

Güvenlik önlemleri içinde eğitim konusu, bilgi sistemlerini tasarlayan ve yazılım geliştiren uzmanlar için de önem taşımaktadır. Sistem hatalarından kaynaklanan güvenlik zafiyetlerinin sayısının artmasında, sistem tasarımcılarının bu konuyu yeterince önemsememelerinin de etkisi bulunmaktadır. Üniversitelerin bilgisayar bilimlerine ilişkin alanlarda, bilgi güvenliğine yönelik yeterli düzeyde program ve ders bulunmadığı görülmektedir (McCumber, 2005). Bunun yol açtığı sonuçlardan biri olarak, yeni sistem ya da programlar için genellikle ihlallerin gerçekleşmesinden sonra güvenlik önlemleri alınmaktadır. Türkiye'de üniversitelerde bilgi güvenliği eğitiminin yeterli düzeyde verilememesi, bilgi güvenliği alanında yetişmiş öğretim üyesinin bulunmaması ile açıklanmaktadır (Bil.Güv.Müh. ABD, 2013). Güvenlik önlemlerinin alınması kapsamında verilen eğitimler, "bilgi" ve "performans" seviyelerinden oluşan iki farklı düzeyde verilmektedir. "Bilgi" düzeyinde, bilgi sistemlerine yönelik tehditler ve verileri korumak için gerekli politikalar hakkında eğitim verilmektedir. "Performans" düzeyinde

[125] Hash değerine ilişkin detaylı bilgi için bkz. (Henkoğlu, 2011)

ise, bilgi güvenliği politikalarının verilerin işlenmesi esnasında uygulanması ve çalışanlara bu yeteneğin kazandırılması hedeflenmektedir (NSTISSI, 1994). Üniversitelerde kişisel verileri işleyen birimlerde çalışan personelin her iki düzeyde de eğitim alması, farkındalığın etkin olarak uygulamada görülebilmesi açısından önemlidir.

Üniversitelerde işlenen kişisel verilerin korunmasına yönelik risk değerlendirmesi ve bunun sonucuna bağlı olarak eğitim programları yapılırken; bilgi sistemlerinin yapısı, kayıtlı personel sayısı, kişisel bilgilere erişim sağlama, kişisel verilerin hangi amaçla kullanıldığı gibi unsurlar da göz önüne alınmalıdır. Üniversitelerde kişisel verilerin bulunduğu bilgi sistemlerinin bağlı olduğu iletişim ağına bağlı olarak, belirlenen politikaların ve uygulanan güvenlik önlemlerinin etkinliği farklılık gösterebilmektedir. Bu konuda kullanım yaygınlığı ile orantılı olarak en fazla ihlalin gerçekleştiği sosyal paylaşım ağları örneğine kısaca değinmekte fayda bulunmaktadır. Yapılan araştırmalar, sosyal paylaşım ağlarının kişisel veri elde etmek için kullanılan en etkili araçlardan biri olduğunu göstermektedir (ENISA, 2013). Her ne kadar sosyal paylaşım ağlarında kişisel veriler açıkça paylaşılmasa da, kullanıcıların kurumsal veri transfer servisleriyle ilgili teknik sorunlar yaşadıklarında daha pratik olması nedeniyle sosyal paylaşım ağları üzerinden veri transferi yaptıkları görülmektedir. Ancak bu transfer edilen bilgiler kullanıcı tarafından silinse dahi, aktarımın gerçekleştiği sunucular üzerinde uzun süre bir kopyası tutulmaktadır. Bu nedenle, özellikle kurumsal işlemlerde bu tür verilerin sosyal ağlar üzerinde bulundurulması ya da aktarılması konusunda daha dikkatli olunması gerekmektedir[126].

3.3. ÜNİVERSİTELERDEKİ MEVCUT DURUMUN DEĞERLENDİRİLMESİ

AB sınırları içinde yer alan üniversitelerde bilgi güvenliğine yönelik olarak alınan önlemler ve geliştirilen uygulamalar, "bilgi güvenliğinin sağlanması" konusu çerçevesinde tanımlanmaktadır[127]. Bu üniversitelerde kişisel verilerin elde edilmesi ve

[126] 2006 yılında yaşanan AOL skandalı, bu konudaki önemli örneklerden biridir. AOL, 658 bin kullanıcısının bilgi arama sonuçlarından elde ettiği ve kişisel bilgi olarak nitelendirilebilecek 20 milyon özel bilgiyi içeren dosyaları ifşa etmiştir (Erola, Castellà-Roca, Viejo ve Mateo-Sanz, 2011).

[127] Bkz. http://www.admin.cam.ac.uk/univ/information/dpa/studentdata.html
http://www.admin.ox.ac.uk/councilsec/compliance/dataprotection/policy/
http://www.southampton.ac.uk/inf/dppolicy.pdf

işlenmesi sürecinin tümünü kapsayan yazılı bilgi güvenliği ve kişisel verileri koruma politikalarının, hukuksal düzenlemelerin de dikkate alınarak yapıldığı ve bu politikaların üniversite yönetim birimlerinin (konsey sekreterliği gibi) web sayfalarında yayınlandığı görülmektedir (Cambridge University, 2013; Oxford University, 2013). Türkiye'deki farklılık ya da eksikliklerin görülebilmesi amacıyla, aynı koşullarda bir ön incelemenin yapılması gerektiği değerlendirilmiştir. Türkiye'deki üniversitelerde bilgi güvenliğinin sağlanması ve kişisel verilerin korunmasına ilişkin politikaların varlığını araştırmak amacıyla, araştırma kapsamında yer alan Ankara'daki 15 üniversitenin web siteleri detaylı olarak incelenmiştir. Bu incelemede üniversite BİDB, PDB ve bilgi merkezlerinin sayfaları ile birlikte, üniversite etik kurallarına ilişkin yönergeler üzerinde de içerik analizi yapılmıştır.

Üniversitelerin web sayfaları üzerinde yapılan inceleme ve elde edilen bulgulara göre, bilgi güvenliğini sağlamaya ilişkin sorumluluğun tüm üniversitelerde BİDB'lığına verildiği ve bu nedenle bilgi güvenliği önlemlerinin alınmasına yönelik çalışmaların sadece üniversitelerin BİDB'lığı tarafından yürütüldüğü görülmektedir. Personel ve öğrencilere ait kişisel verileri işleyen üniversite PDB ve bilgi merkezlerinin web sayfalarında, bu verilerin işlenmesine ve korunmasına yönelik politika ve etik ilkelerin bulunmadığı tespit edilmiştir. Üniversite etik kurul yönergelerinde de bu konuya ilişkin ifadelere yer verilmemiş ve gereken etik duyarlık gösterilmemiştir.

Bilgi güvenliği konusunun sadece BİDB'lığı ya da bilgi işlem birimlerinin sorumluluğunda olması, üniversitelerin bilgi güvenliğine yaklaşımı üzerinde de etkili olmaktadır. Üniversitelerin web sayfalarında bilgi güvenliğinin sağlanmasına ilişkin olarak sadece teknik önlemlerin alınması üzerinde durulduğu görülmektedir. Bu önlemler arasında bilgi güvenliği kapsamında yer alan bilginin durumu, bilgi güvenliği politikaları ve hukuksal boyutu ikinci planda kaldığı gibi, kişisel verilerin korunması konusunun gündeme dahi alınmadığı görülmektedir. Bazı üniversitelerin "Bilişim Hizmet ve Kaynakları Kullanım Yönergesi"'nde bir cümle ile mahremiyetin korunacağına ilişkin

---

http://www.helsinki.fi/atk/tike/en/tietoturva/politiikat_ja_saannot.html
http://www.eng.unibo.it/PortaleEn/PolicyPrivacy.htm
http://www.ucd.ie/dataprotection/policy.htm
http://www.us.es/eng/legal/condiciones

ifade bulunsa da, bunun nasıl sağlanacağı, sorumluluklar ve hukuksal dayanaklarından bahsedilmemektedir.

İki üniversitenin BİDB'lığı web sayfasında OECD ilkelerine yer verildiği görülmektedir. Kullanıcı bilinçliliğini sağlamaya katkıda bulunan bu yaklaşımın olumlu olduğu değerlendirilmektedir. Ancak içeriğinde risk yönetimi ve tehditlere karşı alınacak önlemlerle ilgili tüm sorumluluğun kullanıcılara verilmiş olduğu bu belgenin üniversiteler için tek başına yetersiz olduğu değerlendirilmektedir. Bununla birlikte, bir ticari örgüt olarak OECD'nin hazırlamış olduğu rehber ilkelerde, verilerin serbest dolaşımının kişilik haklarının korunmasından daha öncelikli değerlendirildiği söylenebilir. OECD rehber ilkelerinin temel amacı, ülkelerin ulusal veri koruma kanunları arasındaki farklılıkların sınır ötesi veri akışına engel olmasına dikkat çekmektir. OECD rehber ilkelerine web sayfalarında yer veren üniversitelerde bu rehber ilkelerin üniversite için "nasıl" uygulanacağını da adresleyen güvenlik politikalarının geliştirilmemiş olduğu görülmektedir.

Üç üniversitenin web sayfasında 5651 sayılı kanunun üniversiteye uyarlanmış ve kullanıcı sorumluluklarının altını çizen bir belgenin yayınlanmış olduğu görülmektedir. Kişisel verilerin korunmasına dolaylı olarak katkı sağlayan bu belgelerin hazırlanmış olması üniversiteler için önemli bir adım olarak görülmekle birlikte, bilişim sistemleri ve veri korumaya ilişkin hukuk mevzuatı içinde çok küçük bir payı oluşturan bu düzenlemenin de yetersiz olduğu düşünülmektedir.

Web sayfaları incelenen 15 üniversitenin hiçbirinde, kayıt altına alınan kişisel verilerin sınırlandırılması, korunması, ne kadar süre ile saklanacağı ve nasıl imha edileceğine dair sorumlulukların açıklanmadığı görülmektedir. Bu nedenle web siteleri üzerinden yapılan araştırma sonucunda, veri sahiplerinin kişisel haklarına üniversitelerin göstermiş olduğu hassasiyetin yeterlilik düzeyine ilişkin bir çıkarımda bulunulamamaktadır. Verilerin saklanması ile ilgili olarak sadece bir üniversitenin web sayfasında detaylı "saklama planı" bulunduğu ve saklama sürelerine ilişkin bilgilere yer verildiği görülmektedir. Ayrıca bazı üniversitelerin web sayfalarında Arşiv Hizmetleri Hakkında Yönetmeliğin bulunduğu ve arşiv hizmetlerinin bu yönetmeliğe göre yürütüldüğü görülmektedir. Ancak

bu yönetmeliklerin içeriğinin Devlet Arşiv Hizmetleri Hakkında Yönetmeliğe uygun olarak hazırlanmış olduğu ve bu nedenle elektronik arşiv malzemelerinin korunmasına ilişkin olarak fiziksel güvenlik önlemleri ile sınırlı kaldığı görülmektedir.

4. BÖLÜM

BULGULAR

Üniversitelerde bilgi güvenliğinin sağlanmasına yönelik olarak araştırma kapsamında Ankara'da bulunan 15 üniversitede kişisel verilerin yoğun olarak işlendiği ve bu verilerin korunması konusunda öncelikli olarak sorumluluğu bulunan bilgi işlem, personel ve bilgi merkezi daire başkanlarına yüz yüze görüşme yoluyla anket uygulanmıştır. Toplam 44 daire başkanı (15 BİDB, 14 PDB ve 15 KDB) araştırmaya katılarak görüş bildirmiştir. Bir PDB katılımcısı üniversite rektörlüğünün bilgi güvenliğine yönelik görüşmeleri uygun bulmadığı gerekçesiyle görüşmeyi kabul etmemiştir. Araştırma sonucunda nicel bulguların yanı sıra açık uçlu sorulara verilen yanıtlardan ve görüşmeden elde edilen veriler de elde edilmiştir. Veri elde edilen konuyu açıklamak amacıyla bu verilerin tamamı bir arada verilmiştir.

Araştırma soruları; hukuksal düzenlemelerin yeterliliği, kişisel verilerin korunmasına ilişkin bilgi güvenliği politikaları, üniversitelerde kişisel verilerin toplanması, düzenlenmesi ve güncellenmesi, kişisel verilerin kullanımı ve paylaşımı, üniversitelerde kişisel verilerin korunması amacıyla alınan bilgi güvenliği önlemleri ve bunların hukuksal düzenlemelere uyumluluğu, verilerin korunmasına ilişkin sorumluluklar, üniversitelerde bilgi güvenliğine ilişkin risk durumu ile eğitim ve farkındalık durumuna ilişkin bulgular elde etmek amacıyla hazırlanmıştır. Soruların hazırlanmasında hukuk mevzuatlarından elde edilen veriler temel alınmıştır. Araştırma sorularının konusu olan kişisel veriler, gerçek kişi ile ilişkili olarak değerlendirilmektedir. Bilgi güvenliğine ilişkin bu konularda elde edilecek bulgular ile mevcut durum, eksiklikler ve ihtiyaçlar hakkında bilgi sağlanarak, üniversiteler için hukuksal düzenlemeler ve örnek bilgi güvenliği modeli çerçevesinde bir bilgi güvenliği politikasının geliştirilmesi amaçlanmıştır.

Araştırma kapsamında katılımcılara yöneltilen sorular EK 1'de yer almaktadır. Tablo ve değerlendirmede sık kullanılan üniversite daire başkanları ve birimleri, BİDB (Bilgi işlem daire başkanlığı), PDB (Personel daire başkanlığı) ve KDB (Kütüphane ve dokümantasyon daire başkanlığı) kısaltmaları ile kullanılmıştır. Soruların niteliğine ve

daire başkanlıklarının görev kapsamlarına bağlı olarak; bazı sorular sadece BİDB ya da KDB katılımcılarına yöneltilmiş; bazıları ise BİDB, PDB ve KDB katılımcılarının tümüne yöneltilmiştir. Ancak üniversite birimlerinin sorulara bakış açılarında farklılıklar bulunduğu için, bu tür sorular da tablo üzerinde ayrı ayrı hesaplanarak gösterilmiştir. Elde edilen veriler içerisinde görüşmeye katılmayan bir PDB katılımcısı da diğer bazı soruları yanıtlamayan katılımcılar ile birlikte değerlendirmeye alınmamış ve değerlendirme dışı (DD) olarak belirtilmiştir. Tablolarda belirtilen oranlar, sorulara yanıt veren katılımcılar üzerinden hesaplanmıştır.

4.1. ÜNİVERSİTELERDE HUKUKSAL DÜZENLEMELER VE KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN BİLGİ GÜVENLİĞİ POLİTİKALARI

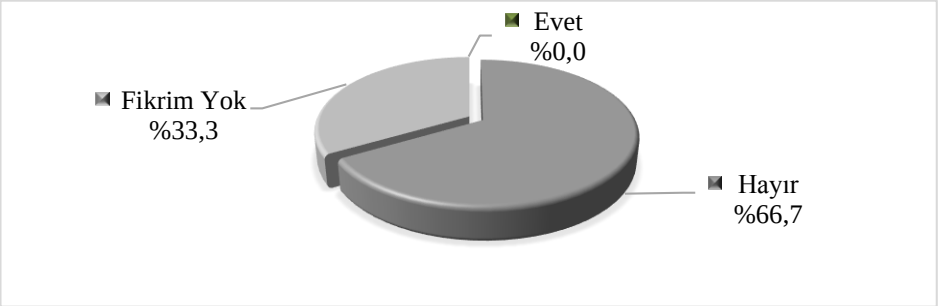
Üniversitelerdeki hukuksal düzenlemeler ve kişisel verilerin korunmasına ilişkin bilgi güvenliği politikaları, çalışma kapsamında öncelikli olarak üniversite web sayfalarında içerik analizi yapılarak incelenmiştir. Araştırma kapsamında yer alan Ankara'daki 15 üniversitenin web sayfaları üzerinde yapılan incelemelere ve elde edilen bulgulara göre; bilgi güvenliğinin sağlanmasına ilişkin düzenleme bulunmadığı gibi, etik kurul yönergelerinde ve bilişim hizmet ve kaynak kullanım yönergelerinde kişisel verilerin korunmasına ilişkin gereken duyarlılığın bulunmadığı görülmektedir. Bununla birlikte, iki üniversitede OECD ilkelerine atıfta bulunulduğu, üç üniversitede ise 5651 Sayılı Kanunun üniversiteye uyarlandığı görülmektedir. Ancak yapılan içerik analizi sonrasında her iki yaklaşımın da kişisel verilerin ve kişisel hak ve özgürlüğün korunması amacının uzağında ya da yetersiz olduğu anlaşılmaktadır.

Araştırma kapsamında yer alan 15 üniversitede görüşme yoluyla uygulanan anketlerden elde edilen bulgular, kişisel verilerin korunmasına yönelik hukuksal düzenlemelerin üniversiteler tarafından nasıl uygulandığı ve bilgi güvenliği politikalarının varlığı, yeterliliği, uygulanabilirliği ve bu konudaki farkındalığa ilişkin diğer detaylı bilgilere ulaşılmasını sağlamıştır. Üniversite BİDB, PDB ve KDB katılımcılarının bu konuya ilişkin sorulara vermiş oldukları yanıtlar ve belirtmiş oldukları görüşlere bağlı olarak elde edilen bulgular, hukuksal düzenlemeler ve politikalara ilişkin başlıklar altında verilmiştir.

4.1.1. Kişisel Verilerin Korunmasına İlişkin Hukuksal Düzenlemeler ve Sorumluluklar

Bilgi güvenliği ve kişisel verilerin korunması konusundaki hukuksal düzenlemelerin yeterliliğine ve bu çerçevedeki sorumluluklara ilişkin görüşler Şekil 2 ve Tablo 1'de yer almaktadır. Üniversitelerde bilgi güvenliğinin sağlanması kapsamında teknik önlemlerin alınmasına ilişkin sorumlulukları üstlenen bilgi işlem daire başkanlarına, kişisel verilerin korunmasına ilişkin hukuksal düzenlemelerin yeterliliği hakkındaki görüşleri sorulmuş ve elde edilen bulgular Şekil 2'de gösterilmiştir.

Üniversitelerde kişisel verilerin korunmasına ilişkin olarak tüm daire başkanlarına (BİDB, PDB ve KDB) ne gibi sorumlulukları olduğu sorulmuş ve bunu hukuksal düzenlemeler çerçevesinde belirtmeleri istenmiştir. Katılımcıların Tablo 1'de yer alan hukuksal düzenlemeler içerisinde birden fazla seçeneği işaretlemelerine olanak sağlanmıştır. Elde edilen bulgular Tablo 1 üzerinde üniversite daire başkanlıklarının bu konuya bakış açılarındaki farklılıkları ve geneli yansıtacak şekilde ayrı ayrı verilmiştir.



Şekil 2 Kişisel verilerin korunmasına ilişkin hukuksal düzenlemelerin yeterliliği

Üniversitelerde kişisel verilerin saklandığı veri tabanlarının korunması konusunda sorumluluğu bulunan BİDB katılımcılarının %66,7'si, bilgi güvenliği ve kişisel verilerin korunmasına ilişkin hukuksal düzenlemelerin yeterli olmadığını düşünmektedirler. Diğer BİDB katılımcıları (%33,3) ise, hukuksal düzenlemelere ilişkin hiçbir fikrinin olmadığını belirtmektedir.

Tablo 1 Hukuksal düzenlemeler çerçevesinde sorumluluklar

Kişisel verilerin korunmasına ilişkin olarak hangi hukuksal düzenlemeler çerçevesinde sorumluluklarınız olduğunu düşünüyorsunuz?								
	BİDB		PDB		KDB		Toplam	
	N	%	N	%	N	%	N	$\%_{Ort}$
T.C. Anayasası	8	53,3	10	76,9	7	46,7	25	58,1
Türk Ceza Kanunu	11	73,3	9	69,2	6	40	26	60,5
5651 Sayılı Kanun	12	80	3	23,1	4	26,7	19	44,2
KVKK Tasarısı	8	53,3	4	30,8	7	46,7	19	44,2
AB Veri Koruma Kanunu	2	13,3	1	7,7	2	13,3	5	11,6
Hukuksal çerçevede sorumluluğumun olduğunu düşünmüyorum	0	-	1	7,7	2	13,3	3	7
Fikrim Yok	2	13,3	1	7,7	3	20	6	14
DD	-	-	2	-	-	-	2	-

Tablo 1'de yer alan sonuçlar, BİDB, PDB ve KDB katılımcılarının kişisel verilerin korunmasına ilişkin hukuksal düzenlemelere karşı farklı sorumluluklar hissettiklerini ortaya koymaktadır. Kişisel verilerin korunmasıyla ilişkili olarak katılımcıların yarıdan fazlası Anayasa (%58,1) ve TCK (%60,5), yaklaşık olarak yarısı 5651 Sayılı Kanun (%44,2) ve KVKKT (%44,2) çerçevesinde sorumluluklarının olduğunu düşünmektedirler. BİDB katılımcılarının büyük bölümü (%80) 5651 Sayılı Kanun çerçevesinde sorumluluklarının olduğunu düşünürken, PDB ve KDB katılımcıları en fazla Anayasa çerçevesinde (sırasıyla %76,9 ve %46,7) sorumluluklarının olduğunu düşünmektedirler. Bununla beraber, BİDB katılımcılarının tamamı, görüşme esnasında 5651 sayılı kanun dışındaki diğer düzenlemelerin içeriği hakkında detaylı bilgi sahibi olmadıklarını ifade etmişlerdir. Burada dikkat çekici noktalardan biri de PDB ve KDB katılımcılarının %73'ünden fazlasının 5651 sayılı kanun çerçevesinde sorumluluklarının bulunmadığını düşünmeleridir.

BİDB ve PDB katılımcılarının büyük bölümü ikinci öncelikli olarak TCK kapsamında da sorumluluklarının bulunduğunu belirtirken, KDB katılımcılarının KVKKT kapsamında daha fazla sorumluluklarının olduğunu düşünmeleri dikkat çekicidir. KDB katılımcıları içeriği hakkında tam olarak bilgi sahibi olmadıklarını belirtmekle birlikte, KVKKT ile uygulamakta oldukları etik kuralların daha fazla ortak yönünün olabileceğini düşünerek

bu seçeneği işaretlediklerini ifade etmişlerdir. Görüşme esnasında hukuksal düzenlemeler çerçevesinde sadece Anayasa ve TCK ile ilgili sınırlı sorumlulukları olduğunu düşünen PDB ve KDB katılımcıları, hukuksal düzenlemelerin yetersiz olduğunu ve bu nedenle kişisel verilerin korunmasına ilişkin olarak daha çok etik kurallar kapsamında sorumluluk hissettiklerini ifade etmişlerdir. Görüşme esnasında katılımcıların büyük çoğunluğu bu konunun hukuk mevzuatı içinde çok dağınık bir şekilde işlendiği ve bu nedenle mevzuat içerisinden sorumluluklarının belirlenmesinin kendileri için mümkün olmadığını da ifade etmişlerdir.

BİDB, PDB ve KDB katılımcılarının yaklaşık %90'ı AB Veri Koruma Kanunu kapsamında sorumluluklarının bulunmadığını ve bu kanunun içeriği hakkında bilgi sahibi olmadıklarını ifade etmektedirler. Buna karşın, henüz tasarı halinde olan KVKK kapsamında sorumluluğu olduğunu düşünen katılımcı oranının 5651 Sayılı Kanun kapsamında sorumlu olduğunu düşünenler ile aynı seviyede olduğu görülmektedir. KVKKT kapsamında sorumluluğu olduğunu düşünen katılımcılar, görüşme esnasında bu tasarının önemine de dikkat çekerek, mevcut hukuksal düzenlemelerin eksik olduğu hususlarda geliştirilecek etik kurallar için bu tasarıdan faydalanılabileceğini ifade etmişlerdir. Üç katılımcı (1 PDB ve 2 KDB) hukuksal düzenlemeler çerçevesinde herhangi bir sorumluluğunun bulunmadığını belirtmektedir. Altı katılımcı ise (2 BİDB, 1 PDB ve 3 KDB) kişisel verilerin korunmasıyla ilgili olarak hukuksal düzenlemelere hiç bakmadıklarını ve bu nedenle fikir sahibi olmadıklarını belirtmektedir. Bir BİDB katılımcısı, Tablo 1'de yer alan hukuksal düzenlemelere ilâve olarak Bilgi Edinme Kanunu ve Elektronik İmza Kanunu kapsamında da sorumluluklarının bulunduğunu ifade etmiştir.

4.1.2. Üniversitelerde Kişisel Verilerin Korunmasına İlişkin Bilgi Güvenliği Politikaları

Üniversitelerde bilgi güvenliği politikalarının varlığı, içeriği, yeterliliği, iş sürecine etkisi ve katılımcıların hukuksal koşullar hakkındaki düşüncelerine ilişkin sorulara daire başkanlarının vermiş oldukları yanıtlar Tablo 2'de yer almaktadır. Araştırma kapsamındaki tüm daire başkanlarına (BİDB, PDB ve KDB) üniversite genelinde ya da

birimlerinde uygulanan yazılı bilgi güvenliği politikalarının olup olmadığı sorulmuş ve tüm daire başkanlarından alınan yanıtlar Tablo 2 üzerinde birlikte gösterilmiştir. Bilgi güvenliği politikalarının hukuksal önlemleri ve kişisel verilerin korunmasına ilişkin hususları içerip içermediğine yönelik sorular ise sadece BİDB katılımcılarına yöneltilmiştir. Bilgi güvenliği politikalarının iş sürecine olan etkileri hakkında tüm daire başkanlarının görüşü alınmasına karşın, BİDB katılımcılarının görüşlerinde farklılık olması nedeniyle Tablo 2 üzerinde ayrı olarak gösterilmiştir.

Tablo 2 Üniversitelerde kişisel verilerin korunmasına ilişkin bilgi güvenliği politikaları

	Evet		Hayır		Fikrim Yok		DD	
	N	%	N	%	N	%	N	%
Bilgi güvenliği politikası kapsamlı teknik ve hukuksal önlemleri içeriyor mu? (BİDB)	1	6,7	14	93,3	-	-	-	-
Bilgi güvenliği politikası kişisel verilerin korunmasına ilişkin hususları içeriyor mu? (BİDB)	2	13,3	13	86,7	-	-	-	-
Kişisel verilerin korunmasına ilişkin bilgi güvenliği politikalarının olması iş süreci ve sorumluluğun tanımlanmasını kolaylaştırır mı? (BİDB)	15	100	0	-	-	-	-	-
Kişisel verilerin korunmasına ilişkin bilgi güvenliği politikalarının olması iş süreci ve sorumluluğunuzu belirlemeye katkısı olur mu? (PDB ve KDB)	24	82,8	3	10,3	2	-	1	-

Üniversite BİDB, PDB ve KDB katılımcılarının yazılı bilgi güvenliği politikasının varlığıyla ilgili olarak vermiş oldukları yanıtlar, üniversitelerde yayınlanmış kapsamlı bir bilgi güvenliği politikasının bulunmadığını göstermektedir. Araştırma kapsamında yer alan sadece iki üniversitede (%13,3) yazılı bilgi güvenliği politikasının olduğu ifade edilmiştir. Ancak bu yönde görüş bildiren üniversitelerin katılımcıları, görüşme esnasında mevcut hukuk mevzuatı içinde yer alan bazı düzenlemeleri ya da kullanım politikalarını (5651 sayılı kanun, ULAKBİM Kabul Edilebilir Kullanım Politikası gibi) üniversitenin bilgi güvenliği politikası olarak düşündüklerini ifade etmişlerdir. Bu katılımcılar, politikaların varlığına ilişkin soruyu tamamlayan "politikalara nereden erişilebilir?" sorusuna, üniversiteler tarafından geliştirilmemiş ve katkı sağlanmamış kullanım politikalarını ya da ilgili hukuksal düzenlemeleri adres göstermektedirler. Bu soru ile ilişkili olarak, üniversite BİDB katılımcılarına mevcut bilgi güvenliği politikalarının

hukuksal önlemleri ve kişisel verilerin korunmasına ilişkin hususları içerip içermediği sorulmuştur. Bilgi güvenliği politikası olduğu yönünde görüş bildiren iki üniversitenin BİDB katılımcılarından biri, üniversite için var olduğu belirtilen bilgi güvenliği politikasının kapsamlı teknik ve hukuksal önlemleri içermediğini ifade etmektedir. Bilgi güvenliği politikalarının hukuksal önlemleri ve kişisel verilerin korunmasına ilişkin hususları içerip içermediğine yönelik sorulara üniversite BİDB tarafından verilen yanıtlar değerlendirildiğinde, katılımcıların bu iki soruya vermiş olduğu yüksek orandaki (sırasıyla %93,3 ve %86,7) "hayır" yanıtlarından, bir üniversite dışında var olduğu düşünülen politikaların kapsamlı teknik ve hukuksal önlemleri içermediği ve kişisel verileri korumak için yeterli olmadığı anlaşılmaktadır. Bununla birlikte, görüşme esnasında yazılı bilgi güvenliği politikası bulunan üniversitenin BİDB katılımcısı, mevcut politikanın kişisel verilerin korunmasına yönelik hususları içermesine rağmen yetersiz olduğunu, bu konuda yeni bir çalışma yapıldığını ve onay sürecine gelindiğini ifade etmektedir. Yazılı bilgi güvenliği politikalarının varlığı konusunda, üniversite birimlerinden elde edilen bilgilerin kendi içinde tutarlı olduğu görülmektedir.

BİDB, PDB ve KDB katılımcılarının büyük bölümü (%88,6) kişisel verilerin korunmasına yönelik bilgi güvenliği politikalarının iş süreci ve sorumlulukların tanımlanmasına katkı sağlayacağı görüşünde birleşmektedirler. Özellikle bu soruyu yanıtlayan BİDB katılımcıların tamamı olumlu yanıt vermekle birlikte, üniversitelerde bilgi güvenliği politikalarının geliştirilmesine katkı sağlayacak bu tür çalışmaların da BİDB'lerin çalışma şartlarının ve sorumluluklarının belirlenmesi için önemli olduğu ifade etmektedirler. Bir KDB katılımcısı bilgi güvenliği politikalarının iş süreci ve sorumlulukların belirlemesine katkı sağlamayacağını düşündüğü halde, uygulamaya dönük açıklamaları ve beklentileriyle vermiş olduğu yanıtı çelişkili hale getirmiştir. Bu katılımcı, 5651 sayılı kanun gibi bazı hukuksal düzenlemelerin üniversitelerin yapısına uygun olmadığı için tam anlamıyla uygulanamadığını ve bu nedenle üniversitelerin bu tür düzenlemeleri dikkate alarak kendi uygulama politikalarını belirgin hale getirmelerinin zorunlu olduğunu ifade etmektedir. Bilgi güvenliği politikalarının iş süreci ve sorumlulukların belirlemesine sağlayacağı katkıya yönelik olarak olumsuz görüş bildiren diğer KDB katılımcısı, bu konudaki hukuksal düzenlemelerin herkes tarafından bilinmesi gerektiğini ve bunun yeterli olacağını ifade etmiştir. Görüşme esnasında olumlu görüş

bildiren katılımcılara genel iş sürecinde ne tür etkilerinin olabileceği de sorulmuştur. Olumlu görüş bildiren BİDB, PDB ve KDB katılımcıları, yazılı bilgi güvenliği politikalarının iş sürecini kolaylaştırmanın da ötesinde; sorumlulukların belirlenmesi, birimler arasındaki koordinasyonun sağlanması ve eksikliklerin giderilmesi için bir zorunluluk haline geldiğinin önemini vurgulamaktadırlar.

4.2. VERİLERİN TOPLANMASI, DÜZENLENMESİ VE SAKLANMASI

4.2.1. Üniversitelerde Kişisel Verilerin Toplanması

Üniversite birimlerinde kişisel verilerin elde edilmesi ve elde edilen kişisel veriler hakkında veri sahibine gerekli bilgilendirmelerin yapılmasına ilişkin bulgular Tablo 3 üzerinde yer almaktadır. Ayrıca Tablo 3 üzerinde danışma hizmetleri kapsamında yapılan araştırma kayıtlarının hizmet sunulan kişi ile ilişkilendirilmesiyle ilgili bulgulara da yer verilmiştir. Üniversite birimlerinde işlenen kişisel verilere ilişkin güncel bilgiye ulaşabilmek amacıyla, kişisel bilgilerin kaydedildiği veri tabanlarından sorumlu BİDB katılımcılarının bilgisine başvurulmuştur. Bir BİDB katılımcısı bu soruyu yanıtlamak istememiştir. Üniversitelerde en fazla ve doğrudan kişisel verilerin elde edildiği birimlerden biri olması nedeniyle, elde edilen verilere ilişkin veri sahiplerine bilgi verilmesi konusunda PDB katılımcılarının görüşü alınmıştır. İki PDB katılımcısı bu soruyu yanıtlamamıştır. Elde edilen verilerin sunulan hizmetlerle ilişkilendirilerek kullanımı konusunda ise KDB katılımcılarının görüşü alınmıştır.

Tablo 3 Üniversitelerde verilerin elde edilmesine ilişkin politikalar

	Evet		Hayır		Fikrim Yok		DD	
	N	%	N	%	N	%	N	%
Üniversite birimlerinde hangi bilgisayarlar üzerinde kişisel verilerin işlendiği bilinmekte midir? (BİDB)	9	64,3	5	35,7	-	-	1	-
Kişilerin kendisine ait toplanan tüm veriler hakkında bilgisi var mıdır? (PDB)	11	84,6	2	15,3	-	-	2	-
Danışma hizmetleri kapsamında yapılan araştırma konusu ve notları hizmet sunulan kişi ile ilişkilendirilerek kayıt altına alınıyor mu? (KDB)	2	13,3	13	86,7	-	-	-	-

BİDB katılımcılarına üniversite birimlerinde bulunan bilgisayarların hangileri üzerinde kişisel verilerin bulunduğunun bilinip bilinmediği sorulmuş ve üniversitelerin %64,3'ünde bu bilgiye sahip oldukları yanıtı alınmıştır. Ancak bu bilgiye sahip olmadıklarını belirten üç BİDB katılımcısı, üniversitelerin sahip olduğu bilgisayar sayısı (30-35 bin) dikkate alındığında, bilgisayar sayısının çok fazla olduğu üniversitelerde kontrol ve denetimlerin BİDB gibi tek bir merkezden yapılmasının mümkün olmadığına dikkat çekmektedir. BİDB ile yapılan görüşmelerde, bu tür üniversitelerin her birimde bulunan bilgi işlem sorumluları ile koordineli olarak tüm sorumlulukların paylaşılmasını sağladıkları bilgisi alınmıştır. Kontrol ve denetimlerin nispeten daha kolay yapılabildiği vakıf üniversitelerinin %80'inde kişisel verilerin işlendiği bilgisayarlar biliniyorken, bilgisayar sayısının çok fazla olduğu devlet üniversitelerinde bu oran %40 seviyesindedir.

PDB katılımcılarından kişisel hak ve özgürlüklerin korunmasıyla ilişkili olarak, elde edilen kişisel veriler hakkında veri sahibinin bilgi sahibi olup olmadığını belirtmeleri istenmiştir. Buna göre katılımcıların %84,6'sı personelin bilgisi dışında elde edilen veri olmadığını düşünmektedir. PDB katılımcıları görüşme esnasında bu konuyla ilgili olarak, üniversitelerde personele ve öğrencilere ilişkin kişisel verilerin personelin ve öğrencilerin kendilerinden ya da kendileri tarafından bilgilerinin girilmiş olduğu sistemler (ÖSYM, YÖKSİS vb.) üzerinden elde edildiğini ifade etmektedirler. Bu nedenle kişilerin kendisi hakkında elde edilen verilere ilişkin bilgisi olduğu düşüncesi, doğrudan kişilerin kendisinden elde edilmeyen veriler için de geçerliliğini korumaktadır.

KDB katılımcılarından kişisel hak ve özgürlüklerin korunmasıyla ilişkili olarak, üniversite bilgi merkezlerinde danışma hizmetleri kapsamında elde edilen verilerin, veri sahibinin bilgisi dışında kişisel verilerle ilişkilendirilip ilişkilendirilmediğini belirtmeleri istenmiştir. Katılımcıların %86,7'si bilgi merkezlerinde danışma hizmetleri kapsamında tutulan bilgilerin kullanıcılarla ilişkilendirilmediğini ortaya koymaktadır. Ancak görüşme esnasında katılımcıların %53,6'sı bu uygulamanın kişisel verilerin korunması amacıyla değil, ihtiyaç duyulmaması nedeniyle yapıldığını ifade etmişlerdir. Bu katılımcılar farklı bir soruya vermiş oldukları yanıtta da, "Kullanıcının danışma hizmetleri kapsamında edindiği bilgilere ilişkin kayıtların" hassas ya da kişisel veri olarak korunması gerektiğini düşünmediklerini belirtmektedirler. Bu nedenle danışma hizmetleri kapsamında tutulan bilgilerin kullanıcılarla ilişkilendirilmediğini gösteren araştırma bulguları, bilgi güvenliğine ilişkin önlemler kapsamında bilinçli olarak yapılan bir uygulamanın sonucu olarak nitelendirilmemektedir.

Araştırma kapsamında PDB ve KDB katılımcılarına, kişisel verilerin elde edilmesinde dikkate alınan kriterler ve elde edilecek kişisel verilere nasıl karar verdikleri de sorulmuştur. PDB ve KDB tarafından toplanan kişisel bilgilerin dayandığı yasal düzenlemeler ve gerekçeler konusunda katılımcılardan çok farklı yanıtlar alınmıştır. Bu konuda KDB ile PDB'nin yaklaşımlarında da farklılıklar bulunmaktadır. KDB katılımcılarının %92,3'ü kişisel veriler elde edilirken "gerekli minimum bilginin" toplandığını belirtmektedirler. Ancak PDB katılımcılarının %69,2'si, bu konuda inisiyatif kullanmalarının mümkün olmadığını, toplanacak bilgilerin mevzuatta yer aldığını ve ihtiyaç duyulmayan bilgilerin de bu zorunluluk nedeniyle toplandığını ve personel dosyasında yer aldığını belirtmektedirler. PDB katılımcılarının kişisel verilerin toplanması konusunda dikkate aldıkları başlıca hukuksal düzenlemeler arasında; 4857 Sayılı İş Kanunu, 657 Sayılı Devlet Memurları Kanunu, 2547 Sayılı Yükseköğretim Kanunu ve 2914 Sayılı Yükseköğretim Personel Kanunu bulunmaktadır. Görüşme esnasında herhangi bir hukuksal düzenlemeyi dikkate almaksızın sadece ihtiyaç duyulan minimum bilgiyi topladıklarını belirten dört PDB katılımcısı, vakıf üniversitesi olmaları nedeniyle bu konuda inisiyatif kullanabildiklerini ifade etmişlerdir. Bir PDB katılımcısı tarafından görüşme esnasında, e-devlet projeleri kapsamında verilen yetkili şifrelerle de gereğinden fazla kişisel bilgiye erişimin mümkün olduğuna dikkat çekilmiştir.

4.2.2. Üniversitelerde Kişisel Verilerin Düzenlenmesi

Üniversitelerde verilerin sınıflandırılmasına ilişkin bilgiler Tablo 4'te yer almaktadır. Personel ya da kullanıcı kayıtları içeren belgelerin en yoğun olduğu PDB ve KDB birimlerinde bu kayıtların gizlilik derecelerine göre sınıflandırılıp sınıflandırılmadığı sorulmuş ve görüşme esnasında ayrıca uygulamanın gerekçeleri hakkında bilgi alınmıştır. Bu soruya ilişkin olarak İki PDB ve bir KDB görüş bildirmemiştir. Tablo 4'te belirtilen oranlar, sorulara yanıt veren katılımcılar üzerinden hesaplanmıştır.

Tablo 4 Üniversitelerde verilerin sınıflandırılmasına ilişkin politikalar

Personel kayıtları içeren belgeler gizlilik seviyesine göre sınıflandırılıyor mu?						
	PDB		KDB		Toplam	
	N	%	N	%	N	$\%_{Ort}$
Evet	9	69,2	3	21,4	12	44,4
Hayır	3	23,1	11	78,6	14	51,9
Kısmen	1	7,7	-	-	1	3,7
DD	2	-	1	-	3	-

Tablo 4'te yer alan verilere göre, PDB ve KDB açısından ayrı ayrı değerlendirildiğinde, bilgilerin gizlilik seviyelerine göre sınıflandırılması konusuna yaklaşımda farklılıkların olduğu görülmektedir. KDB katılımcılarının büyük bölümü (%78,6) kullanıcı kayıtlarının öğrenci ve personel bilgi sistemi üzerinden alındığı gerekçesiyle kendileri tarafından ayrıca sınıflandırma yapılmasına ihtiyaç duyulmadığını belirtmektedirler. PDB katılımcılarının ise %69,2'si tüm bilgilerin gizlilik seviyelerine göre sınıflandırıldığını ifade ederken, diğerleri bunun kısmen yapılabildiğini ya da henüz kullanmış oldukları sistemin tam olarak etkin hale gelmemesi nedeniyle ihmal edildiğini belirtmektedirler. Verilerin sınıflandırıldığını ifade eden PDB katılımcılarının uygulamalarındaki ortak nokta ise, özlük haklarına ilişkin bilgilerin sınıflandırılmasıdır. Verilerin sınıflandırılmasına ilişkin olarak, vakıf ve devlet üniversiteleri arasında işlem yoğunluğu ya da personel yetersizliği gibi nedenlere bağlı farklılıklar görülmemektedir.

4.2.3. Üniversitelerde Kişisel Verilerin Saklanması

Üniversite birimlerinde kişisel verilerin ne kadar süre saklandığı ve saklama koşulları için dikkate alınan yazılı politikaların olup olmadığı PDB ve KDB katılımcılarına sorulmuş ve elde edilen bulgular Tablo 5 üzerinde gösterilmiştir. Tablo 5 üzerinde ayrıca PDB katılımcılarından elde edilen üniversitelerde e-imza kullanımına ilişkin bilgilere de yer verilmiştir. Personel kayıtlarının saklanmasına ilişkin soruyu yanıtlamayan bir PDB katılımcısı ile e-imza kullanımına ilişkin soruyu yanıtlamayan iki PDB katılımcısı tablo üzerindeki hesaplamalarda dikkate alınmamıştır.

Tablo 5 Üniversitelerde verilerin saklanması ve güncellenmesine ilişkin politikalar

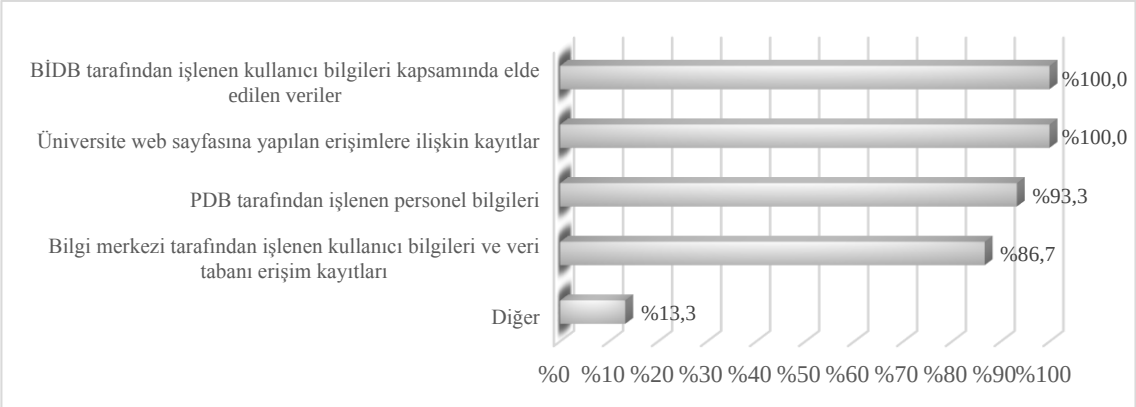
	Evet		Hayır		DD	
	N	%	N	%	N	%
Kullanıcı kayıtlarının ne kadar süre ile saklanacağı yazılı olarak belirlenmiş midir? (KDB)	4	26,7	11	73,3	-	-
Personel kayıtlarının ne kadar süre ile saklanacağı yazılı olarak belirlenmiş midir? (PDB)	12	85,7	2	14,3	1	-
Belge güvenliği için elektronik imza kullanılıyor mu? (PDB)	3	23,1	10	76,9	2	-

PDB ve KDB katılımcılarına yöneltilen kayıtların saklama sürelerine ilişkin sorulara verilen yanıtlarda büyük farklılık bulunmaktadır. PDB katılımcılarının %85,7'si kayıtların saklama sürelerinin belirlenmiş olduğunu ifade etmektedirler. KDB katılımcılarının yanıtlarında bu oranın %26,7 seviyesinde olduğu görülmektedir. PDB katılımcıları saklama sürelerine ilişkin olarak vermiş oldukları yanıtları arşiv hizmetlerine yönelik hukuksal düzenlemelere dayandırmaktadırlar. Bu nedenle PDB katılımcılarından verilerin saklanma sürelerine yönelik olarak 99, 100 ya da 101 yıl yanıtları alınmıştır. Ancak görüşme esnasında iki PDB katılımcısı, vakıf üniversitesi olarak bu konuda kendilerini sorumlu hissettikleri ya da takip ettikleri bir hukuksal düzenleme bulunmadığını belirtmişlerdir. KDB katılımcıları ise kullanıcı kayıtlarının saklanmasına ilişkin bir hukuksal dayanaklarının bulunmadığını belirtmektedirler. Bu nedenle, kayıtların ne kadar süreyle saklanacağının yazılı olarak belirlendiğini ifade eden dört KDB katılımcısı, bu sürenin kendileri tarafından belirlendiğini ifade etmişlerdir. Bu

sürelerin; personelin ilişik kestiği tarih, 1 yıl ya da 5 yıl olarak belirlendiği ifade edilmiştir.

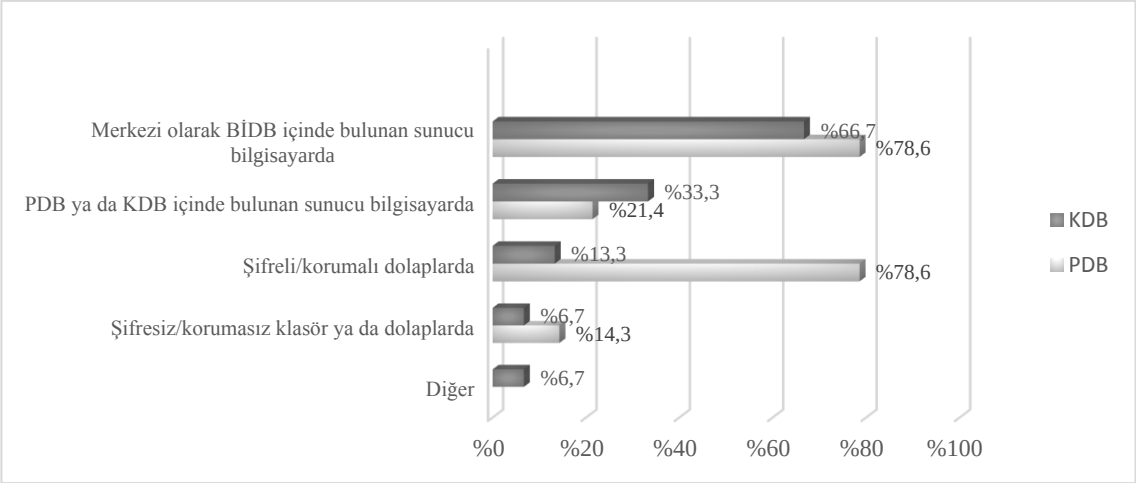
PDB katılımcılarına elektronik imza kullanım durumu sorulmuş ve sadece üç üniversitede (%23,1) elektronik imza kullanımının uygulandığı bilgisi alınmıştır. Katılımcılar bu üç üniversitede sertifika sürelerinin sınırsız olduğunu belirtmektedirler. Görüşme esnasında elektronik imzanın kullanıldığını ifade eden katılımcılar tarafından, konuya ilişkin hukuksal düzenlemeler ve hedeflenen güvenlik hakkında bilgilendirilmedikleri belirtilmiştir. Elektronik imza kullanan katılımcılar, üniversiteden ayrılan personelin daha önce imzalamış olduğu e-belgeler ile ilişkisinin ne olacağı ve imzanın arşiv formatında güncellenerek uzun süre korunması gereken dokümanların "arşiv imza" ile korunmasına yönelik bir uygulama planı bulunmadığını da ifade etmektedirler. Bu katılımcılardan biri, sistem erişim yetkilerinin birimler için de ayrıca tanımlandığını ve böylece üniversite ile ilişiği kesilen personelin yetkisiz erişim sağlamasının engellendiğini belirtmektedir.

Üniversitelerde kişisel verilerin hangi birimler tarafından saklandığını tespit edebilmek amacıyla, verileri merkezi olarak saklama sorumluluğu bulunan BİDB'ye hangi birimlerin verilerinin BİDB sunucularında saklandığı sorulmuş ve elde edilen bulgular Şekil 3 üzerinde gösterilmiştir. BİDB sunucularında saklanana bilgilere ilişkin soru tüm BİDB katılımcıları tarafından yanıtlanmıştır. PDB ve KDB katılımcılarına da verilerini hangi ortamlarda, nerede ve nasıl sakladıkları sorulmuş ve yanıtlar Şekil 4 üzerinde her iki daire başkanlığı için ayrı ayrı gösterilmiştir. KDB katılımcılarının tamamı soruyu cevaplandırırken, PDB katılımcılarından biri cevaplandırmamıştır. Bu soru ile üniversite birimleri arasındaki elektronik ya da yazılı-basılı belge kullanım ve saklama oranlarının da görülmesi sağlanmıştır. Katılımcıların Şekil 3 ve Şekil 4'te yer alan birim ve kayıtlara ilişkin birden fazla seçeneği işaretlemelerine olanak sağlanmıştır.



Şekil 3 BİDB sorumluluğundaki sunucularda merkezi olarak saklanan veriler

BİDB katılımcıları, Şekil 3'te yer alan birimlere ait verilerin üniversite BİDB sorumluluğundaki sunucularda tutulduğunu belirtmektedirler. Bunun yanı sıra iki BİDB katılımcısı (%13,3), bilimsel araştırma projeleri, patent çalışmaları ve kimlik paylaşım sistemi gibi önemli miktarda kişisel bilgi içeren dosyaların da merkezi olarak BİDB sorumluluğundaki sunucularda bulunduğuna dikkat çekmektedir. BİDB katılımcıları bu soruyu yanıtlarken, verilerin saklama sorumluluğu ile işleme ve paylaşımına ilişkin sorumlulukların çoğu zaman yanlış algılandığı ve üniversitedeki diğer birimlerin tüm sorumluluğun BİDB'de olduğunu düşündüklerini belirtmişlerdir.



Şekil 4 Personel ve kullanıcı kayıtlarının saklandığı ortamlar

Şekil 4 üzerinde yer alan verilerin elde edilmesi için PDB ve KDB katılımcılarına yöneltilen sorularda PDB katılımcılarına personel kayıtları, KDB katılımcılarına ise kullanıcı kayıtlarının saklanma koşulları sorulmuştur. Elde edilen bulgular, her iki daire

başkanlığının da birden fazla ortamda elektronik ve yazılı-basılı bilgilerin bulunduğunu göstermektedir. Araştırmanın konusunu oluşturan ve Şekil 4'te yer alan PDB ve KDB birimlerinde elektronik ortamda işlenen kişisel verilerin %72'sindan fazlası BİDB sorumluluğunda bulunan veri tabanlarında saklanmaktadır. Üç PDB katılımcısı (%21,4) ile beş KDB katılımcısı (%33,3), BİDB ile birlikte ya da sadece kendi birimleri içinde yer alan ve sorumluluklarının bulunduğu sunucular üzerinde verilerini sakladıklarını belirtmektedirler. PDB katılımcılarının %78,6'sı yazılı-basılı belgeleri şifreli ya da korumalı dolaplarda sakladıklarını belirtirken; KDB katılımcılarının şifreli ya da korumalı dolap kullanım oranı %13,3'ü geçmemektedir. KDB katılımcılarının yazılı-basılı belgeler için belirtmiş olduğu şifresiz ya da korumasız dolap kullanım oranının da (%14,3) düşük olması dikkat çekicidir. Görüşme esnasında KDB katılımcıları bilgi ve belgelerinin tamamen elektronik ortamda saklandığını ve bu nedenle diğer saklama ortamlarına yazılı-basılı belge için sınırlı olarak ihtiyaç duyduklarını belirtmişlerdir. PDB katılımcılarının merkezi olarak BİDB sorumluluğunda saklanan verilere ilişkin vermiş oldukları yanıt ile Şekil 3'te gösterilen BİDB'nin vermiş olduğu yanıtların tutarlı olduğu görülmektedir. Üç BİDB ile PDB katılımcısından kaynaklanan farklılığın biri soruya yanıt verilmemiş olması, diğer ikisi ise PDB katılımcılarının veri tabanı dışındaki kayıtları bu kapsamda değerlendirmemelerinden kaynaklanmaktadır. Şekil 3'te yer alan BİDB katılımcılarının yanıtları ile KDB katılımcılarının yanıtlarındaki farklılık ise, üç katılımcının kendileri tarafından kaydedilmemiş ve diğer sistemler üzerinden (öğrenci/personel bilgi sistemi vd.) almış oldukları kullanıcı bilgilerini, kendi verileri olarak değerlendirmemelerinden kaynaklanmaktadır. Elde edilen verilerin vakıf ve devlet üniversiteleri arasındaki dağılımına bakıldığında, verilerin güvenli ortamlarda saklanmasına ilişkin önlemlerin alınması konusunda vakıf ve devlet üniversiteleri arasında fark bulunmadığı görülmektedir.

Üniversitelerde personel verilerini doğrudan elde eden ve işleyen birimlerden biri olması nedeniyle, PDB katılımcılarına bu verileri hangi sıklıkta güncelledikleri de sorulmuştur. PDB katılımcılarının tamamı personel bilgilerinde değişme olduğunda bilgilerin güncellendiğini belirtirken, %85,7'si aynı zamanda ilişik kesme gibi işlemlerin yapılması esnasında da kayıtların güncellendiğini ya da gözden geçirildiğini belirtmişlerdir. Bununla beraber iki katılımcı, bilgilerin güncellenmesi için periyodik olarak personelden

talepte bulunulduğunu belirtmektedir. Ancak diğer katılımcılar personel sayısının çok fazla olması nedeniyle bu tür uygulamanın mümkün olamayacağını belirtmektedirler. Görüşme esnasında üç PDB katılımcısı personele ait kişisel bilgilere dışarıdan ya da üniversite içinden yetkisiz erişim yapılarak verilerin değiştirilebileceği endişesini taşıdıklarını ifade etmiştir. İç ve dış tehdit olarak algılanan bu unsurlar arasında yazılımları geliştiren firmalar ve üniversite BİDB personeli de bulunmaktadır. İki PDB katılımcısı ise bu konuda almış oldukları teknik önlemler ve yapılan her işlem için detaylı kayıt tutma yöntemleriyle bu riski en düşük seviyeye indirdiklerini ya da tamamen ortadan kaldırdıklarını ifade etmektedir.

4.3. KİŞİSEL VERİLERİN KULLANIMI VE PAYLAŞIMI

Üniversitelerde kişisel verilerin hangi koşullarda paylaşıldığı PDB ve KDB katılımcılarına sorulmuş ve katılımcıların bu konudaki görüşleri Tablo 6 üzerinde gösterilmiştir. Tablo 6 üzerinde yer alan verilerin elde edilmesi için PDB ve KDB katılımcılarına yöneltilen sorularda PDB katılımcılarına personel kayıtları, KDB katılımcılarına ise kullanıcı kayıtlarının paylaşım koşulları sorulmuştur. PDB ve KDB katılımcıları arasındaki görüş farklılığının da görülebilmesi amacıyla, Tablo 6 üzerinde bu iki daire başkanlığından elde edilen veriler ayrı ayrı gösterilmiştir. Bu soruya iki PDB katılımcısından yanıt alınamamıştır. Şekil 4'te belirtilen oranlar, sorulara yanıt veren katılımcılar üzerinden hesaplanmıştır. Katılımcıların Tablo 6'de yer alan tercihlere ilişkin birden fazla seçeneği işaretlemelerine olanak sağlanmıştır.

Tablo 6 Üniversitelerde personel ve kullanıcı kayıtlarının paylaşımı

Personele ya da kullanıcılara ait kayıtların hangi gerekçe ile paylaşımına izin verilmektedir?	PDB		KDB	
	N	%	N	%
Yasal çerçevede savcılık tarafından istenmesi durumunda	10	76,9	9	60
Bilgi Edinme Hakkı Kanunu çerçevesinde	10	76,9	3	20
İstatistiksel amaçlı olarak istenmesi halinde	-	-	-	-
Bilimsel araştırmada kullanılmak şartıyla	-	-	-	-
Üniversite üst yönetimi tarafından istenmesi halinde	8	61,5	13	86,7
Kamu menfaati için kişisel haklar gözetilmeksizin	-	-	1	6,7
Veri sahibinin kendisi hakkında tutulan bilgileri istemesi halinde	9	69,2	11	73,3
Personel/Kullanıcı bilgileri hangi sebeple olursa olsun verilmez.	-	-	-	-
DD	2	-	-	-

Tablo 6 üzerinde yer alan veriler dikkate alındığında, PDB ve KDB tarafından elde edilen kişisel bilgilerin paylaşımı konusunda tüm katılımcıların duyarlı olduğu görülmektedir. Katılımcılar, bu bilgilerin istatistiksel amaçlı, araştırmalarda kullanılması amacıyla ya da kişisel haklar gözetilmeksizin kamu menfaati için bilgilerin paylaşılmasını kesinlikle doğru bulmamaktadırlar. Bu sorulara verilen yanıtlardaki dağılım ise, üniversitelerin uygulamalarından kaynaklanan farklılıkları yansıtmaktadır. Örneğin bazı üniversitelerde birimlerin savcılığa doğrudan bilgi vermesi sürecin işleyişine uygun olarak kabul edilirken, bazı üniversitelerde bunun ancak üniversite üst yönetiminin (ya da idari amir) onayı ya da aracılığıyla mümkün olabileceği görüşü benimsenmektedir. Ancak görüşme esnasında elde edilen verilere göre, üst yönetimin ya da idari amirin onayını alma eğiliminin üniversite yapılanması (devlet ya da vakıf) ya da üst yönetimin bu yöndeki tutumu ile ilişkisi bulunmamaktadır. PDB ve KDB katılımcıların bilgilerin savcılık ile paylaşımı konusundaki tutumlarını yansıtan oranlar arasında da (sırasıyla N=10, %76,9 ve N=9, %60) önemli fark bulunmamaktadır. Tablo 6 üzerinde KDB katılımcılarının Bilgi Edinme Hakkı Kanunu çerçevesinde bilgi paylaşımına ilişkin oranının düşük (%20) olması dikkat çekicidir. Görüşme esnasında bu seçeneği işaretlemeyen KDB katılımcıları bu kapsamda kendilerinden istenebilecek verilerin bulunmadığı ve daha önce böyle bir taleple karşılaşmadıklarını ifade etmişlerdir.

PDB ve KDB katılımcılarına, kişisel bilgilerin paylaşılması durumunda veri sahibine bilgi verip vermemeleri konusundaki düşünceleri de sorulmuştur. PDB katılımcılarının

%91,7'si ile KDB katılımcılarının %80'i kişisel bilgilerin paylaşılması durumunda veri sahibine bilgi verilmeyeceğini ya da kısmen bilgi verileceğini belirtmektedir. Ancak görüşme esnasında bunun nedeni olarak, savcılık ya da üniversite üst yönetimi tarafından istenen bilgilerin genellikle soruşturma kapsamında ve gizlilik içerisinde yürütülüyor olması gerekçe gösterilmiştir. Katılımcıların bu konuda göstermiş oldukları sorumluluk almama eğilimi ile meydana gelen olayları öncelikle idari amirlerine yönlendirme ya da idari amirlerle paylaşma eğilimleri arasında doğrusal ilişki bulunmaktadır.

PDB ve KDB katılımcılarına ayrıca, elde edilen kişisel bilgilerin amaç dışı kullanılmayacağı, izinsiz olarak paylaşılmayacağı ve bu verilerin korunacağına ilişkin olarak veri sahibine yazılı taahhütte bulunup bulunmadıkları sorulmuştur. Bu soruyu yanıtlayan PDB katılımcılarının tamamı (N=13) ile KDB katılımcılarının %93,3'ü kişisel bilgilerin elde edilmesi sürecinde veri sahibine herhangi bir taahhütte bulunmadıklarını belirtmektedirler. Görüşme esnasında PDB katılımcıları bireysel hakların korunmasının bu açıdan ikinci planda kaldığını ifade ederken, bu konuda zorunluluklarının olmadığının da altını çizmektedirler. KDB katılımcıları ise ağırlıklı olarak bilgileri mevcut sistemler (personel ve öğrenci bilgi sistemleri gibi) üzerinden alıyor olmaları nedeniyle, bu konuda sorumluluklarının bulunmadığını düşünmektedirler.

4.4. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN BİLGİ GÜVENLİĞİ ÖNLEMLERİ

Tablo 7 üzerinde üniversitelerde alınan bilgi güvenliği önlemlerinin gizliliğin ve kişisel hakların korunmasındaki etkinliği, bilgi varlıklarının korunması amacıyla uygulanan yöntemler, alınan teknik ve idari önlemler ve güvenlik denetimine yönelik uygulamalara ilişkin bulgular yer almaktadır. Tablo 7 üzerinde yer alan soruların tamamı BİDB katılımcılarına yöneltilmiş ve tüm katılımcılardan (N=15) yanıt alınmıştır.

Tablo 7 Bilgi güvenliği önlemlerinin etkinliği ve güvenlik denetimleri

	Evet		Hayır		Kısmen	
	N	%	N	%	N	%
Bilgi güvenliği amacıyla "kriptolama" yöntemi kullanılıyor mu?	5	33,3	10	66,7	-	-
Kişisel verilerin bütünlüğü için "hash" değeri hesaplanıyor mu?	5	33,3	10	66,7	-	-
Alınan bilgi güvenliği önlemleri verinin gizliliğini koruyor mu?	14	93,3	1	6,7	-	-
Alınan bilgi güvenliği önlemleri bireylerin kişisel hak ve özgürlüğünü koruyor mu?	14	93,3	1	6,7	-	-
Kişisel verilerin işlendiği ya da depolandığı bilgisayarların oturum açma kayıtları tutuluyor mu?	12	80,0	2	13,3	1	6,7
Üzerinde kişisel bilgi bulunan bilgisayarlar uygun etiketlendirme ve ikaz notları ile işaretleniyor mu?	1	6,7	14	93,3	-	-
Üzerinde kişisel bilgi bulunan bilgisayarların güvenlik denetimleri yapılıyor mu?	7	46,7	8	53,3	-	-

Bilgi bütünlüğünün sağlanmasına ilişkin etkin yöntemler olarak bilinen kriptolama ve hash değeri hesaplama yöntemleriyle ilgili soruları yanıtlayan BİDB katılımcılarının %66,7'si, bu yöntemleri kullanmadıklarını ifade etmektedirler. Bu yöntemlerin kullanıldığını belirten üç BİDB katılımcısı ise, veri tabanı sistemlerinin kendi içinde var olan kriptolama ve hash hesaplama işlemlerini düşünerek bu sorulara yanıt verdiklerini belirtmektedirler. Ancak kişisel verilerin işlendiği birimlerdeki bilgisayarlar üzerinde bulunan diğer dosyalar ile BİDB sorumluluğundaki dosya sunumcuları üzerindeki dosyalar için bu tür işlemler yapılmamaktadır. Bununla beraber, görüşme esnasında katılımcıların hemen hemen tamamı üniversite birimlerinden bu tür taleplerin gelmesi ve verilerin ilgili birimler tarafından sınıflandırılması halinde bu yöntemlerin kullanılmasının teknik açıdan mümkün olabileceğini belirtmişlerdir.

BİDB katılımcılarının ikisi haricinde tümü kişisel verilerin işlendiği bilgisayarlarda oturum açma kayıtlarının tutulduğunu belirtmektedirler. Ancak bu kayıtlar özellikle çok sayıda bilgisayar bulunan üniversitelerde istenildiğinde incelenebilir durumda ve merkezi olarak tutulmamaktadır. Kullanıcılar üzerinde bilgi güvenliği farkındalığını arttırmaya yönelik uyarı ve ikaz notlarının kullanımının ise sadece bir üniversitede uygulandığı görülmektedir. Dört katılımcı, domain yapısının bulunmadığı, çok fazla sayıda bilgisayarın bulunduğu ve kullanılan sistemlerdeki çeşitliliğin fazla olduğu üniversitelerde bunun uygulanamayacağı görüşünü savunmaktadırlar. Bu kısıtlamaların kişisel verilerin işlendiği bilgisayarların denetimi konusunda da engel teşkil ettiği

görülmektedir. Katılımcıların yarısı (%46,7) kişisel verilerin bulunduğu bilgisayarların denetimin yapıldığını ifade ederken, bu denetimlerin yalnızca merkezi olarak bilgilerin bulunduğu sunucu bilgisayarların üzerinde ve çoğunlukla düzensiz aralıklarla sistem yöneticileri tarafından yapıldığı belirtilmektedir.

BİDB katılımcılarına kişisel verilerin korunmasına yönelik ne tür teknik ve idari önlemler alındığını belirtmeleri istenmiştir. Bu soruyu yanıtlayan tüm katılımcılar (N=15), üniversitelerde bilgi güvenliğinin sağlanması konusunda alınabilecek temel teknik önlemlerin (IDS/IPS, firewall, antivirüs, erişim yetkilendirmeleri) BİDB tarafından alındığı yanıtını vermişlerdir. Buna ilave olarak, iki üniversitede kalite yönetim sistemi standartları ve kullanıcı eğitimleri ile alınan teknik önlemlerin desteklendiği ifade edilmiştir. Ancak idari önemlere ilişkin herhangi bir uygulamadan bahsedilmemiştir. BİDB katılımcılarının %93,3'ü, alınan bilgi güvenliği önlemlerinin verinin gizliliğini ve bireylerin kişisel hak ve özgürlüğünü koruduğunu düşünmektedirler. Ancak altı katılımcı bireylerin kişisel hak ve özgürlüğünün korunmasına ilişkin soruyu yanıtlarken, kişisel hak ve özgürlüklere ilişkin yeterli bilgiye sahip olmadıklarını da ifade etmiştir.

4.5. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ÖNLEMLERİN STANDARTLAR VE YASALARA UYUMLULUĞU

Tablo 8 üzerinde üniversitelerde bilgi güvenliğini sağlamaya yönelik sistem güvenlik testleri ve kişisel verilerin kullanımı, bilgi varlıklarının korunmasına yönelik önlemlerin hukuksal düzenlemelere uyumluluğuna ilişkin bulgular yer almaktadır. Tablo 8 üzerinde yer alan sorular BİDB katılımcılarına yöneltilmiş ve tüm katılımcılardan (N=15) yanıt alınmıştır.

Tablo 8 Bilgi güvenliğini sağlamaya yönelik standartlar ve etik kurallar

	Evet		Hayır	
	N	%	N	%
Sistem güvenlik testleri yapılıyor mu?	10	66,7	5	33,3
Sistem güvenlik testleri yapılırken veri tabanında bulunan kişisel ve hassas veriler de kullanılıyor mu?	2	13,3	13	86,7
Bilgi varlıklarının hangi yasal düzenlemeler kapsamında korunduğu açık olarak belirtiliyor mu?	3	20,0	12	80,0

Üniversitelerin %66,7'sinde BİDB sorumluluğunda bulunan bilgi sistemleri ve veri tabanlarının güvenlik denetimleri yapılmaktadır. BİDB katılımcıları bu güvenlik denetimlerinin sistemi tasarlayan ya da yöneten personel tarafından ve ağırlıklı olarak erişim yetkilendirmelerine ilişkin olarak yapıldığını belirtmektedirler. Görüşme esnasında ayrıca bu testlerin planlı ve düzenli olarak yapılmadığı, genellikle sistem ya da konfigürasyon değişikliklerine bağlı olarak yapıldığı bilgisi alınmıştır.

BİDB katılımcılarına saklama sorumlulukları bulunan veri tabanları üzerinde, sistem güvenlik testleri ve diğer işlemlerin yapılması esnasında kişisel verilerin kullanılıp kullanılmadığı sorulmuştur. Bu soru ile kişisel verilerin risk durumuna ilişkin bilgi alınması hedeflenmiştir. Katılımcıların %86,7'si veri tabanları üzerinde bulunan kişisel verilerin test sürecinde kullanılmadığını ifade ederken, iki katılımcı veri tabanları üzerinde herhangi bir veri sınıflandırması yapılmamış olması nedeniyle bu süreç içerisinde tüm verilerin yer aldığını ifade etmiştir. Veri tabanları üzerinde yapılan işlemlerde kişisel verilerin kullanılmadığını ifade eden 13 katılımcının 10'u, personel ve öğrenci bilgileri gibi kişisel verilerin bulunduğu veri tabanlarının diğer veri tabanlarından farklı ortam ya da sanal ağlarda bulunduğunun da altını çizmişlerdir.

Bilgi varlıklarının korunmasına yönelik olarak alınan güvenlik önlemlerinin hangi yasal düzenlemeler kapsamında alındığının açık olarak belirtilip belirtilmediği sorusuna, üniversite BİDB katılımcılarının %80'i "Hayır" yanıtını vermiştir. Bu soruda "Evet" yanıtını işaretleyen iki katılımcı, alınan güvenlik önlemlerinin belirtildiği belgelere ilişkin olarak; bilgi varlıklarının korunması açısından yeterli içeriğe sahip olmayan "Bilişim Kaynakları Kullanım Yönergesi" ya da gizliliğin ihlali sonrasında uygulanacak belgeleri adres göstermişlerdir.

Hukuksal düzenlemelerin yanı sıra PDB ve KDB katılımcılarına üniversite birimlerinde dikkate alınan mesleki etik ilkeler ve uluslararası standartların olup olmadığı sorulmuştur. PDB katılımcılarının %30,8'i, KDB katılımcılarının ise %40'ı dikkate aldıkları mesleki etik ilkeler ve standartların bulunduğunu belirtmişlerdir. Bu soruya "Evet" yanıtını veren KDB katılımcıları "Türk Kütüphanecileri Derneği (TKD) Mesleki Etik İlkeleri"ni dikkate

aldıklarını belirtirken; PDB katılımcıları resmi yazışmalarda uyulacak yazışma usul ve esasları ile yazılı olmayan temel etik normların uygulandığını belirtmektedirler. PDB ve KDB katılımcı gruplarının mesleki etik ilkelerin uygulanmasına yönelik görüşleri ile üniversitenin yapısı (vakıf ya da devlet üniversitesi) arasında ilişkili bulunmamaktadır.

4.6. KİŞİSEL VERİLERİN DEPOLANMASI VE KORUNMASINA İLİŞKİN SORUMLULUKLAR

Tablo 9 üzerinde üniversitelerde kişisel verilerin korunmasına ilişkin sorumlulukların paylaşılması, bilgi güvenliğinin sağlanması konusunda personel görevlendirmeleri, üniversite üst yönetiminin bilgi güvenliğinin sağlanması konusundaki hassasiyeti, kişisel verilerin merkezi veri depolama ortamları üzerinde sınıflandırılması ve ayrılmasına ilişkin bulgular yer almaktadır. Tablo 9 üzerinde yer alan sorular BİDB katılımcılarına yöneltilmiş ve tüm katılımcılardan (N=15) yanıt alınmıştır.

Tablo 9 Üniversitelerde kişisel verilerin korunmasına ilişkin sorumlulukların paylaşılması

	Evet		Hayır		Kısmen		Fikrim Yok	
	N	%	N	%	N	%	N	%
Bilgi güvenliği konusunda özel olarak görevlendirilmiş personel bulunuyor mu?	6	40,0	9	60,0	-	-	-	-
Üst yönetim kademelerinde bilgi güvenliğinin sağlanması konusuna önem verildiğini düşünüyor musunuz?	11	73,3	3	20,0	-	-	1	6,7
Bilgi güvenliği sorumluluğu üniversitenin tüm birimleri tarafından paylaşılıyor mu?	7	46,7	7	46,7	-	-	1	6,7
Üniversite personelinin görev tanımında kişisel bilgilerin korunmasına ilişkin sorumluluklar açık olarak belirtiliyor mu?	3	20	11	73,3	-	-	1	6,7
Üniversitede birimlerinin "bilişim sorumluları" yazılı olarak belirlenmiş mi?	5	33,3	10	66,7	-	-	-	-
Üniversitedeki bilişim faaliyetlerinin düzenlenmesi amacıyla kurulan bir "bilişim komisyonu" bulunuyor mu?	6	40,0	9	60,0	-	-	-	-
Kişisel veriler sınıflandırılarak diğer verilerden ayrı fiziksel ortamlarda saklanıyor mu?	6	40,0	9	60,0	-	-	-	-
Kişisel verilerin bulunduğu bilgisayarların farklı sanal ağlar üzerinde bulunması sağlanıyor mu?	10	66,7	5	33,3	-	-	-	-
Bilgi güvenliğinin sağlanmasına yönelik donanımsal gereksinimler yönetim tarafından ivedilikle karşılanıyor mu?	11	73,3	2	13,3	2	13,3	-	-

Üniversite BİDB'lerin %60'ında bilgi güvenliğinin sağlanması ve denetimine yönelik olarak görevlendirilmiş personel bulunmamaktadır. Bununla beraber, bilgi güvenliğinin sağlanması amacıyla bir personelin görevlendirildiğini belirten altı BİDB katılımcısının beşi, bu görevi yürüten personelin asıl ve öncelikli sorumluluğunun farklı olduğunu belirtmiştir. Buna bağlı olarak, bu görevi yürütme sorumluluğu verilen personelin de asıl uzmanlık alanının farklı olduğu bilgisi alınmıştır. Sadece bir üniversitede BİDB içerisinde ayrı bir bilgi güvenliği birimi oluşturulmuş ve özel olarak bu göreve personel atanmıştır. Bir üniversitede ise bu konuya önem verdikleri ve kadro çalışmalarının başlatıldığı ifade edilmiştir. Görüşme esnasında özellikle vakıf üniversitelerinin personelden daha etkin faydalanabilmek amacıyla görev birleştirme ve bazı görevleri ek görev olarak mevcut personele paylaştırma yöntemlerini daha fazla benimsedikleri görülmüştür.

BİDB katılımcılarının %73,3'ü, üniversite üst yönetiminin bilgi güvenliğinin sağlanması konusuna önem verdiklerini düşünmekte ve bilgi güvenliğinin sağlanmasına yönelik donanımsal gereksinimlerin ivedilikle karşılandığını belirtmektedirler. Ancak üniversitelerin yarısında (%46,7) bilgi güvenliği sorumluluklarının birimler arasında paylaşılmadığı, %60'ında bilişim faaliyetlerini düzenleyen bir bilişim komisyonunun olmadığı ya da komisyonlarda kişisel verilerin korunmasına ilişkin gündem maddelerinin yer almadığı ve ayrıca üniversitelerin %66,7'sinde birimlerde bilişim sorumlularının belirlenmediği görülmektedir. Bununla beraber, üniversitelerin %73,3'ünde kişisel verilerin yoğun olarak işlendiği birimlerde ya da bu verilerin saklanmasından sorumlu BİDB'de çalışan personelin görev tanım formlarında bu konuya ilişkin sorumlulukların belirtilmediği görülmektedir.

Kişisel verilerin korunmasına yönelik birtakım teknik önlemlerin alınması konusunda PDB ve KDB katılımcılarından da sorumluluklarının olup olmadığını belirtmeleri istenmiştir. PDB katılımcılarının %38,5'i ile ve KDB katılımcılarının %46,7'si bu konuda sorumluluklarının bulunduğunu düşünmektedirler. KDB katılımcılarının PDB katılımcılarına oranla daha fazla teknik önlem alma sorumluluklarının olduğunu düşünmeleri, birim içinde daha fazla merkezi bilgi sistemlerinin bulunmasından kaynaklanmaktadır. Bu sonuçlar ile verilerin merkezi olarak PDB ya da KDB içinde saklanma oranları arasında doğrusal ilişki bulunmaktadır. Teknik önlemlerin alınmasına ilişkin sorumlulukların bazıları; kişisel verilerin işlendiği bilgisayarlar üzerindeki güvenlik yazılımlarının güncelliğinin korunması için BİDB ile koordinasyonun sağlanması, bilgi merkezlerindeki kullanıcı erişim kayıtlarının temizlenmesi, sistem erişim yetkilendirmelerinin güncellenmesi ve PDB ya da KDB içinde bulunan sunucuların güvenliğinin sağlanması olarak ifade edilmiştir. Teknik sorumlulukların yerine getirilmesi kapsamında KDB katılımcılarının %53,3'ü, bilgi merkezlerinde kullanıcıların araştırma ya da katalog tarama amacıyla kullanmış oldukları bilgisayarların kayıtlarının düzenli olarak temizlendiğini ifade etmektedirler.

Üniversitelerin %60'ında BİDB sorumluluğunda bulunan sunucular üzerindeki merkezi veri depolama alanları aynı fiziksel ortamda bulunmaktadır. Ayrı fiziksel ortamların sağlanamaması halinde de bilgi güvenliği açısından açıklarının büyük ölçüde

kapatılmasını sağlayan farklı sanal ağların kullanımı ise üniversitelerin %66,7'sinde sağlanmaktadır. 10 BİDB katılımcısı sanal ağların kullanılmasının bilgi güvenliğinin sağlanması için çok önemli olduğu, fazladan maddi yük getirmediği ve her üniversitede uygulanabileceği konusunda görüş bildirirken, sadece bir BİDB katılımcısı bu güvenlik önlemlerinin kullanılabilirliği olumsuz etkileyeceğini düşünmektedir. Sanal ağların kullanımı açısından devlet ve vakıf üniversiteleri arasında fark bulunmamaktadır.

PDB ve KDB katılımcılarına olası ihlaller karşısında uygulanacak yaptırımların belirlenip belirlenmediği ve ne tür yaptırımların uygulanmasının öngörüldüğü sorulmuştur. Bu konuya ilişkin olarak PDB ve KDB birimlerinin hazırlık düzeylerinin farklı olduğu görülmektedir. PDB katılımcılarının %53,8'i, KDB katılımcılarının ise %26,7'si uygulanacak yaptırımların belirlenmiş olduğunu ifade etmektedir. Yaptırımların belirlenmiş olduğunu ifade eden PDB ve KDB katılımcıları, yazılı ya da sözlü uyarı, disiplin soruşturmaları ve cezaları, idari para cezası, işten uzaklaştırma ve kanunlar çerçevesinde öngörülen diğer yaptırımların uygulanabileceğini belirtmektedirler. Bununla birlikte katılımcıların tamamı görüşme esnasında henüz böyle bir durumla karşılaşmadıklarını ifade etmişlerdir.

BİDB katılımcılarına kaydedilen kişisel verilerin sorumluluğunun üniversite birimleri arasında nasıl paylaşıldığı sorulmuş ve soruyu yanıtlayan 14 katılımcıdan dört farklı yanıt alınmıştır. Sadece üç üniversitede birimlerin sorumluluklarının ve yetkilendirme koşullarının "yazılı" olarak belirlenmiş olması dikkat çekicidir. Sekiz BİDB katılımcısı kısmen ya da tamamen BİDB'nin bu verilerin korunması konusunda sorumlu olduğunu düşünmektedir. Üç katılımcı ise birimler arasında sorumlulukların paylaşılmadığını ifade etmelerine karşın BİDB olarak verilerin sadece saklanması konusunda sorumluluğunun olduğunu belirtmektedir. Elde edilen bulgular birleştirildiğinde, her ne kadar üniversitelerin %78,6'sında belirgin bir sorumluluk paylaşımı yapılmamış olsa da, tüm BİDB katılımcıları merkezi sunucular üzerinde bulunan verilerin saklanması ve korunması konusunda sorumluluklarının bulunduğunu düşünmektedirler. Ayrıca dokuz BİDB katılımcısı sorumluluk paylaşımına ilişkin sorunların tek çözüm adresi olarak BİDB'nin gösterildiğini ifade etmişlerdir.

BİDB katılımcılarına merkezi olarak saklama sorumlulukları bulunan kişisel verilerin hangi sıklıkta yedeklendiği sorulmuştur. Bu soruya tüm katılımcılar (N=15) günlük olarak yedekleme yapıldığı yanıtını vermiştir. Bunun yanı sıra bir katılımcı bilgi merkezi kayıtları gibi anlık değişen verilerin saatlik olarak da yedeklendiğini belirtmiştir. Ayrıca görüşme esnasında katılımcıların %86,7'si, veri yedekleme işleminin en önemli BİDB faaliyetleri arasında olduğunu ve bunun için gerekli donanım maliyetinden kaçınılmadığını ifade etmişlerdir.

4.7. RİSK FAKTÖRLERİ, RİSK YÖNETİMİ VE ALTERNATİF PLANLAR

Tablo 10 üzerinde üniversitelerde bilgi varlıklarının değerlendirilmesi, risk yönetimi, yazılı eylem planları, üniversite dışından teknik destek alma durumu ve veri tabanlarına yönelik saldırı girişimlerine ilişkin bulgular yer almaktadır. Tablo 10 üzerinde yer alan tüm sorular BİDB katılımcılarına yöneltilmiştir. Kişisel verilerin bulunduğu veri tabanlarına yönelik saldırı girişimlerine ilişkin soru bir katılımcı tarafından yanıtlanmazken, diğer sorular tüm katılımcılar (N=15) tarafından yanıtlanmıştır.

Tablo 10 Üniversitelerde bilgi varlıklarının değerlendirilmesi ve risk yönetimi

	Evet		Hayır		Kısmen	
	N	%	N	%	N	%
Bilgi Sistemlerinin bakım/onarımı için dışarıdan destek alınıyor mu?	9	60,0	6	40,0	-	-
Dışarıdan destek veren şirket çalışanları için güvenlik araştırması yapılıyor mu?	10	66,7	3	20,0	2	13,0
Üniversitede yapılmış bir bilgi varlığı değerlendirmesi ve risk analizi raporu bulunuyor mu?	6	40,0	9	60,0	-	-
Herhangi bir veri ihlali olması durumunda uygulanabilecek bir yazılı eylem planınız var mı?	2	13,3	13	86,7	-	-
Kişisel verilerin bulunduğu veri tabanlarına yönelik saldırı girişimleri oluyor mu?	9	64,3	5	35,7	-	-

Üniversite BİDB katılımcılarının %60'ı dışarıdan teknik destek aldıklarını belirtmektedir. Üniversitenin büyüklüğü, desteklenen bilgisayar sayısı ve BİDB'de çalışan personel sayısı ile dışarıdan destek alma oranını arasında doğrusal ilişki bulunmaktadır. Bazı katılımcılar sadece merkezi sistemler için ve mutlaka bir personel gözetiminde destek aldıklarını vurgularken; bazı katılımcılar sözleşme çerçevesinde üniversite birimlerinin

de doğrudan iletişim kurarak ilgili şirketlerden destek alabildiklerini belirtmektedirler. İki katılımcı, dışarıdan destek sağlanan firmanın doğrudan birimlere yönlendirilmesi halinde, kullanıcının kişisel verilerini koruma sorumluluğu bulunduğu ve bunun için de farkındalığın arttırılması gerektiğini ifade etmektedir. Üç katılımcı haricindeki tüm BİDB katılımcıları, dışarıdan her türlü faaliyet kapsamında destek alınan şirket çalışanları için kısmen de olsa güvenlik araştırması yapıldığını ifade etmektedir. İki BİDB katılımcısı kısmen yapılan güvenlik araştırmalarında ilgili şirket ve çalışanlarının önceki iş referans ve kayıtlarının değerlendirildiğini belirtmişlerdir. Katılımcılar bu kapsamda genel olarak şirket çalışanlarından adli sicil kaydı ve sahip oldukları çalışma referansları gibi belgelerin istenildiğini belirtmektedirler. Güvenlik araştırmasının yapılıp yapılmadığına ilişkin soruya "Hayır" yanıtını veren katılımcılar ise, dışarıdan hiçbir koşulda destek almadıklarını ve soruyu bu kapsamda yanıtladıklarını belirtmektedirler.

Üniversitelerin %60'ında bilgi varlıklarının değerlendirmesinin yapılmadığı ve bir risk analizi raporunun oluşturulmadığı görülmektedir. Bununla bağlantılı olarak BİDB katılımcılarına herhangi bir veri ihlali olması durumunda uygulanabilecek yazılı eylem planının olup olmadığı sorulmuş ve sadece iki üniversitede (%13,3) yazılı eylem planının hazırlanmış olduğu yanıtı alınmıştır. Bu tür eylem planlarının hazırlanmamış olmasının, veri ihlallerinin ya da veri tabanlarına yönelik saldırı girişimleriyle de ilişkisi bulunmamaktadır. Zira BİDB katılımcılarının %64,3'ü veri tabanlarına yönelik olarak her hafta saldırı girişimlerinin olduğunu ifade etmektedirler. Üniversite birimlerindeki bilgisayarların dışarıdan yapılabilecek saldırılara karşı risk durumunu da değerlendirebilmek amacıyla PDB ve KDB katılımcılarına kişisel verilerin de işlendiği bilgisayarların internet bağlantı durumu sorulmuştur. Katılımcıların %93,1'inden PDB ve KDB'de kullanılan tüm bilgisayarların internete bağlı olarak çalıştığı yanıtı alınmıştır. Bu durumda üniversitelerde bilgi güvenliği açısından risk alanlarının geniş olduğu söylenebilir.

BİDB katılımcılarına görüşme esnasında risk analizine yönelik olarak ISO 27001 gibi uluslararası standartların nasıl katkı sağlayabileceği de sorulmuştur. Katılımcıların hemen hemen tamamı (%86,6), bu tür standartların üniversitelerde tam olarak uygulanabilmesinin mümkün olmadığını ve bu nedenle satın alınması halinde sertifika

süreci tamamlanamayacağı için hedefe ulaşılamayacağını ifade etmektedirler. BİDB katılımcıları üniversitelerin özellikle denetim sürecinde tüm birimlerde istenilen şartları tam olarak yerine getirmelerinin çoğu zaman mümkün olamayacağını belirtmektedirler. Katılımcılar, bu standartların içeriğinin üniversitelerin hukuksal ve idari sorumlulukları ile de tam olarak örtüşmediğini düşünmektedirler. Ancak katılımcıların tamamı, bu standartlarının içeriğinin bilinmesi ve uygulanabilir olanların üniversitenin kendi belirlemiş olduğu güvenlik politikaları çerçevesinde uygulanmasının önemli bir kazanım olacağı noktasında birleşmektedirler. Personel yetersizliği, kuruluş sürecinin tamamlanmamış olması ve hukuksal düzenlemelere uyum çalışmaları gibi diğer öncelikli yükümlülüklerin yerine getirilmesi için gereken işlemlerin tamamlanmamış olması nedeniyle; dokuz katılımcı henüz güvenlik standartlarını detaylı olarak inceleme ve uygulama imkânlarının olmadığını ifade etmiştir. Altı katılımcı ise bu standartları en azından sistemlere yönelik güvenlik önlemlerini uygularken gözden geçirdiklerini ifade etmiştir.

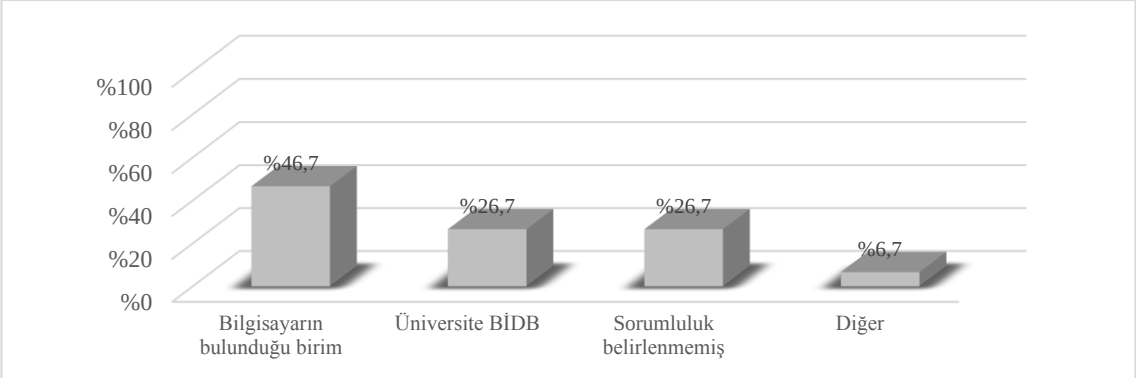
BİDB katılımcılarına herhangi bir felaket durumunda sistemin ne kadar süre içinde yeniden aktif hale getirilebileceği de sorulmuştur. BİDB katılımcıları günlük olarak almış oldukları tüm verilerin ve sistemlerin yedeklerini herhangi bir felaket durumunda yine aynı gün içerisinde geri yükleyerek sistemin yeniden aktif hale getirilebileceğini belirtmektedirler. Üç üniversitede verilerin sınıflandırılmasına bağlı olarak bu işlem süresinin 10 dakika ile 4 saat aralığına kadar düşürülebileceği ifade edilmiştir.

4.8. KİŞİSEL VERİLERİN İMHA EDİLMESİ VE SİSTEM KAYITLARININ TEMİZLENMESİ

Üniversitelerde kişisel verilerin imha sürecine ilişkin politikalar ve bu kapsamda değerlendirilecek üniversite birimlerindeki imha işlemlerine ilişkin sorumluluklara yönelik soruların BİDB katılımcıları tarafından yanıtlanması istenmiştir. BİDB katılımcılarının %93,3'ü (N=14) verilerin imha sürecine ilişkin olarak belirlenmiş ve uygulanan bir politika bulunmadığını belirtirken, bir katılımcı da bu konuda fikrinin olmadığını ifade etmektedir. Görüşme esnasında BİDB katılımcılarının büyük çoğunluğu bu konudaki eksikliklerinin farkında olduklarını ancak henüz bir çalışmalarının

bulunmadığını ifade etmişlerdir. Dört katılımcı bu konunun özel bilgi ve uzmanlık gerektirdiğini ve bu nedenle uzman personele ihtiyaç duyulduğunu da vurgulamıştır. Ayrıca üniversite birimlerinden başlayarak, tüm üniversitede farkındalığın oluşturulması ile sürecin sağlıklı olarak işleyeceğine inanmaktadırlar. Sadece bir üniversitede bilgi güvenliğinden sorumlu birim tarafından veri imha işlemlerine ilişkin bir taslak oluşturulduğu bilgisi alınmıştır.

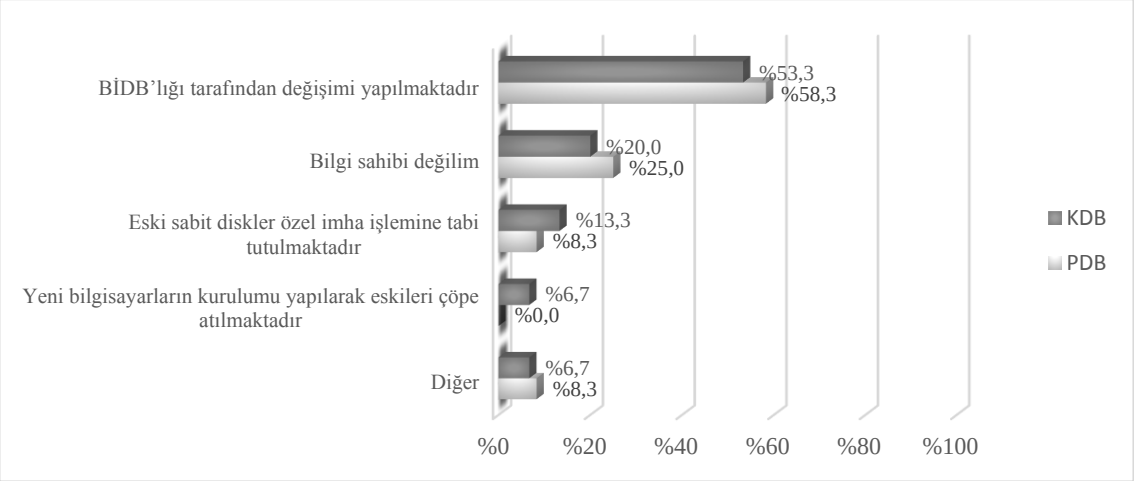
Şekil 5'te üniversitelerde verilerin imha işlemlerine yönelik sorumluluklar ve Şekil 6'da işlem önceliklerine ilişkin veriler yer almaktadır. Üniversite birimlerinde imha işlemlerinden kimlerin sorumlu olduğu BİDB katılımcılarına sorulmuş ve elde edilen bulgular Şekil 5 üzerinde gösterilmiştir. Kullanım süresi sona eren verilerin imhasına yönelik işlemlerin üniversite birimlerinde nasıl yapıldığına ilişkin bilgiler ise PDB ve KDB katılımcılarından elde edilmiş ve Şekil 6 üzerinde gösterilmiştir. İmha sorumluluğu ve birimlerde buna ilişkin işlemlerin yapılmasına yönelik soruların katılımcılar tarafından daha iyi anlaşılabilmesi amacıyla, "birimde kullanım süresi dolan sabit diskler" imha edilecek bilgi deposu örneği olarak kullanılmıştır.



Şekil 5 Üniversite birimlerinde kullanım süresi dolan sabit disklerin imha sorumluluğu

Üniversitelerde veri imha işlemlerine ilişkin politikaların bulunmaması, bu konudaki sorumlulukların paylaşılmasına ilişkin sorulara verilen cevapların da farklılaşmasına neden olmaktadır. Üniversitelerde kullanım süresi dolan (ya da arızalanan) sabit disklerin geri dönüşümü olmayacak şekilde teknik yöntemlerle silinmesi ve imhasından sadece BİDB'nin sorumlu olduğunu düşünen BİDB katılımcılarının oranı %26,7'dir. Ancak Şekil 6 üzerinde yer alan verilere göre, sabit disk değişiminin BİDB tarafından yapıldığını

belirten PDB ve KDB katılımcılarının tamamı, kalıcı silme ve özel imha işlemleri konusunda da BİDB'nin sorumlu olduğunu düşünmektedirler. Bu görüş farklılığı, imha işlemlerine ilişkin sorumluluk ve politikaların belirlenmediği ya da birimler arasında koordinasyon bulunmayan üniversite sayısının Şekil 5'te görünen değerlerin üzerinde olduğunu göstermektedir.



Şekil 6 Kullanım ömrü dolan sabit disklere yapılan işlemler

PDB katılımcıların sadece %8,3'ü ile KDB katılımcılarının %13,3'ü bu tür sabit disklere kendi birimlerinde özel imha işlemi uygulandığını belirtmektedirler. Bu konuda BİDB'nin sorumlu olduğunu düşünen ya da bilgi sahibi olmadığını ifade eden PDB ve KDB katılımcılarının oranı oldukça yüksektir (sırasıyla %83,3 ve %73,3). Görüşme esnasında BİDB katılımcılarına bu özel teknik bilgi ve imkânları gerektiren imha ve silme işlemlerinin BİDB tarafından yapılması konusundaki düşünceleri de sorulmuştur. Katılımcıların tamamı bu konuda talep olması halinde birimlere gerekli desteği sağlayabileceklerini ya da bu tür disklerin imha sürecinin en son halkasında BİDB'nin bulunabileceğini ifade etmişlerdir.

Üniversite PDB'de yazılı-basılı evrakların da yoğun olarak kullanılıyor olması nedeniyle PDB katılımcılarına ayrıca bu evrakları nasıl imha ettikleri sorulmuştur. Katılımcıların %92'si evrak imha makinelerinin kullanıldığını ve bu konuda herhangi bir eksiklik bulunmadığını ifade etmektedirler.

4.9. BİLGİ GÜVENLİĞİNİN SAĞLANMASINA İLİŞKİN EĞİTİM VE FARKINDALIK

Bilgi güvenliğinin sağlanmasına ilişkin eğitim ve farkındalık konusunda hazırlanan sorular, üniversitelerde hukuksal düzenlemelerin ve alınan teknik önlemlerin yetersizliği karşısında katılımcıların ne tür önlemler aldıkları ve eksikliklerin giderilmesi için hangi yöntemlerin etkin olabileceğini düşündüklerini anlamaya yönelik olarak hazırlanmıştır. Sorular hazırlanırken; katılımcıların konuya ilişkin olarak almış oldukları eğitim, bilgi düzeyi ve farkındalıkları ayrı ayrı ölçülerek, alınan eğitimin farkındalığa dönüşümüne ilişkin bilgilerin de elde edilmesine çalışılmıştır. Elde edilen bulgular ışığında, geliştirilecek olan bilgi güvenliği politikasında eğitim ve farkındalığın ağırlığının ne ölçüde olacağına ilişkin çıkarımda bulunulması hedeflenmiştir. Bu amaçla BİDB, PDB ve KDB katılımcılarına; bilgi varlıklarının korunmasına ilişkin eğitim ve toplantı durumu, veri ihlali olması halinde uygulanacak eylem planı, hassas ve kişisel veri kapsamında değerlendirilen bilgilerin neler olduğu kişisel verilerin korunmasına yönelik önlemlerin önceliğine ilişkin farklı sorular yöneltilmiştir.

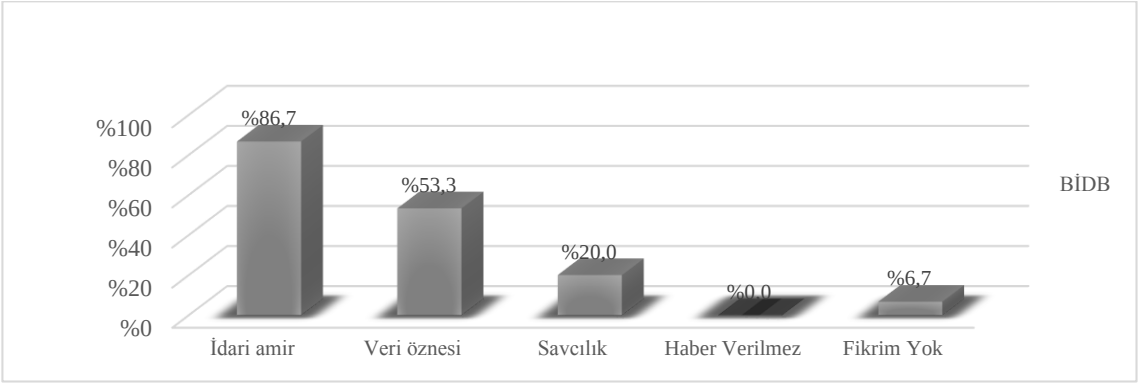
Üniversitelerde kişisel verilerin yoğun olarak işlendiği birimlerin yöneticileri olarak PDB ve KDB katılımcılarına bilgi varlıklarının korunmasına ilişkin eğitim ve toplantılara katılma durumları sorulmuş ve katılımcıların yanıtları Tablo 11 üzerinde ayrı ayrı gösterilmiştir. Bir PDB katılımcısı haricindeki tüm katılımcılardan (N=29) bu soruya yönelik yanıt alınmıştır. Görüşme esnasında bilgi varlıklarının korunmasına ilişkin eğitim ve bilinçlendirme toplantılarıyla ilgili durumun yanı sıra, uygulamalar ve önceliklerin belirlenmesi hakkında da bilgiler alınmıştır.

Tablo 11 Bilgi varlıklarının korunmasına ilişkin eğitim ve toplantı durumu

Kişisel verilerin korunmasına ilişkin olarak bilgilendirildiniz mi?						
	PDB		KDB		Toplam	
	N	%	N	%	N	$\%_{Ort}$
Evet	6	42,9	1	6,7	7	24,1
Hayır	8	57,1	14	93,3	22	75,9
DD	1	-	-	-	1	-

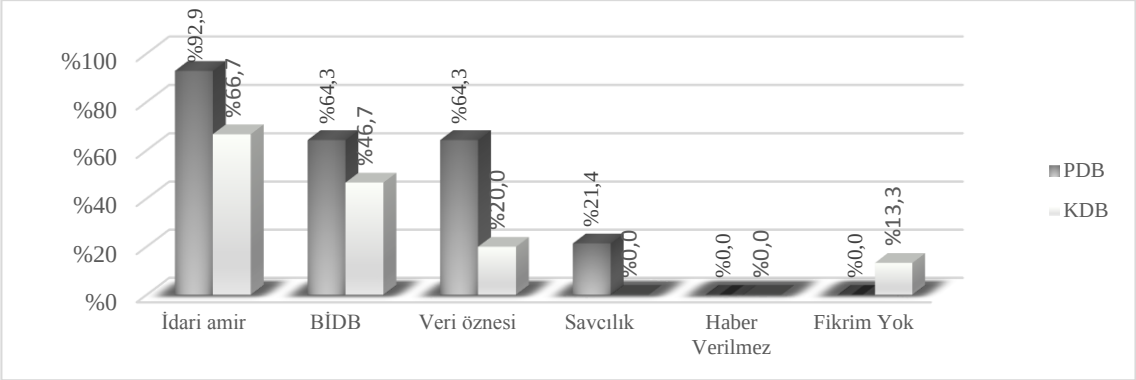
PDB katılımcılarının %57,1'i, KPB katılımcılarının ise %93,3'ü bilgi varlıklarının korunmasına ilişkin olarak herhangi bir bilgilendirme toplantısına katılmadıklarını belirtmektedirler. Bilgilendirme toplantılarına katıldığını belirten altı PDB katılımcısının dördü, soru üzerindeki açıklama kısmında diğer kurum ve kuruluşlarda (Sosyal Güvenlik Kurumu, Yükseköğretim Kurulu, Arşivler Genel Müdürlüğü vd.) yapılan bu tür eğitim ve toplantılara kendi istek ve taleplerine bağlı olarak katıldıklarını ifade etmişlerdir. Sadece bir PDB ve bir KDB katılımcısı üniversite tarafından bilgi güvenliği konusunda bilinçlendirme toplantıları düzenlendiğini ancak bunun da düzenli aralıklarla yapılmadığını belirtmektedir. Katılımcıların açıklamaları da dikkate alınarak değerlendirildiğinde, üniversitelerin %89,5'inde bilgi varlıklarının korunmasına ilişkin yeterli ve düzenli bilgilendirme toplantılarının yapılmadığı görülmektedir.

BİDB, PDB ve KDB katılımcılarına kişisel verilerin ihlal edilmesi durumunda konuya ilişkin olarak kimlerin ya da hangi birimlerin haberdar edileceği sorulmuştur. PDB ve KDB katılımcılarına yöneltilen soruya BİDB'ye yöneltilen sorudan farklı olarak "BİDB'nin haberdar edilmesi" seçeneği de ilâve edilmiştir. BİDB'ye yöneltilen soru tüm katılımcılar (N=15) tarafından yanıtlanmış, PDB ve KDB'ye yöneltilen sorular ise bir PDB katılımcısı haricindeki (N=29) tüm katılımcılar tarafından yanıtlanmıştır. BİDB'den elde edilen bulgular Şekil 7 üzerinde, PDB ve KDB'den elde edilen bulgular ise Şekil 8 üzerinde gösterilmiştir. Katılımcıların bu soruları yanıtlarken birden fazla seçeneği işaretlemelerine olanak sağlanmıştır. Şekil 8 üzerinde belirtilen oranlar, sorulara yanıt veren katılımcılar üzerinden hesaplanmıştır.



Şekil 7 Kişisel verilerin ihlal edilmesi durumunda haberdar edilme önceliği (BİDB)

Üniversitelerde henüz veri ihlali nedeniyle yaşanmış bir adli olay ya da soruşturmanın olmadığı tüm katılımcılar tarafından ifade edilmektedir. Bununla beraber, herhangi bir veri ihlali ya da bilgi varlıklarına yönelik saldırılar nedeniyle zararın oluşması durumunda, BİDB katılımcılarının %86,7'si öncelikle bağlı bulunulan idari amirin haberdar edileceğini belirtmektedirler. Bu katılımcıların bir bölümü savcılığın haberdar edilmesi gereken durumlarda bunun idari amir tarafından yapılması gerektiğini düşünmektedirler. BİDB katılımcılarının yarısı (%53,3), kişisel bilgileri ihlal edilen veri sahiplerinin de gerekli önlemleri alabilmeleri amacıyla haberdar edilmeleri gerektiğini düşünmektedirler.



Şekil 8 Kişisel verilerin ihlal edilmesi durumunda haberdar edilme önceliği (PDB ve KDB)

PDB ve KDB katılımcılarının da kişisel verilerin ihlal edilmesi durumunda haberdar edilecek kişi ve birimlere ilişkin sorulara vermiş oldukları yanıtlar BİDB ile benzer niteliktedir. PDB katılımcılarının %92,9'u ile KDB katılımcılarının %66,7'si, öncelikle bağlı bulunulan idari amirin haberdar edileceğini belirtmektedirler. BİDB'nin bu soruya vermiş olduğu yanıtlardan farklı ve ilâve olarak, PDB katılımcılarının %64,3'ü ile KDB katılımcılarının %46,7'si, BİDB'nin de durum ve gelişmelerden haberdar edilmesi gerektiğini düşünmektedirler. Kişisel verileri ihlal edilen kişilerin bilgilendirilmesi gerektiğine inanan PDB katılımcılarının oranı %64,3 iken, KDB katılımcılarının oranı %20'dir. PDB ile KDB katılımcıları arasındaki bu görüş farkının nedeni, KDB katılımcılarının kendileri tarafından kaydedilmemiş ve diğer sistemler üzerinden (öğrenci/personel bilgi sistemi vd.) almış oldukları bu bilgilere ilişkin olarak veri sahibine karşı kendilerini sorumlu hissetmemeleridir. Bu açıdan bakıldığında, KDB katılımcılarının verilerin saklanmasına ilişkin sorumlulukları hakkındaki düşünceleri ile

kişisel verilerin ihlal edilmesi durumunda ilgili birim ya da kişilerin haberdar edilmesi konusundaki düşünceleri arasında doğrusal ilişki bulunmaktadır. BİDB, PDB ve KDB katılımcılarının hiçbiri "haber verilmeksizin en kısa sürede sistem yeniden aktif hâle getirilir" seçeneğini işaretlememişlerdir.

PDB ve KDB katılımcılarına hassas ve kişisel veri kapsamında hangi bilgilerin korunması gerektiğini düşündükleri sorulmuş ve elde edilen bulgular Tablo 12 ve Tablo 13 üzerinde gösterilmiştir. Üniversite PDB ve KDB birimlerinde işlenen kişisel veriler farklı olduğu için, PDB ve KDB katılımcılarına yöneltilen soruların içeriğinde ilgili birime uygun seçeneklere yer verilmiş ve bu soruya verilen yanıtlar ayrı ayrı değerlendirilmiştir. PDB katılımcılarına yöneltilen soru 14 katılımcı tarafından yanıtlanırken, KDB katılımcılarına yöneltilen soru tüm katılımcılar (N=15) tarafından yanıtlanmıştır. Tablo 12 üzerinde belirtilen oranlar, sorulara yanıt veren katılımcılar üzerinden hesaplanmıştır.

Tablo 12 Hassas ya da kişisel veri kapsamında korunan bilgiler (PDB)

Aşağıdaki seçeneklerden hangilerinin personel ile ilişkilendirilmesi halinde "hassas" ya da "kişisel veri" kapsamında korunması gerektiğini düşünüyorsunuz?	PDB	
	N	%
Personelin sicil bilgileri	11	78,6
Personelin PDB kaynaklarına bağlandığı IP adresi	9	64,3
Personelin kimlik bilgileri (Ad-Soyad, TC kimlik numarası vd.)	14	100
Personelin iletişim bilgileri (adres, telefon, e-posta adresi vd.)	14	100
Personelin akademik özgeçmişine ilişkin bilgiler	8	57,1
Personelin etnik, din, dil, ırk bilgileri	13	92,9
Hiçbiri	-	-
DD	1	-

PDB katılımcılarının %50'si, seçeneklerde yer alan tüm bilgilerin kişisel veri olarak korunması gerektiğini düşünmektedirler. İki katılımcı sicil bilgilerinin artık kullanılmadığı gerekçesiyle bu seçeneği işaretlememiştir. Ancak eski sicil bilgilerini de bu kapsamda dikkate alabileceklerinin belirtilmesi üzerine, iki katılımcı da bu bilgilerin kişisel veri olarak korunması gerektiğini düşündüklerini ifade etmişlerdir. Bu nedenle, seçeneklerde yer alan tüm bilgilerin korunması gerektiğini düşünen katılımcılar hesaplanırken, bu iki katılımcı da değerlendirmeye dâhil edilmiştir. PDB katılımcıları bu soruyu yanıtlarken, en fazla IP adreslerinin (%64,3) ve personelin akademik özgeçmişine

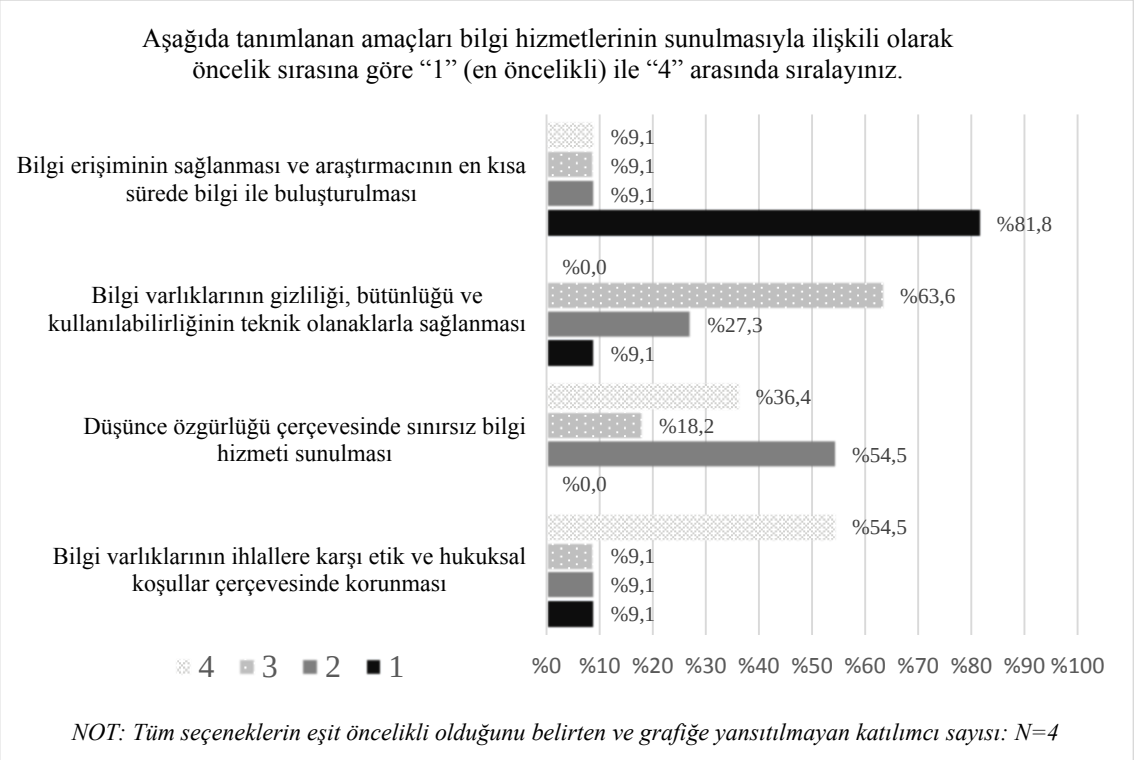
ait bilgilerinin (%57,1) kişisel veri olarak korunması gerektiği ya da gerekmediği noktasında tereddüt etmektedirler. Katılımcılar görüşme esnasında genel olarak IP adresinin korunması konusunda detaylı bilgi sahibi olmadıklarını, akademik özgeçmiş bilgilerinin ise internet ortamından da erişilebilir olduğu ifade etmişlerdir. Kimlik ve iletişim bilgilerinin kişisel veri kapsamında korunması gerektiği noktasında ise tüm katılımcılar birleşmektedir.

Tablo 13 Hassas ya da kişisel veri kapsamında korunan bilgiler (KDB)

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

KDB katılımcılarının hassas ve kişisel veri kapsamında korunması gereken bilgilerin neler olabileceğine ilişkin düşüncelerinde farklılıklar bulunmaktadır. Bu nedenle seçeneklerde sunulan tüm bilgilerin kişisel veri olarak korunması gerektiğine yönelik görüş bildiren KDB katılımcısı oranı düşük seviyededir (%26,7). KDB katılımcılarının hassas ya da kişisel veri kapsamında korunmasına ilişkin olarak en fazla tereddüt ettikleri bilgiler, ödünç alınan yayınların listesi (%33,3), danışma hizmetleri kapsamında edinilen bilgilerin listesi (%53,3) ve IP adresleridir (%53,3). KDB katılımcılarının büyük çoğunluğu bu üç seçeneği işaretleme konusunda tereddüt etmişlerdir. Ancak görüşme esnasında bu verilerin neden korunması gerektiği konusunda bilgi verilmesi sonrasında bu seçenekleri işaretlemişlerdir. İletişim ve kimlik bilgilerinin korunması gerektiği konusunda ise KDB katılımcılarının büyük bölümünün (%93,3) tereddüdü bulunmamaktadır. PDB ve KDB katılımcılarının vermiş olduğu yanıtlardan, her iki birimin de konuya ilişkin görüşlerinde büyük benzerlik olduğu görülmektedir.

KDB katılımcılarının bilgi varlıklarının korunmasına vermiş oldukları önem ve önceliklerinin daha detaylı olarak anlaşılabilmesi amacıyla, bilgi hizmetlerinin sunulmasına yönelik önceliklerini belirtmeleri istenmiştir. Katılımcılara bilgi hizmetlerinin sunulması esnasında göz önünde bulundurulabilecek ve aynı zamanda hukuksal, teknik, etik ve uygulamaya yönelik mesleki prensipleri içeren seçenekler sunularak aralarında bir öncelik sıralaması yapmaları istenmiştir. Soru tüm KDB katılımcıları (N=15) tarafından yanıtlanmıştır. Ancak dört KDB katılımcısı tüm seçeneklerin kendileri için eşit öneme sahip olduğunu vurgulayarak tercihlerini bu doğrultuda yapmışlardır. Bu katılımcıların yanıtları Şekil 9 üzerinde yer alan diğer öncelik değerlerini değiştirmemesi için ayrıca gösterilmiştir. Şekil 9 üzerindeki hesaplamalar, öncelik belirten katılımcıların (N=11) vermiş oldukları yanıtlara bağlı olarak yapılmıştır.



NOT: Tüm seçeneklerin eşit öncelikli olduğunu belirten ve grafiğe yansıtılmayan katılımcı sayısı: N=4

Şekil 9 Bilgi hizmetlerinin sunulmasıyla ilgili hukuksal, teknik ve etik öncelikler

Bu soruyu yanıtlarken katılımcılardan bilgi hizmetlerinin sunulması esnasında "ihmal edilebilirliği" göz önünde bulundurmaları istenmiştir. Ancak yanıtların dağılımı içerisinde katılımcıların %81,8'inin "bilgi erişiminin sağlanması ve araştırmacıların en

kısa sürede bilgi ile buluşturulmasını" en öncelikli olarak işaretlediği görülürken; %54,5'inin "bilgi varlıklarının etik ve hukuksal koşullar çerçevesinde korunmasına" en düşük önceliği vermeleri dikkat çekicidir. Katılımcılara bu seçeneğe ilişkin olarak "bilgi varlığı" kavramı ile hassas ve kişisel verilerin kast edildiği bilgisi verilmiştir. Bu seçeneği öncelikler arasında son sıraya yerleştiren katılımcıların oranı, "düşünce özgürlüğü çerçevesinde sınırsız bilgi hizmeti sunulması" seçeneğini son sıraya yerleştiren katılımcıların oranından (%36,4) daha fazladır. Katılımcıların büyük bölümünün (%63,6) üçüncü öncelikli olarak gördükleri seçenek ise "bilgi varlıklarının gizliliği, bütünlüğü ve kullanılabilirliğinin teknik olanaklarla sağlanması" olmuştur. Bununla beraber, sunulan tüm seçeneklerin öncelikli olduğunu belirten dört katılımcının (%26,6) olması önem taşımaktadır. Bu katılımcılar, sunulan seçenekler arasında bir denge bulunduğunu ve birinin tamamen ihmal edilmesi halinde diğerlerinin üzerinde olumsuz etkisi olabileceğini ifade etmektedirler. Şekil 9'dan elde edilen veriler, genel olarak KDB katılımcıları için bilgi hizmetlerinin sunulmasında hukuksal, etik ve teknik önlemlerin alınmasının daha düşük öncelikli olduğunu göstermektedir. Bu soruya verilen yanıtlar ile katılımcıların kişisel veri kapsamında korunması gereken bilgilere ilişkin görüşlerini ortaya koyan soruya vermiş oldukları yanıtlar arasında doğrusal ilişki olduğu görülmektedir.

PDB ve KDB katılımcılarına ayrıca kişisel verilerin işlendiği bilgisayarlardaki oturum açma politikalarına ilişkin uygulamaları sorulmuştur. İki PDB katılımcısı haricindeki tüm PDB ve KDB katılımcıları (N=28) bu soruyu yanıtlamıştır. Alınan yanıtların biri haricinde tamamı (%96,4), kişisel verilerin işlendiği bilgisayarları her personelin kendi kullanıcı hesabı ile açabildiğini ve böylece yapılan işlemlerin hangi personel tarafından gerçekleştirildiği bilgilerine ulaşılabileceğini belirtmişlerdir. Ortak kullanıcı hesabı kullanıldığını ifade eden KDB katılımcısı ise, kurulum aşamasında olduklarını ve henüz yeterli sayıda bilgisayarın bulunmadığını belirtmektedir.

PDB ve KDB katılımcılarından personel ve kullanıcılara ait kişisel verilerin korunmasına ilişkin önlemleri öncelik sırasına göre sıralamaları istenmiş ve elde edilen bulgular Tablo 14 üzerinde gösterilmiştir. Bu sıralama ile katılımcıların kişisel verilerin korunmasına yönelik hangi önlemlerin (hukuksal, teknik, idari ve etik) öncelikle alınmasına ihtiyaç

duyduklarının ve daire başkanlarının bu konuya bakışlarındaki farklılıkların belirlenmesi hedeflenmiştir. Bir PDB katılımcısı haricindeki tüm katılımcılar (N=29) soruyu yanıtlamıştır. Ancak dört KDB katılımcısı tüm seçeneklerin ya da içlerinden bazılarının kendileri için eşit öneme sahip olduğunu vurgulayarak tercihlerini bu doğrultuda yapmışlardır. Bu katılımcıların yanıtları Tablo 14 üzerinde yer alan öncelik değerlerini değiştirmemesi için hesaplamalarda değerlendirme dışı bırakılmıştır.

Tablo 14 Personel ve kullanıcılara ait kişisel verilerin korunmasına ilişkin öncelikler

Personel ve kullanıcılara ait kişisel verilerin korunmasına ilişkin önlemleri öncelik sırasına göre "1" (en öncelikli) ile "4" arasında sıralayınız.																
	1				2				3				4			
	PDB		KDB		PDB		KDB		PDB		KDB		PDB		KDB	
	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%
Hukuksal düzenlemeler kapsamında korunmalıdır	10	71,4	8	72,7	2	14,3	1	9,1	-	-	1	9,1	2	14,3	1	9,1
Teknik önlemler alınmalıdır	1	7,1	1	9,1	3	21,4	3	27,3	8	57,1	5	45,5	2	14,3	2	18,2
İdari önlemler alınmalıdır	-	-	1	9,1	7	50	2	18,2	6	42,9	5	45,5	1	7,1	3	27,3
Etik ilkeler çerçevesinde korunmalıdır	3	21,4	1	9,1	2	14,3	5	45,5	-	-	-	-	9	64,3	5	45,5
DD	1	-	4	-	1	-	4	-	1	-	4	-	1	-	4	-

PDB katılımcıların %71,4'ü ile KDB katılımcıların %72,7'si kişisel verilerin korunmasına ilişkin olarak alınması gereken önlemlerin hukuksal düzenlemeler kapsamında olması gerektiğine inanmaktadırlar. Seçenekler arasında PDB ve KDB katılımcılarının büyük bölümü (sırasıyla %64,3 ve %45,5) en düşük önceliği etik ilkelere bağlı olarak alınacak önlemlere vermişlerdir. Ancak KDB katılımcılarının ikinci öncelikli olarak alınması gereken önlemler konusunda da "etik değerler" üzerinde yoğunlaştıkları (%45,5) görülmektedir. Bu sonuçlar, KDB katılımcılarının görüşme esnasında vurgulamış olduğu "hukuksal düzenlemelerin yetersizliği nedeniyle bilgi güvenliği önlemleri etik kurallar çerçevesinde alınıyor" ifadesiyle de örtüşmektedir. Uygulamadaki yaklaşım ile olması gerektiği düşünülenler arasında bu tür farklılıklar görülebilmektedir. Uygulamada KDB katılımcıları etik ilkeleri daha fazla dikkate almakta ve bu kapsamda sorumluluklarının bulunduğunu düşünmektedirler. PDB katılımcılarının ikinci öncelikli olarak alınması gereken önlemler konusunda KDB katılımcılarından farklı düşündükleri ve "idari önlemler" üzerinde yoğunlaştıkları (%50) görülmektedir. Teknik önlemlerin alınması konusu ise PDB ve KDB katılımcılarının ancak üçüncü öncelikli tercihi olabilmiştir.

Kişisel verilerin korunmasına ilişkin sorumluluğu bulunmadığını düşünen ve bu nedenle öncelik belirlemek istemeyen katılımcılar için, soruya "kişisel verilerin korunması PDB'nin sorumluluklarından biri değildir" seçeneği de ilâve edilmiştir. Ancak PDB ve KDB katılımcıları arasında kişisel verilerin korunması konusunda sorumluluğunun bulunmadığını düşünen katılımcı bulunmamaktadır.

Tablo 14 üzerinde yer alan veriler incelendiğinde, KDB katılımcılarının bilgi hizmetlerinin sunulması esnasındaki öncelikleri ile kişisel verilerin korunmasına yönelik önlemlerin alınmasındaki öncelikleri arasındaki farklılık dikkat çekmektedir. Bu fark katılımcılardaki iki soruya yönelik algı farkının ötesinde, bilgi hizmetlerinin sunulması esnasındaki risklere yönelik algılarından kaynaklanmaktadır. KDB katılımcıları bilgi hizmetleri kapsamında edinilen bilgilere ilişkin kayıtların hassas ya da kişisel veri olarak korunması gerektiğini düşünmemektedirler. Bilgi hizmetlerinin sunulması esnasındaki risk algısının düşük olması, hukuksal düzenlemelere yönelik önceliği azaltırken; kişisel

verilerin korunmasına ilişkin önlem alınması söz konusu olduğunda, KDB katılımcıları öncelikle hukuksal düzenlemeler kapsamında önlem alınmasını öngörmektedirler.

4.10. KATILIMCILARIN KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN İLÂVE GÖRÜŞ VE ÖNERİLERİ

Uygulanan anket sonunda katılımcıların konuya ilişkin görüşlerini ifade edebilmeleri için oluşturulan kısımda belirtmiş oldukları ilâve görüş ve önerilerden elde edilen bulgular ve katılımcıların açık uçlu sorulara yönelik değerlendirmelerinde öne çıkan hususlara Tablo 15 üzerinde yer verilmiştir. Katılımcılar tarafından belirtilen ilâve görüşler ve bu görüşleri sunan katılımcının çözüm önerileri, üzerinde herhangi bir değişiklik ya da ilâve yapılmaksızın Tablo 15 üzerinde gösterilmiştir. Birden fazla katılımcı tarafından belirtilen öneri ve görüşler, ilgili birimler altında gruplandırılmıştır. Sadece bir katılımcı tarafından belirtildiği halde üniversiteler için önemli olabileceği değerlendirilen görüş ve önerilere de Tablo 15 üzerinde ayrıca yer verilmiştir. Araştırma kapsamında elde edilen diğer verilerle birlikte açık uçlu sorulardan elde edilen bu veriler de "değerlendirme ve sonuç" bölümünde irdelenmektedir.

Tablo 15 Üniversitelerde bilgi güvenliğinin sağlanmasına ilişkin ilâve görüş ve öneriler

Görüş Bildiren Başkanlık	**Görüş**	**Çözüm Önerisi**
PDB KDB (N=13)	Yazılı kaynakların olmaması, özellikle yeni kurulan üniversiteler için kişisel verilerin korunması sürecini daha uzun ve zorlu hale getirmektedir.	Türkiye'de kişisel verilerin korunmasına yönelik tüm kurum ve kuruluşları kapsayan bir çerçeve düzenlemeye ihtiyaç vardır. Kurum ve kuruluşlar bu çerçeve düzenlemeye dayanarak kendi özel koşullarını içeren kurumsal düzenleme ve politikalarını oluşturmalıdırlar.
BİDB (N=6)	Geleneksel veri saklama yöntemleri ve verilerin saklandığı yer konusundaki köklü değişiklikler ve farklılıklar değerlendirilmelidir.	Elektronik bilgilerin saklanması, derlenmesi ve kullanılması konusundaki sorumlulukların ve sorumluluk sahiplerinin yeniden tanımlanması gerekmektedir.
PDB (N=4)	Devletin oluşturduğu merkezi projeler kapsamında kimlik numarası ile erişim sağlanan veri tabanları için gereğinden fazla yetki verilmekte ve kişinin tüm bilgilerine ulaşılabilmektedir.	Bu durum risk yönetimi kapsamında üniversitelerde alınacak önlemlerin belirli bir noktadan sonra yetersiz kalmasına neden olabilir. Daha geniş kapsamlı platformlarda konu gündeme taşınmalıdır.

Tablo 15 (Devam)

BİDB (N=12)	Eksikliklerin görülmesi ve konunun detaylarının fark edilmesi için yeni çalışmalara ihtiyaç duyulmaktadır.	Bu tür çalışmalar eksikliklerin görülmesi ve konunun detaylarının fark edilmesi açısından büyük önem taşımaktadır. Bu araştırma soruları sayesinde yazılı politikaların önemi daha iyi anlaşılmaktadır. Yazılı politikalar üniversite birimleri arasında sorumlulukların paylaşılmasına da katkı sağlayacaktır. Her kurum ve birimin bu konuda yazılı politikaları bulunmalıdır.
BİDB PDB KDB (N=34)	Kişisel verilerin korunmasına ilişkin hukuksal dayanakların oluşturulması için birçok farklı hukuksal düzenlemeden faydalanılmaktadır. Hangi hukuksal düzenleme içinde ne tür sorumlulukların bulunduğu hakkında bilgi sahibi olunmadığı gibi, hukuk mevzuatı içerisinden bu sorumlulukların üniversite birimleri tarafından belirlenmesi de çok zor ve uzun bir süreç içinde yapılacak çalışmaları gerektirmektedir.	Hukuksal sorumlulukların da yer aldığı bu tür çalışmalara ağırlık verilmesi üniversiteler için önemli bir kazanım olacaktır.
BİDB PDB KDB (N=27)	Hukuksal düzenlemelerin ihtiyacı karşılamaması nedeniyle eğitim ve farkındalık konusu son yıllarda daha önemli hale gelmiştir.	Kişisel verileri işleyen personele yönelik farkındalık eğitimlerine daha fazla önem verilmelidir.
PDB KDB (N=6)	Yasal sorumlulukların belirlenmesi ve uyum sağlanması konusunda sorunlar yaşanmaktadır.	Özellikle yeni kurulan üniversitelerde yasal sorumluluklara daha hızlı ve kolay uyum sağlanabilmesi için bu sorumlulukların belirlenmesi ve yalın bir dille kontrol listesi haline getirilmesine ihtiyaç duyulmaktadır.
KDB (N=5)	Yönetim konumunda olan kişilerin daha duyarlı ve bilinçli olmaları gerekmektedir.	Çalışanların özenle seçilmesi, üst düzey yönetici konumunda olan kişilerin mesleki eğitim ve etik ilkeler konusunda bilgi birikimi olması, orta düzey yönetici konumunda olan kişilerin denetim ve gözetimleri sürekli olarak yapması ve "insanın ve kişisel verilerin öncelikli olduğu" bilincinin oluşması önem taşımaktadır.
BİDB (N=1)	Alınan teknik önlemlerin farklı boyutları ve etkileri göz önünde bulundurulmalıdır.	Bilgi güvenliği kapsamında alınan teknik önlemler, kullanıcıların bilgi erişim haklarını sınırlandırmamalıdır.
PDB KDB (N=4)	Üniversite birimlerinin elde ettiği verilerin kullanımına ilişkin şartların belirlenmesi gerekir.	Öğrencilerin kayıt aşamasında oluşturulan "özlük bilgi formu" kapsamında, kişisel verilerin ve not bilgilerinin ailesi ya da diğer üçüncü kişilerle paylaşılmasına ilişkin olarak yazılı onay alınmalı ve üniversite birimleri bu şartlara uymalıdır.
KDB (N=3)	Dağınık ve geçici düzen içerisinde verilen hizmetin kalitesi düştüğü gibi, risk yönetiminin yapılması da zorlaşmaktadır.	Yeni kurulan üniversitelerde öncelikle altyapı planlaması yapılmalıdır.

Tablo 15 (Devam)

PDB (N=1)	EBYS'nin kullanıldığı üniversitelerde zaman zaman verilere erişim sorunları yaşanması nedeniyle henüz yeterli güven sağlanamamış ve yazılı-basılı evrak arşivlerinin kullanım oranında azalma olmamıştır.	EBYS sistemleri yapılan işlemlerin detaylı olarak takip edilebilirliğini sağlaması açısından önemlidir. Ancak bu sistemlerin sorunsuz çalışma noktasına gelmesi zaman alacağı için bu süreçte yazılı-basılı evrak arşivleri ihmal edilmemelidir.
PDB (N=3)	Her birimin kendi arşivini korumak zorunda olması ve bunun nasıl yapılacağı konusunda belirlenmiş yazılı politikaların olmaması, iş sürecini ve risk yönetim sürecini olumsuz etkilemektedir.	Üniversitelerde elektronik ve yazılı-basılı evrak arşivleri merkezileştirilmelidir. Ayrıca elektronik arşivlerin korunmasına ilişkin yasal düzenlemeler ivedilikle yapılarak bu konudaki endişeler giderilmelidir.
PDB (N=2)	EBYS yazılım çeşitliliği oldukça fazladır. Ancak bu yazılımların ya da ilgili şirketlerin herhangi bir güvenlik standardına uyma zorunluluğu bulunmamakta ve denetimi yapılamamaktadır. Yazılım şirketleri ile kurulan bağ ise yazılımın satın alınması ile sonlanmamakta ve servis desteği ile devam etmektedir.	Yazılımların kurulduğu tüm bilgisayarların internete bağlı olması, bu konudaki endişeleri arttırmaktadır. Bu nedenle bazı üniversiteler kendi geliştirmiş oldukları yazılımları kullanmaktadırlar. Bu konuda standartlar belirlenmeli ve yazılımların belirli bir güvenlik standardına sahip olması zorunlu hale getirilmelidir.
BİDB PDB (N=7)	Devlet üniversitelerinde çalışan ve kişisel verileri işleyen personelin devlet memuru olması nedeniyle de ayrıca hukuksal sorumlulukları bulunmaktadır.	Vakıf üniversitelerinde bu tür sorumlulukların personel ile yapılan sözleşmeye ilâve edilmesi önem taşımaktadır.
BİDB PDB (N=12)	Veri tabanlarına erişim yetkilendirmeleri konusunda endişeler bulunmaktadır.	Kişisel verilerin işlendiği veri tabanı yazılımlarının erişim yetkileri düzenlenirken "bilmesi gereken prensibi" göz önünde tutulmalıdır. Aynı birim içinde çalışanlar ya da BİDB çalışanlarının da bu prensip çerçevesinde veri tabanlarına erişim yetkilerinin düzenlenmesi ve işlem kayıtlarının tutulması gerekmektedir. Ayrıca programların (örneğin özlük programı) birimde bulunan tüm bilgisayarlarda yüklü olması gerekmemektedir. Kişisel verileri işleyen birimler, bu veriler üzerinde BİDB ve diğer birimlerin yapmış olduğu işlemleri ve yapılan değişiklikleri düzenli aralıklarla kontrol etmelidirler.
PDB KDB (N=8)	Kişisel verilerin işlendiği üniversite birimlerinde elektronik ortamlarda yer alan bilgilerin saklanması ve imha edilmesine ilişkin olarak yeterli düzeyde bilgi sahibi olunmadığı için farkındalık da oluşmamaktadır. Elektronik ortamlardaki bilgilerin korunmasına ilişkin standartlar belirlenmemiştir. Kişisel verileri işleyen personel sadece mesleki eğitim kapsamında edindiği etik ilkeleri ve personel katılış bilgilendirmelerini dikkate almaktadır.	Kişisel verileri işleyen personele farkındalık eğitimleri düzenlenmeli ve belirli aralıklarla tekrar edilmelidir. Üniversitelerde verilerin işlenmesi, saklanması ve imha edilmesine ilişkin süreçler belirlenmelidir.

Tablo 15 (Devam)

BİDB PDB KDB (N=33)	Üniversitelerde sabit disklerin kalıcı olarak silinmesi ve imhasına yönelik olarak hangi standartların kullanılacağına ilişkin politikalar bulunmamaktadır.	Bu konuda üniversite BİDB ile koordinasyon sağlanmalı ve sorumluluklar belirlenmelidir.
BİDB (N=2)	BİDB tarafından yerine getirilmesi istenen işlemler kayıt altına alınmadığı için, yapılan işlemlere ilişkin sorumluluklar belirsiz olarak kalmaktadır.	Üniversite birimlerinin BİDB tarafından yerine getirilmesini istediği işlemlere ilişkin, başvuru yapabileceği ve işlem taleplerinin kayıt altına alındığı bir bilgi işlem yardım masası oluşturulmalıdır. Böylece veri tabanlarına yapılan toplu veri girişleri de dâhil olmak üzere gerektiğinde birçok işlem hakkında bilgi edinilmesi sağlanabilecektir.
BİDB (N=10)	ULAKBİM Kabul Edilebilir Kullanım Politikası kapsamındaki sorumluluklar üniversite birimleri tarafından bilinmemektedir.	ULAKBİM Kabul Edilebilir Kullanım Politikası kapsamındaki sorumluluklar üniversite birimlerine devredilerek, birimlerin bu konudaki farkındalığı ve iç denetim etkinliğinin arttırılması sağlanabilir.
BİDB (N=2)	Üniversite BİDB'nin bölümlerde bilgi işlem faaliyetlerine ilişkin yetkilendirme, denetim ya da yaptırım uygulama yetkileri bulunmamaktadır. Bununla beraber, bölüm sayısının çok fazla olduğu üniversitelerde BİDB'nin bilinçlendirme çalışmaları yetersiz kalabilmektedir.	Bu tür bilinçlendirme çalışmaların birim bilgi işlem sorumluları tarafından BİDB ile koordineli olarak yürütülmesinin etkinliği arttıracağı düşünülmektedir.

5. BÖLÜM

DEĞERLENDİRME VE SONUÇ

Değerlendirme ve sonuç bölümünde, kişisel verilerin korunmasına ilişkin olarak AB ve Türk Hukuk Mevzuatından elde edilen temel veriler ve bu kapsamda BİDB, PDB ve bilgi merkezlerinde yapılan araştırma sonucunda elde edilen bulgular tartışılmakta ve yorumlanmaktadır. Genel değerlendirme kapsamında araştırmada elde edilen bulguların temelinde hangi gerçeklerin bulunduğu açıklanarak, üniversiteler için geliştirilecek olan bilgi güvenliği politikalarında yer alacak unsurların gerekçelerinin ortaya konulması amaçlanmaktadır. Böylece bilgi güvenliğinin sağlanması ve kişisel verilerin korunmasına yönelik olarak yazılı politika geliştirilerek, üniversitelerde uygulanabilir ve hukuksal düzenlemelerle uyumlu bir bilgi güvenliği politikasının ilk örneği ortaya konulacaktır.

Bu bölümde, hukuksal düzenlemelerin yeterliliği, kişisel verilerin korunmasına ilişkin bilgi güvenliği politikaları, üniversitelerde kişisel verilerin toplanması, düzenlenmesi ve güncellenmesi, kişisel verilerin kullanımı ve paylaşımı, üniversitelerde kişisel verilerin korunması amacıyla alınan bilgi güvenliği önlemleri ve bunların hukuksal düzenlemelere uyumluluğu, verilerin korunmasına ilişkin sorumluluklar, üniversitelerde bilgi güvenliğine ilişkin risk durumu ile eğitim ve farkındalık durumuna ilişkin bulgular değerlendirilerek araştırma sorularına cevap aranmaktadır. Ulaşılan sonuçlar geliştirilecek olan bilgi güvenliği politikalarına rehber olabilecek ve yön verebilecek nitelikte olmakla birlikte, bu konudaki eğitim ihtiyaçlarını da ortaya koymaktadır. Araştırma bulgularının değerlendirildiği bu bölümde ulaşılan sonuçların, diğer kurum ve kuruluşların da göz önünde bulundurmaları gereken bir kaynak niteliğinde olduğu düşünülmektedir.

5.1. HUKUKSAL DÜZENLEMELER VE ÜNİVERSİTELERDE KİŞİSEL VERİLERİN KORUNMASI

Kişisel verilerin korunmasına ilişkin olarak AB ülkelerinde yapılan çalışmaların teknik, hukuksal ve bilgi güvenliği politikaları boyutlarıyla birbiriyle bütünleşmiş olarak

yürütüldüğü görülmektedir. Dünya genelinde de insan haklarına duyarlı birçok ülke (ABD, Kanada, Japonya, Avusturalya vd.) AB'ne benzer bir yaklaşımla kişisel verilerin korunması konusunu gündeme taşımakta ve çözüm için yeni arayışlar içine girmektedirler. Özellikle e-ticaret ile birlikte uluslararası boyuttaki kişisel verilerin transferinin risklerin oranını arttırması, bu konuda uluslararası boyuttaki çalışmaların da hız kazanmasına neden olmuştur. Bu açıdan bakıldığında, ülkelerin kişisel verilerin korunmasına yönelik olarak yapacağı çalışmaların, ülke içindeki gereksinimleri karşılamasının yanı sıra, uluslararası standartları da karşılayacak nitelikte olması önem taşımaktadır. Hukuksal düzenlemeler, kişisel verilerin korunması amacıyla yapılan çalışmaların önemli bir parçası olmakla birlikte, uygulamaya dönük resmi dayanağı niteliğindedir. Bu nedenle, hukuksal düzenlemelerin eksikliğini gidermek amacıyla bilgi güvenliği önlemleri kapsamında öne sürülen diğer çözüm önerileri, herhangi bir zorunluluk ya da yaptırım içermeyen ve bireysel hakları koruma noktasında tek başına yetersiz kalan çözümler olarak değerlendirilmektedir.

AB veri koruma direktiflerinin özünde e-ticarete ilişkin kullanıcı kaygılarının azaltılarak ekonominin canlandırılması bulunmaktadır. Bu kaygıların ana unsurunu kişisel verilerin korunması konusu oluşturmaktadır. Bu açıdan bakıldığında, bilgi güvenliği için alınan önlemlerin odak noktası kişisel verilerin korunmasıdır. Ancak Türkiye'de e-ticarete yönelik kaygıların çevrimiçi ekonomiyi etkileyecek düzeyde olmaması nedeniyle, daha çok gizliliğin korunmasına yönelik önlemler alınmaktadır. Türkiye'nin veri koruma kanunu için gerekçeleri temelde AB ile benzer yönler taşımakla birlikte, AB'ye uyum sağlama süreci daha ön planda tutulmakta ve temel hak ve özgürlüklerin korunması amacı KVKK'ya duyulan gereksinimler içinde ikinci öncelikli sırayı almaktadır. Bununla beraber, kişisel verilerin korunmasına ilişkin düzenlemeler ve bu alandaki reform çalışmaları AB hukuk sisteminde önemli bir yer teşkil etmektedir. Bu nedenle, AB'ye katılım sürecinde kişisel verilerin korunmasına ilişkin hukuksal düzenlemelerin AB hukuku ile uyumlu olarak yapılması, bu konudaki bilgi ve tecrübe birikimini almak ve aynı zamanda adalet sisteminde yapılan reformlarda ilerleme sağlamak açısından da önemlidir. AB üyeliği için aday ülkelerin AB hukukuna ve AB'nin benimsemiş olduğu ilkelere uyumu, Komisyon tarafından her yıl yayınlanan raporlarla takip edilmektedir. Türkiye'ye yönelik raporlarda yer alan eleştirilerin içerisinde kişisel verilerin

korunmasına ilişkin hukuksal düzenlemelerin yetersizliğine yapılan vurgu dikkat çekicidir (Avrupa Komisyonu, 2012d).

AB üyelik sürecinde açılan yargı ve temel haklara ilişkin 23. fasılda, Temel Haklar Şartı ile garanti edilen temel haklara saygı gösterilmesinin üye devletler tarafından sağlanacağı ifadesi yer almaktadır (T.C. AB Bakanlığı, 2011). Buna bağlı olarak, Türkiye'nin Temel Haklar Şartı'ndaki standartları karşılaması beklenmektedir. Kişisel verilerin korunması konusunun Temel Haklar Şartında ayrı bir başlık altında düzenlendiği göz önüne alınarak genel yönelim hakkında çıkarımda bulunulduğunda, AB üyeliğine giden yolda kişisel verilerin korunması konusunun daha fazla ertelenemeyeceği değerlendirilmektedir. Lizbon Antlaşması ve ABAD içtihatları gereğince, çatışma olması halinde AB hukuk kurallarının üstünlüğü ve önceliği bulunmaktadır. AB üyelik sürecinde olan Türkiye'nin kişisel verilerin korunmasına ilişkin yaptığı hukuksal düzenlemelerde AB hukuku ile uyumluluğu dikkate aldığı düşünüldüğünde; üniversitelerde AB hukuk normları dikkate alınarak geliştirilecek politikalar, kişisel hakların korunması için daha doğru bir yaklaşım olacaktır. Kişisel verilerin korunmasına ilişkin olarak, Türkiye'de öncelikle kişisel verilerin korunmasına ilişkin mevzuat çalışmalarının hızlandırılması ve bağımsız bir veri koruma ve denetleme otoritesinin kurulması gerekmektedir. Bu süreçte üniversitelerde de benzer bir bilgi güvenliği kurulu kurularak; bilgi güvenliği önlemlerine ilişkin üst yönetime görüş bildirmesi, tavsiyelerde bulunması ve bireysel şikâyetlere yönelik olarak idari birimlerde incelemelerde bulunarak belirlenen güvenlik politikalarının uygulanmasına katkı sağlamasının önemli bir başlangıç olacağı değerlendirilmektedir.

Üniversiteler, kişisel verilerin ağ üzerinden iletimi, yetkisiz erişim, değiştirme ve kazara ya da yasa dışı yöntemlerle yapılacak tahribe karşı gerekli teknik ve kurumsal önlemleri almalıdırlar. Bunun yanı sıra, üniversitelerde kişisel verilere erişim hakkı bulunan işleyici ve işleyici yetkisi altındaki kişiler, kendileri için tanımlanan görev ve yetki kapsamında verileri işlemelidirler. Bu konuda 95/46/EC sayılı direktifin 16. ve 17. Maddeleri, 108 Sayılı Sözleşmenin 7. Maddesi ve KVKKT'nin 11. Maddesi dikkate alınarak üniversitelerde kişisel verilerin korunması, sorumlulukların belirlenmesi ve gerekli teknik önlemlerin alınması büyük önem taşımaktadır. Bazı AB ülkelerinde bu maddelere ilişkin iç hukukta ve uygulamada sorumlulukları genişleten farklılıklar bulunabilmektedir.

Örneğin İngiltere'de, üniversitelerde kişisel verilerin bulunduğu birimlerde çalışan tüm personelin (doğrudan veriyi işleme ya da dağıtım sorumluluğu olmasa dahi) kişisel ve hassas verilerin korunması ve risklerin azaltılması yükümlülükleri bulunmaktadır. Ayrıca, veri koruma direktifinde tanımlanan ihlâllerin gerçekleşmesi durumunda, önemli miktarda yaptırımlar da (para cezası olarak) uygulanabilmektedir (Johnston, 2011).

Anayasa'nın 20. Maddesi kişisel verilerin korunmasını öngörmekte ve kanunda öngörülen hallerde veya kişinin açık rızası ile kişisel verilerin işlenebileceğini söylemektedir. Bu madde ile birlikte, üniversitelerde toplanan ve işlenen kişisel veriler üzerinde veri sahipleri mutlak hak sahibidirler. Kişisel verilerin korunmasına yönelik temel hak ve hürriyetin sadece kanunla sınırlandırılabileceği Anayasa'nın 13. Maddesinde ifade edilmektedir. Buna göre, kişisin açık rızası olmaksızın kişisel verilerin işlenmesinin ancak kanun ile yapılması ve çıkarılan kanunun anayasaya uygun olması gerekmektedir. Bu açıdan değerlendirildiğinde, üniversitelerde ve diğer kamu kuruluşlarında idari düzenlemelere bağlı olarak işlenen kişisel verilere ilişkin sorumluluk, idare ve veriyi işleyen tüm personeli kapsamaktadır. Üniversitelerde kişisel verilerin işlenmesi ve transferine ilişkin uygulamalarda görev alan personelin, Anayasa'nın 137. Maddesinde "kanunsuz emir" başlığı altında ifade edilen hükümlere uygun olarak hareket etmeleri önem taşımaktadır.

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

5.2. ÜNİVERSİTELERDE KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN SORUMLULUKLAR VE BİLGİ GÜVENLİĞİ POLİTİKALARI

Toplumsal hayatın her alanında ihtiyaç duyulan bilgi güvenliğinin sağlanmasına ilişkin olarak, üniversitelerde hukuksal düzenlemelerle uyumlu ve standartlaşmış bilgi güvenliği politikaları bulunmamaktadır. Bilgi güvenliği konusunun çok yönlü oluşu ve disiplinler arası işbirliğini gerektirmesi, bu konunun ötelenmesine ve üniversiteler, kurum ve kuruluşlar için risklerin artmasına neden olmaktadır. Literatürde yer alan veri koruma ve bilgi güvenliğine ilişkin çalışmaların belirli disiplinler altında sınırlı olarak yapılmış olması nedeniyle, sorumlulukların nasıl paylaşılacağı ve uygulamada ne yapılması gerektiği konusunda belirleyici yöntemler ve standartlar geliştirilememiştir.

5.2.1. Hukuksal Düzenlemeler Kapsamında Kişisel Verilerin Korunmasına İlişkin Sorumluluklar

Bilgi güvenliğinin sağlanması konusu ile kişisel verilerin korunmasına ilişkin veri koruma kanunları arasındaki yakınlık, bu iki konunun birbirinden bağımsız olarak ele alınmaması gerektiğini düşündürmektedir. Bununla birlikte, kişisel verilerin korunmasına yönelik hukuksal düzenlemeler, bilgi güvenliğine ilişkin politikaların üretilmesi ve uygulanmasının en önemli dayanağını oluşturmaktadır.

Anayasal bir hak olarak tanımlanan kişisel verilerin korunması hakkı, kişinin rızası ya da hukuksal düzenlemelerde yer alan zorunlu haller dışında sınırlanamayan, devredilemeyen ve vazgeçilemeyen temel haklardan biridir. Bu nedenle kamu yararı için dahi olsa, veri sahibinin rızası, yasal dayanağın bulunması, kullanım amacının belirginliği ve sadece amaca yönelik minimum seviyede kişisel bilginin toplanması ve işlenmesi önem taşımaktadır.

Kişisel verilerin korunması hakkı, bireyin özel hayatını ilgilendiren, kişilik haklarının ve onurun korunması anlamına da gelen bir temel haktır. Kişisel verilerin korunmasıyla, bireyin kendisine ait kişisel veriler üzerindeki karar verme özgürlüğünün ve bu verilerin hukuka aykırı müdahalelere karşı korunması amaçlanmaktadır. Kişinin rızası dışında ve

hukuka aykırı olarak kişisel verilerin elde edilmesi ve işlenmesi, genel kişilik hakkına ve kişiliğin özgürce geliştirilmesi hakkına da müdahale edilmesi anlamına gelmektedir.

Kişisel hak ve özgürlüklerin korunabilmesi için, uygulanabilir nitelikte hukuksal düzenlemelerin yapılması zorunludur. Birçok ülkede, özel hayatın gizliliğinin korunabilmesi amacıyla hukuksal düzenlemeler yapılmış ve buna uyulmaması halinde uygulanacak cezai yaptırımlar belirlenmiştir. Temel hak olmasının yanı sıra hukuksal düzenlemelerle de korunduğu için, birçok ülkede bilginin durumuna (elde edilmesi, işlenmesi, depolanması) bağlı olarak bütünlüğünün ve gizliliğinin sağlanmasına yönelik önlemler alınmaktadır. Hukuksal düzenlemelere uygun olarak, kurum ve şirketler kendi bilgi güvenliği politikalarını oluşturmaktadırlar. Türk Hukuk Mevzuatında yer alan düzenlemeler, üniversitelerde kişisel verilerin korunması konusunda yeterli değildir. Bu nedenle AB Hukuk Mevzuatı da dikkate alınarak, üniversiteler için kapsamlı bir bilgi güvenliği politikasının geliştirilmesi ve tüm üniversite birimlerinde sorumlulukların belirlenmesi gerekmektedir. Türkiye'deki üniversiteler için her ne kadar bağlayıcı olmasa da, AB Hukuk Mevzuatındaki verilerin korunmasına ilişkin düzenlemeler, bu konuda geliştirilecek olan güvenlik önlemleri ve politikalar için önemli bir kaynak niteliğindedir. Üniversitelerde bilgi güvenliği politikaları geliştirilirken AB Hukuk Mevzuatından da faydalanılabileceği gibi; özellikle milletlerarası antlaşmaların göz ardı edilmemesi gerekmektedir. Anayasanın 90. Maddesinde, imzalanan milletlerarası antlaşmaların yasa hükmünde olduğu, çıkabilecek uyuşmazlıklarda milletlerarası antlaşmaların hükümlerinin esas alınacağı ifade edilmektedir. Buna göre, AİHM'nin karar ve yorumları çerçevesinde, kişisel veriler AİHS'nin 8. Maddesi[128] kapsamında korunmakta ve değerlendirilmektedir.

Üniversitelerde kişisel verilerin korunmasına yönelik hukuksal düzenlemeler kapsamında güvenlik önlemlerinin alınabilmesi için, Türk Hukuk Mevzuatı içerisindeki birçok düzenlemenin incelenmesi ve bu kapsamda sorumlulukların belirlenmesi gerekmektedir. Uzun bir süreç içerisinde yapılabilecek bu tür çalışmaların bulunmaması nedeniyle,

[128] **AİHS, 8. Madde:** 1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.
2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.

üniversite birimlerinin hangi hukuksal düzenleme kapsamında ne tür sorumluluklarının olduğu yeterince açık değildir. Bununla birlikte, araştırma sonucunda elde edilen bulgulara göre bu tür çalışmaların üniversite birimleri tarafından yürütülebilmesinin, özellikle sınırlı personel gücü ile faaliyetleri takip eden vakıf üniversitelerinin %80'inde mümkün olamayacağı değerlendirilmektedir. Yeni kurulan üniversiteler başta olmak üzere, sorumlulukların belirlenmesi ve hukuksal düzenlemelere hızlı uyum sağlanabilmesi için, bu tür çalışmalara ağırlık verilmesi ve kontrol listesi niteliğinde kolay anlaşılır politikaların geliştirilmesine ihtiyaç duyulmaktadır.

Üniversitelerde bilgi güvenliğinin sağlanması kapsamında teknik önlemlerin alınmasına ilişkin sorumlulukları üstlenen bilgi işlem daire başkanlarının %33,3'ünün araştırma esnasında hukuksal düzenlemelerin yeterliliği konusunda fikrinin olmadığını belirtmesi; bilgi güvenliğinin sağlanmasına ilişkin disiplinler arası çalışmaların eksikliğinin bir göstergesi olarak değerlendirilmektedir. Aynı zamanda, büyük bölümünün (%80) 5651 sayılı kanun çerçevesinde sorumluluğunun olduğunu ifade ettiği BİDB katılımcıları, sorumlu olduğunu düşündükleri hukuksal düzenlemelerin içeriği hakkında da detaylı bilgiye sahip olmadıklarını ifade etmektedirler. Ayrıca hukuksal düzenlemelerin yetersiz olduğu konusunda görüş bildiren BİDB katılımcılarının da (%66,7) konuyu sadece 5651 sayılı kanun açısından değerlendirmeleri, bu konudaki diğer hukuksal düzenlemelere mesafeli yaklaştıklarını göstermektedir. Özellikle BİDB bünyesinde yeterli sayıda bilgi işlem personeli bulunmayan altı üniversitede, kişisel verilerin korunması gibi uzmanlık ve üzerinde çalışma gerektiren konulara yönelik yeterli zamanın ayrılmasının mümkün olamadığı görülmektedir. Benzer şekilde PDB ve KDB katılımcılarının da %73'ü sorumluluklarının bulunmadığını düşündükleri 5651 sayılı kanuna mesafeli yaklaşırken; Anayasa ve TCK'da kendilerini ilgilendiren düzenlemelerin yapılmış olabileceğini düşünmektedirler. Bununla birlikte hukuksal düzenlemelerin kısmen de olsa yeterli düzeyde olduğunu düşünen katılımcının bulunmaması dikkat çekicidir. Ancak görüşme esnasında katılımcıların %77'sinin hukuksal düzenlemelerin içeriği hakkında bilgi sahibi olmadıklarını ifade etmeleri, yapılan işlemler ve alınan önlemler içerisinde hukuksal düzenlemelerin dikkate alınmasında da eksikliklerin bulunduğunu göstermektedir. Görüşmelerde hukuksal düzenlemelerin dağınık olmasına vurgu yapılsa da, hukuksal düzenlemeleri inceleme konusunda eksikliklerin bulunduğu belirgin olarak gözlenmiştir.

Araştırmada elde edilen bulgular göz önüne alındığında, genel olarak hukuksal düzenlemeler katılımcılar için anlaşılması ve uygulanması zor belgeler olarak nitelendirilebilir. Bu nedenle teknik önlemlerin yanı sıra üniversite birimlerinde hukuksal düzenlemelerin de dikkate alınabilmesi için, katılımcıların hukuk okuryazarlığı konusunda daha iyi seviyede olmaları sağlanmalıdır. KDB katılımcılarının %40'ının özellikle kişisel verilerin korunması konusunda etik kuralları hukuksal düzenlemelerden daha uygulanabilir bulmalarında, hukuksal düzenlemeleri inceleme konusundaki çekincelerinin de etkisi olduğu söylenebilir. Bu konuda örnek alınabilecek AB KVKK gibi hukuksal belgelerin katılımcıların büyük bölümü (%90) tarafından hiç incelenmemiş olması, katılımcıların bu konudaki düzenlemelere olan ilgilerinin düşük olduğunu göstermektedir.

Kişisel verilerin korunması amacına yönelik en önemli bileşenlerden biri, hukusal düzenlemeler kapsamında yer alan KVKK'dır. Ancak üniversite, kurum ve kuruluşlarda etkin bir şekilde veri korumanın sağlanabilmesi için, genel çerçeve niteliğindeki KVKKT'da yer alan temel ilkelerin her kurum ve kuruluş tarafından özel şartların da değerlendirilerek uyarlanması gerekmektedir. Bilgi güvenliği önlemleri kapsamında geliştirilecek bilgi güvenliği politikaları hazırlanırken, kişisel verilerin korunmasına yönelik hukuksal düzenlemeler de göz önünde bulundurulmalıdır.

5.2.2. Üniversitelerde Kişisel Verilerin Korunmasına İlişkin Bilgi Güvenliği Politikaları

Kişisel verilerin korunması konusunda alınacak önleyici tedbirlerin başarısı, hukuksal ve teknik imkânların birlikte kullanımı ve denetimlerde her iki yeterliliğin de aranması ile mümkün olabilmektedir. Üniversitelerde bilgi güvenliği politikalarının geliştirilmesi ve bilgi güvenliği önlemlerinin alınması konusunda ihtiyaçlara cevap veren kapsamlı ve uygulanabilir bir model olarak McCumber bilgi güvenliği modeli, hukuksal ve teknik yeterliliğin sağlanması için gerekli ana çerçevenin oluşturulmasına da imkân sağlamaktadır. McCumber modeli üzerinde bilgi güvenliği konusuna bakıldığında, çok fazla değişkenin bulunduğu dikkati çekmektedir. Kurumsal amaç ve stratejiler, üst

yönetim ve hukuksal düzenlemeler bu değişkenler arasındaki en önemli etkenlerdir. Bir kurumda kişisel verilerin korunmasına yönelik olarak belirlenecek strateji, üst yönetimin bu konuya bakışı ile doğrudan ilişkilidir. İşte bu noktada bilgi sistem yöneticilerin dayanabileceği hukuksal düzenlemelerin varlığı, yeterli düzeyde güvenliğin sağlanması için gerekli bütçenin ayrılması ve üst yönetimin desteğinin alınabilmesi için önemli bir bileşen olarak bilgi güvenliği bütünlüğünü tamamlamaktadır.

Araştırma kapsamında yer alan üniversitelerde kişisel verilerin korunmasına ilişkin kapsamlı bilgi güvenliği politikası bulunmamaktadır. Bilgi güvenliği ve kişisel verilerin korunmasına ilişkin politikaların varlığı konusunda, web sayfaları üzerinden yaptığımız ön araştırma sonuçları ile görüşme sonuçları arasında da farklılık bulunmamaktadır. Üniversitelerin BİDB birimlerine ait web sayfalarında görülen bilgi güvenliği politikaları ise, kişisel verilerin korunmasına ilişkin ihtiyacı karşılayabilecek maddeleri içermemektedir. Genel amaçlı bilgi güvenliği ve kullanım politikaları, üniversitelerin sadece BİDB tarafından geliştirilen ve uygulanan politikalardır.

Üniversitelerde yayınlanmış kapsamlı bilgi güvenliği politikalarının bulunmaması, bilgi güvenliğine ilişkin olarak alınan güvenlik önlemlerinin sadece teknik önlemlerle sınırlı kalmasına ve birimler arasındaki koordinasyonun sağlanamamasına neden olmaktadır. Ancak Charette'nin de belirttiği gibi (Charette, 2012a, 2012b); sadece teknik önlemlerin alınması ile bilgi güvenliği ihlallerinin önüne geçilmesi mümkün değildir. Bilgi sistemleri üzerinde artan veri miktarı, bireylere yönelen tehditler karşısında tüm bilgilerin kriptolanması gibi teknik yöntemlerin uygulanmasını zorlaştırmaktadır. Bu nedenle, mevcut bilgilerin sınıflandırılması ve risk yönetiminin uygulanması, kişisel verilerin korunmasına yönelik olarak alınacak önlemlerin etkinliğini arttırmaktadır. Bilginin sınıflandırılması ve risk yönetimi işlemleri, hukuksal sorumlulukları da içerecek bilgi güvenliği politikaları çerçevesinde yapılmalıdır. İki üniversite tarafından mevcut yasal düzenlemeler bilgi güvenliği politikası olarak değerlendirilmesine karşın; bu yasal düzenlemeler çerçevesinde üniversitelerde kişisel verilerin korunabilmesi için, ilâve çalışma ve uyarlamaların yapılarak birimler arasında sorumlulukların paylaşılması gerekmektedir. Üniversitelerde bilgi güvenliğinin sağlanmasına yönelik olarak yaşanan en önemli sorunlardan biri, iki üniversite dışında birimler arasında sorumlulukların

paylaşılmamış olmasıdır. Sekiz üniversitenin PDB ve KDB birimlerinde bu konuya ilişkin tüm önlemlerin BİDB tarafından alınması gerektiği görüşü hâkimdir. Ancak PDB ve KDB birimlerinin de Anayasa, TCK ve 5651 Sayılı Kanun vd. hukuksal düzenlemeler kapsamında sorumlulukları bulunmaktadır. Üniversiteler için geliştirilecek bilgi güvenliği politikaları bu konudaki belirsizliği ortadan kaldırabileceği gibi, hukuksal düzenlemelerden kaynaklanan eksiklikleri de büyük ölçüde tamamlayacaktır. Hukuksal düzenlemelerin yetersiz olduğu uygulamalarda, yazılı bilgi güvenliği politikaları kişisel verileri işleyen personelin iş sürecini daha güvenli olarak takip etmesine katkı sağlayacaktır.

5.3. VERİLERİN TOPLANMASI, DÜZENLENMESİ VE SAKLANMASI

5.3.1 Üniversitelerde Kişisel Verilerin Toplanması

Üniversitelerde genel olarak kişisel verilerin elde edilmesine ilişkin herhangi bir düzenleme, kriter ya da standart bulunmamaktadır. Özellikle PDB tarafından toplanan bilgiler içerisinde, kullanılmadığı halde tüm kişisel bilgilerin elde edildiği ve bunun bazı hukuksal düzenlemeler (4857 Sayılı İş Kanunu, 657 Sayılı Devlet Memurları Kanunu, 2547 Sayılı Yükseköğretim Kanunu ve 2914 Sayılı Yükseköğretim Personel Kanunu) kapsamında yapıldığı belirtilmektedir. Bu durumun, AB hukuk mevzuatında yer alan kişisel verilerin korunmasına ilişkin tüm düzenlemelerde ve KVKKT'de de yer alan "gerekli minimum bilginin toplanması" ilkesine aykırı olduğu görülmektedir. Üniversite bilgi merkezlerinde bu konuya özen gösterilerek sadece gerekli bilgilerin toplanması sağlanırken, hukuksal düzenlemelerden kaynaklanan tutarsızlıklar nedeniyle üniversite genelinde bu ilkenin uygulanabilirliğinin sağlanması mümkün olamamaktadır. Ancak gereğinden fazla kişisel verinin hukuksal zorunluluklar nedeniyle toplandığı birimlerin (PDB gibi) dışında, daha sonra ihtiyaç olabileceği gerekçesiyle kişisel verilerin toplanmasına, üniversite bilgi güvenliği politikaları ile kısıtlama getirilebileceği ve farkındalığın oluşturulabileceği düşünülmektedir.

Üniversite birimlerinde kişisel bilgiler, doğudan personelin kendisinden ya da personelin kendisi tarafından bilgilerini girmiş olduğu sistemler üzerinden elde edilmektedir. KDB

katılımcılarının %80'i diğer üniversite birimleri tarafından elde edilerek veri tabanına işlenen ya da personelin doğrudan sisteme kaydetmiş olduğu bilgileri kullandıkları için, bu verilerin sahibine karşı sorumluluk hissetmediklerini belirtmektedirler. Ancak kişisel bilgilerin farklı bir üniversite birimi ya da personelin kendisi tarafından bir sistem üzerine aktarılmış olmasının bu sisteme erişim sağlayan tüm kurum, kuruluş ya da üniversite birimleri tarafından alınarak herhangi bir kısıtlama olmaksızın kullanılabileceği şeklinde yorumlanması, kişisel hak ve özgürlüğün sınırlanmasına neden olabilmektedir. Bu tür uygulamalar; Winter'in "kullanıcıların kendilerine ait kişisel bilgilerin ne zaman, nasıl ve ne kadarının başkalarının erişimine açılacağına karar vermeleridir" (Winter, 1997) şeklinde tanımladığı ve 95/46/EC sayılı AB direktifinin yaklaşımıyla da örtüşen "gizlilik" anlayışı ile bağdaşmamaktadır. Kişinin farklı kurum ve sistemler üzerinde tanımlı olan bilgilerinde değişiklik yapması sonrasında; kişinin bilgisi ve rızası dışında bu sistemler üzerinden alınmış bilgilerin yanlış ya da eksik olması ve bunun sonucunda bazı hak kayıplarının oluşma olasılığı bulunmaktadır. 95/46/EC sayılı AB direktifi, 108 Sayılı Sözleşme, TCK ve KVKKT'de de açıkça belirtildiği gibi, kişisel verilerin diğer kurum, kuruluş ya da üniversite birimleri tarafından nasıl elde edildiğine bakılmaksızın, bu verilerin farklı bir kurum ya da üniversite birimi tarafından kullanılması konusunda kişinin rızasının alınması ve gizliliğinin korunması gerekmektedir.

Üniversite bilgi merkezlerinin %86,7'sinde danışma hizmetleri kapsamında elde edilen veriler kişi ile ilişkilendirilmeden kayıt altına alınmaktadır. Ancak araştırma esnasında KDB katılımcılarının %53,6'sı, elde edilen verilerin bireyin kişisel haklarının korunması amacıyla değil, ihtiyaç duyulmaması nedeniyle kişisel verilerle ilişkilendirilmediğini ifade etmiştir. Araştırmada elde edilen bulgular, bilgi merkezlerinde elde edilen bu tür kayıtların kişisel veri kapsamında korunması gerektiğine ilişkin hassasiyetin bulunmadığını ortaya koymaktadır. Hukuksal olarak kamu kurum ve kuruluşlarının kamusal yarar amacıyla kişisel bilgi elde etmesinde bir engel bulunmamaktadır. Ancak bu bilgilerin hangi amaçla alındığı konusunda bilgilendirme yapılması, bilginin işlenmesi, kullanımı, saklanması ve transferine ilişkin olarak bireye tanınan haklar, AİHS'nin 8. Maddesi kapsamında birey için korunma alanı oluşturmaktadır (Anayasa Mahkemesi, 2011). TCK'da da kişisel verilerin korunmasına ilişkin temel ilkeler tanımlanmamış olmasına karşın; kişisel verilerin hukuka aykırı olarak elde edilmesi,

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

Üniversite birimlerinde bulunan bilgisayarların hangileri üzerinde kişisel verilerin bulunduğunun genel olarak bilinmesine (%64,3) karşın, bu bilgiye sahip olmalarının mümkün olmadığını belirten BİDB katılımcılarının da (%35,7) görüşleri dikkate alınmalıdır. Çünkü 30-35 bin kullanıcısı bulunan büyük üniversitelerde, bilgisayar sayısının denetiminin tek merkezden yapılamayacak boyutlara ulaşmış olması önemli bir gerekçe olarak görülmektedir. Bu tablonun, yeni kurulan ve gelişmekte olan üniversitelerin de bir süre sonra karşılaşabilecekleri sorunları işaret ettiği değerlendirilmektedir. Bu nedenle, her ne kadar üniversitelerin birçoğunda merkezi denetim ve kontrol yöntemi uygulanıyor olsa da, bu sorumluluğun üniversite birimlerinde bulunan (ya da oluşturulacak yapılanma içindeki) bilgi işlem sorumluları ile paylaşılmasının faaliyetlerdeki etkinliği arttıracağı düşünülmektedir.

5.3.2 Üniversitelerde Kişisel Verilerin Düzenlenmesi

95/46/EC sayılı AB veri koruma direktifinde, kişisel verilerin korunması konusuna ilişkin kişilerin hak ve özgürlüğünün korunması için, verilerin işlendiği sistemlerin tasarımı esnasında ve verilerin işlenmesi sırasında teknik ve kurumsal önlemlerin alınması gerektiği belirtilmektedir. Ayrıca bu tedbirler alınırken, korunacak verilerin yapısı, risk durumu ve maliyetlerin de dikkate alınması gerektiği vurgulanmaktadır. Veri miktarının artması, verilerin yedeklenmesi ve güvenlik önlemlerinin alınmasına ilişkin maliyetleri de arttırmaktadır. Artan veri miktarına rağmen etkin güvenlik önlemlerinin alınabilmesi için, hassas ve kişisel verilerin sınıflandırılarak[129] diğer verilerden ayrılması ve bu verilere yönelik güvenlik önlemlerinin daha üst seviyede uygulanması önem taşımaktadır. Kriptolama maliyetleri göz önüne alındığında, kişisel verilerin merkezi veri depolama ortamlarında ve sistem yöneticilerinin kontrolünde olmasının maliyetleri ve uygulama problemlerini azaltabileceği değerlendirilmektedir. Diğer ifadeyle, kişisel verilerin sınıflandırılarak depolanma ve transfer durumunda olan diğer verilerden ayrılması, kriptolama işlemi gibi maliyeti yüksek güvenlik önlemleri için ayrılan bütçenin daha verimli kullanılmasına da katkı sağlayacaktır.

Üniversite PDB ve KDB birimlerinin sadece %44'ünde veriler sınıflandırılmaktadır. Verilerin gizlilik seviyelerine göre sınıflandırılması konusunda, birimlere göre de farklılıkların olduğu görülmektedir. Bu farklılıklar büyük ölçüde birimlerin elde etmiş oldukları bilgileri kişisel veri olarak değerlendirip değerlendirmemeleri ile ilişkilidir. 14 üniversite bilgi merkezinin sadece üç tanesinde verilerin sınıflandırılması dikkat çekicidir. Üniversite bilgi merkezlerinde verilerin gizlilik seviyesine göre sınıflandırılmasına ihtiyaç duyulmamasının temel nedeninin, elde edilen bilgilerin kişisel veri kapsamında değerlendirilmemesi olduğu söylenebilir. Üniversitelerde kişisel verilerin korunmasına yönelik bir politikanın bulunmaması nedeniyle, hangi verilerin kişisel veri niteliğinde olduğu, gizlilik seviyesine göre sınıflandırılması ve korunması gerektiği hakkında belirsizlikler bulunmaktadır. Bunun yanı sıra iki PDB katılımcısının da görüşme esnasında belirttiği gibi; üniversitelerde kullanılan elektronik belge yönetim sistemleri ve veri tabanı yazılımlarından yeterli verimliliğin elde edilememesi,

[129] Detaylı bilgi ve örnek sınıflandırma için bkz. (Cole, 2014) ve (Harvard Infosec, 2013)

alışkanlıklardan vazgeçilememesi nedeniyle bu sistemlerin kullanımına yönelik direnç oluşması ya da uyum sürecinin tamamlanmamış olmasının da bilgilerin sınıflandırılması işlemlerinde istenilen düzeyde etkinliğin sağlanamamasında etkili olduğu düşünülmektedir.

5.3.3 Üniversitelerde Kişisel Verilerin Saklanması

Üniversite PDB birimlerinin %85,7'si, verilerin saklanması konusunda kurumun arşiv işlerini merkezi olarak yürüten birimlerle aynı yükümlülükleri taşıdıklarını belirtmektedirler. Bu katılımcılar, üniversitenin merkezi arşiv birimleri olsa dahi, PDB birimi bünyesinde de arşiv dosyalarının bulunduğunu ifade etmektedirler. Ancak üniversite birimlerinde kişisel verilerin ne kadar süre saklandığı konusunda belirsizlikler bulunmaktadır. Araştırma sorularına bu konuda 99, 100 ve 101 yıl gibi çeşitli yanıtlar alınmıştır. Araştırma esnasında, bu belirsizliğin nedeninin iki farklı boyutunun bulunduğu gözlemlenmiştir. Hukuksal düzenlemelerin açık ve anlaşılır olmamasının yanı sıra, üniversitenin hangi kanun ve yönetmelikler kapsamında verilerin saklanacağını belirlememiş olması, bu konudaki eksikliğin bir boyutunu oluşturmaktadır. Bu açıdan bakıldığında, üniversite PDB birimleri arasındaki görüş ve uygulama farklılıklarının ortadan kaldırılması için, hukuksal düzenlemeler çerçevesinde her üniversitenin kurum arşiv merkezleri ile koordineli olarak geliştireceği bir veri saklama politikasına ihtiyacı olduğu düşünülmektedir. Diğer boyutu ise, verilerin saklanacağı depo alanıyla ilgili yer sorunu yaşanmadığı müddetçe tüm verilerin saklanması konusundaki genel eğilimdir. Genel olarak katılımcılar, imha süresi geçmiş olan belgelerin de saklanmasında risk görmezken, imha edilen belgelere süresi dolmasına rağmen ihtiyaç duyulabileceği konusunda çekinceleri bulunmaktadır.

Bilgi merkezleri gibi doğrudan kişisel bilginin elde edilmediği üniversite birimlerinde ise kullanıcı kayıtlarının saklanması konusunda belirsizliklerin daha büyük boyutta olduğu ve sadece %26,7'sinde verilerin saklama sürelerinin yazılı olarak belirlendiği görülmektedir. Sadece dört KDB katılımcısı kullanıcı kayıtlarının bir yıl, beş yıl ya da mezuniyet sonrasında silineceğini belirtirken; diğer 11 KDB biriminde bu sürenin belirlenmemiş olması ve bir KDB katılımcısının kayıtların sonsuza kadar silinmeyeceğini

ifade etmesi dikkat çekicidir. Kullanıcı kayıtlarının, kullanıcının bilgi ve rızası olmaksızın sonsuza kadar saklanması ya da bu şekilde bir politikanın belirlenmesinin kişisel hakların ihlaline neden olabileceği düşünülmektedir. KDB birimlerinin verileri elektronik ortamda saklamalarının da bu konudaki belirsizliklerin oluşmasında etkili olduğu düşünülmektedir. Ancak bu durumda hukuksal olarak elektronik ortamda yer alan bilgilerin de yazılı-basılı ortamlarda bulunan bilgilerle aynı saklama ve koruma şartlarına sahip olması (T.C. Başbakanlık, 1988) ve aynı imha süreçlerinin uygulanması gerektiği göz ardı edilmektedir. Aynı hukuksal nitelikte olmasına karşın, elektronik bilgilerin saklanması ve imha koşullarının daha karmaşık olması ve Türk hukuk Mevzuatında bu konuya ilişkin yeterli düzeyde düzenlemelerin bulunmaması, konuyu daha karmaşık ve belirsiz hale getirmektedir. Bu belirsizliklerin giderilmesi için, bilgi merkezlerinde verilerin saklanmasına ilişkin hukuksal sorumlulukları içeren derslere lisans ve mesleki eğitim programlarında daha fazla yer verilmesi gerektiği düşünülmektedir.

Verilerin saklanmasına ilişkin hukuksal düzenlemelerin hangisinin ne ölçüde dikkate alınacağı konusunda da üniversiteler arasında görüş farklılıkları bulunmaktadır. İki PDB katılımcısı, vakıf üniversitesi olarak verilerin saklanma süreleri konusunda kendilerini sorumlu hissettikleri ya da takip ettikleri bir hukuksal düzenlemenin bulunmadığını belirtmişlerdir. Ancak vakıf üniversiteleri de Yükseköğretim Kurulu (YÖK) Mevzuatına tamamen bağlı ve bu konuda devlet üniversiteleri ile aynı koşul ve nitelikte üniversitelerdir. Bu nedenle, verilerin saklanması, arşiv hizmetlerinin yürütülmesi ve imha işlemlerine yönelik olarak hazırlanmış hukuksal düzenlemelerin gereğini vakıf üniversitelerinin de yerine getirme yükümlülükleri bulunmaktadır.

Üniversitelerin PDB ve KDB birimlerinde toplanan ve elektronik ortamda işlenen kişisel verilerin %72'sinin BİDB sorumluluğunda bulunması nedeniyle, üniversite BİDB'nin bu verilerin güvenliğinin sağlanması konusunda büyük sorumluluğu bulunmaktadır. Ancak araştırmada elde edilen bulgular, üniversitelerin tamamında bu verilerin sorumluluğunun nasıl paylaşılacağı konusunda yazılı politikaların bulunmadığını ve bu konuya ilişkin koordinasyonun yapılmadığını göstermektedir. Bu durum, herhangi bir veri ihlali olması durumunda birimlerin ihtilafa düşmesine neden olabileceği gibi, bilişim suçlarında çözüm ve sonuca ulaşmada en önemli unsurlardan biri olan zaman yönetim sürecini de olumsuz

etkileyebilecektir. Verilerin saklama ve işleme sorumluluklarının hangi birimlere ait olduğu, bilgi güvenliği politikalarında ve koordinasyon toplantılarında detaylı olarak belirtilmelidir. Ancak elde edilen bulgulara göre, üniversitelerde bu tür kapsamlı bilgi güvenliği koordinasyon toplantılarının yapılmasına ilişkin çalışmaların da bulunmadığı görülmektedir.

Üniversitelerde bilgilerin işlenmesinde elektronik ortamların kullanılma durumuna bağlı olarak, birimlerin veri saklama ve koruma tercihlerinde farklılıklar olabilmektedir. Bilgi merkezlerinin %73'ünün işlemlerini tamamen elektronik ortama taşıdıkları görülmektedir. Bu nedenle işlemlerini tamamen elektronik ortama taşıyan KDB birimlerinde, PDB birimlerinde olduğu gibi yazılı-basılı evrakların saklandığı korumalı ya da korumasız dolaplara ihtiyaç duyulmamaktadır. İki üniversitenin PDB biriminde ise EBYS kullanımına bağlı olarak yazılı-basılı belge sayısının önemli ölçüde azaltıldığı görülmektedir. Ancak katılımcıların görüşlerine bağlı olarak; bu sistemlerin henüz yeterli güveni sağlamadığı ve kâğıt kullanımının tamamen ortadan kalkmasının zaman alacağı düşünülmektedir. Henüz EBYS kullanmayan üniversitelerin de çoğunlukta olması, üniversitelerde alınan bilgi güvenliği önlemlerinin sadece elektronik belgelerle sınırlı kalmaması gerektiğini göstermektedir. Ayrıca, üniversitede EBYS'nin kullanılıyor olması da verilerin güvenli olarak işlenmesi, transferi ve saklanması için yeterli olmamaktadır. EBYS'nin üniversite birimleri tarafından kullanımına yönelik eğitimlerin verilerek farkındalığın oluşturulması ve veri erişimine yönelik yetkilendirmelerin yapılması da bu sürecin önemli bileşenleridir. Sadece bir üniversitede EBYS'nin üniversite birimlerinde amacına uygun olarak kullanılması ve buna ilişkin gerekli koordinasyonun sağlanması görevini üstlenen bir belge yönetim ve arşiv sistemi biriminin kurulmuş olduğu görülmektedir. Bir üniversitede de BİDB ile koordineli olarak birimlerde EBYS sorumlularının belirlenmiş olduğu görülmektedir. Üniversitelerde EBYS'nin amacına uygun ve güvenli olarak kullanımının yaygınlaşması için, olumlu örneklerin artması gerekmektedir.

Araştırma esnasında iki PDB katılımcısı, EBYS konusunda çok fazla yazılım seçeneği olmasına karşın; yazılımların herhangi bir standarda uyma zorunluluğunun bulunmaması, herhangi bir güvenlik denetiminden geçmemiş olması ve yazılımın satın alınması

sonrasındaki servis desteğine ilişkin güvensizlik gibi nedenlerden dolayı üniversitelerde EBYS kullanımına geçiş sürecinin yavaş ilerlediğini ifade etmişlerdir. Ancak Elektronik Belge Standartları hakkındaki 2008/16 Sayılı Genelge'de (T.C. Başbakanlık, 2008a), kamu adına görev yapan kurum ve kuruluşların oluşturacakları elektronik belge yönetim sistemlerinde TSE 13298 no'lu standarda göre işlem yapacakları ve genelgenin yayımı tarihinden önce kurulan sistemlerin ise ilgili kamu kurum ve kuruluşlarca gözden geçirilerek iki yıl içinde standarda uyumlu hale getirileceği belirtilmektedir. Farklı bir ifadeyle, TSE 13298 standardına uyum sağlamayan bir EBYS yazılımının üniversitelerde kullanılması mümkün değildir. Diğer üniversitelerde olduğu gibi EBYS'yi en yoğun olarak kullanan iki PDB katılımcısının, EBYS'nin sahip olması gereken standartlar ve güvenli kullanımı konusunda çekincelerinin bulunması, bu konudaki düzenlemeler hakkında bilgi sahibi olmadıklarını göstermektedir. Bu konuya ilişkin dikkate alınması gereken noktalardan bir diğeri de, bu çekinceler nedeniyle EBYS kullanımına geçiş sürecinin yavaş ilerlediğinin ifade edilmesidir. Bu nedenle EBYS için (araştırma kapsamındaki sadece iki üniversitede örneği bulunan) koordinatör birimlerin oluşturulması ve EBYS'nin güvenli kullanımına ilişkin tüm süreç hakkında üniversite birimlerinin bilgilendirilerek farkındalığın oluşturulması önem taşımaktadır.

Üniversitelerde işlenen personel verilerinin bütünlüğünün korunması, bilgi güvenliği önlemleri içinde en zor unsurlardan biri olarak görülmektedir. Bu konuda üniversite birimlerinin kendi çözümlerini geliştirdiği ya da herhangi bir çözüm geliştiremediği için endişe duyduğu görülmektedir. 12 BİDB ve PDB katılımcısı, sınırsız erişim yetkisi bulunduğu için BİDB personelini de iç tehdit unsurları arasında görmektedir. Üniversitelerin BİDB katılımcılarının da bu görüşe katılması ve endişenin yersiz olmadığını ifade etmesi önemlidir. Bu konuya ilişkin olarak üniversitelerde BİDB ve verileri işleyen diğer birimler tarafından bazı önlemler alınmıştır. Veri işlem kayıtlarının verileri işleyen ve verilerin kaydedildiği alandan sorumlu birimlerin takip edebileceği şekilde tutulması, birimler içinde sadece ilgili personele gerekli ölçüde erişim ve işlem yapma yetkisi verilmesi, periyodik olarak personelin kişisel bilgilerinin güncellenmesi, McCumber modelinde öngörülen karşılaştırmalı analiz, inkâr edememe ve kimlik doğrulama yöntemlerinin kullanımı uygulanabilir çözümler olarak değerlendirilmektedir. Bununla birlikte, üniversite birimlerinin BİDB tarafından yerine getirilmesini istediği

işlemleri “bilgi işlem yardım masasından” talep etmesi ve bu taleplerin kayıt altına alınması da geriye dönük takibin yapılabilmesinde kolaylık sağlayacaktır. Ayrıca, bilginin bütünlüğüne yönelik McCumber modelinde öngörülen güvenlik önlemlerinin uygulanması ve AB hukuk normları ölçüsünde gerekli sistem iyileştirmelerinin yapılması halinde; verilerin kriptolu olarak saklanabileceği, veri sahibinin dilediği zaman kendisi hakkındaki bilgilere ulaşmasının sağlanabileceği ve böylece kontrol mekanizmasının da oluşturulabileceği değerlendirilmektedir.

Üniversitelerde elektronik imza kullanımının yaygın olmadığı (%23,1) göz önüne alındığında, katılımcıların bu konuya ilişkin detaylı bilgiye sahip olmamaları normal karşılanmaktadır. Ancak araştırma esnasında elektronik imza kullanmadığını ifade eden üç PDB katılımcısının bulunduğu üniversitenin de Kamu Sertifikasyon Merkezi kayıtlarında aktif nitelikli elektronik sertifikaya sahip olduğu görülmektedir (TÜBİTAK UEKAE, 2014). PDB katılımcıların görüşme esnasındaki görüşlerine bağlı olarak; elektronik imza kullanımına ilişkin olarak verilen yanıtların, PDB katılımcılarının elektronik imzanın güvenilirliği konusundaki çekinceleri ve alışkanlıklarından vaz geçme zorluğu ile ilişkili olduğu düşünülmektedir. Ancak bir PDB katılımcısının EBYS’yi üniversitede en yoğun olarak kullanan birim olduklarını ifade etmesine karşın, elektronik imza kullanmadığını belirtmesi dikkat çekicidir. Çünkü elektronik imza kullanımı, amacına uygun ve güvenli olarak EBYS kullanımının ön şartı olarak görülmektedir. Elektronik imza uygulamasının araştırma kapsamında yer alan üniversitelerin %80’inde etkin bir güvenlik unsuru olarak kullanılması, mevcut şartlarda mümkün görülmemektedir. Özellikle personelin ayrılması sonrasındaki imza yetkilerinin düzenlenmesi konusunda, üniversite BİDB’nin ve sistemi kullanan diğer ilgili birimlerin temel sorumlulukları üstlenmesi ve sistem erişim yetkilendirmelerinin birim bazında yapılandırılmasının sağlanması gerekmektedir. Katılımcılardan alınan görüşler de dikkate alındığında; elektronik imza kanununa ilişkin endişelerin (Özdemirci, 2012) üniversiteler tarafından değerlendirilerek, bilgi eksikliğinin giderilmesi için yapılan çalışmaların arttırılması gerektiği düşünülmektedir.

5.4. KİŞİSEL VERİLERİN KULLANIMI VE PAYLAŞIMI

Araştırmadan elde edilen sonuçlara göre, üniversitelerde (%70) kişisel verilerin paylaşımı konusunda hassasiyet gösterildiği ve kişisel hakların gözetildiği görülmektedir. Ancak veri paylaşımına ilişkin olarak dikkati çeken en önemli nokta, bu hassasiyetin birim yöneticilerinin kişisel görüşlerini ve etik değerlere olan bağlılığını yansıtmasıdır. Üniversite tarafından belirlenmiş ya da hukuk kaynaklarında bu konuya ilişkin düzenlemelerin bulunmaması, kişisel görüş ve uygulamaların daha fazla öne çıkmasına neden olmaktadır. Bilgi paylaşımına ilişkin en büyük farklılık, savcılık tarafından istenen bilgilerin hangi silsile yoluyla iletileceği konusunda ortaya çıkmaktadır. Üniversitelerin genel olarak diğer karar alma süreçlerinde izlemiş olduğu otoriter tutum, bu konuda da aynı ölçüde etkili olmaktadır. Araştırmada bu konuya ilişkin görüşlerin alındığı PDB ve KDB birimleri içinde, nispeten daha az inisiyatifin kullanıldığı üç PDB ve beş KDB birimi, kişisel bilgilerin paylaşımına ilişkin tüm işlemlerin idari amirin onayı ile yapılabileceğini belirtmiştir. PDB ve KDB katılımcılarının %71'i, herhangi bir ihlal oluşması halinde veri sahibinin önlem alması gerektiğini ve kendisine bilgi verilmesinin önemli olduğunu düşünmektedirler. Ancak resmi başvurulara bağlı olarak yapılan tüm bilgi paylaşımlarının gizlilik nedeniyle veri sahibiyle paylaşılamayacağını düşünmektedirler. Bu açıdan bakıldığında da, katılımcıların durumun önem ve niteliğine bağlı olarak tercihlerini belirlemede tereddüt etmeyecekleri anlaşılmaktadır.

BEHK kapsamında KDB katılımcılarının sadece %20'sinin bilgilerin paylaşımı konusunda olumlu yanıt verdiği görülmektedir. Diğer KDB katılımcılarının bu kapsamdaki paylaşıma karşı olmalarının gerekçesi olarak, bilgi merkezlerinden istenilebilecek verilerin bulunmadığını belirtmeleri ise düşündürücüdür. Kullanıcı bilgilerinin diğer üniversite birimleri tarafından elde edildiği ya da merkezi veri depolama alanlarında saklandığı düşünülse dahi, bu bilgilerin bilgi merkezleri tarafından verilen hizmetler ile ilişkilendirilmesi yapılmaktadır. Bu koşullarda oluşturulan tüm yeni kayıtların bilgi merkezlerinin sorumluluğunda olduğu değerlendirilmektedir. Bilgi merkezlerinin BEHK kapsamında yapılacak başvurulara ilişkin olarak, gerekli idarî ve teknik önlemleri almak suretiyle Kanun'da belirtilen sınırlar içinde bilgi verme yükümlülükleri bulunmaktadır.

TCK'nın 136. maddesinde kişisel verilerin hukuka aykırı olarak başkasına verilmesi, yayılması ya da ele geçirilmesi suçlarına ilişkin düzenlenme yapılmıştır. Üniversitelerin BİDB, PDB ve bilgi merkezlerinde çalışan ve kişisel verilerin işlenmesinde görev alan personelin kişisel verileri hukuka aykırı olarak vermeleri de suçun nitelikli halini oluşturmaktadır. Ancak TCK'da yer alan kişisel verilerin "verilmesi" ya da "ele geçirilmesine" ilişkin düzenlemelerin de nasıl değerlendirileceği konusu yeterince açık değildir. Çünkü üniversitelerde kişisel verilerin işlendiği ve tamamı internete bağlı bilgisayarlar üzerinde gerçekleşen bu fiillere ilişkin kesin delillere ulaşılmasının mümkün olmayacağı değerlendirilmektedir. Üniversitelerde kişisel verilerin elde edilmesine ilişkin olarak, AB KVKK'de belirtildiği gibi veri sahibini güvence altına alan herhangi bir hukuksal düzenleme bulunmamaktadır. Böyle bir zorunluluğun olmaması nedeniyle, üniversite PDB ve KDB birimlerinin %93,3'ünde veri toplama esnasında veri sahibine elde edilen verilerin korunacağına ilişkin herhangi bir taahhütte bulunulmamaktadır. Bu nedenle, uygulamada verilerin korunması, sınırlı hukuksal düzenleme ve üniversitelerin dikkate almış oldukları etik değerlere bağlı olarak sağlanmaktadır. Ancak kişisel verilerin kullanımı ve paylaşımına ilişkin kuralların üniversite tarafından belirlenmesine ihtiyaç duyulmaktadır. Üniversite personeli ve öğrencilerin ilk kayıt ya da atama esnasında oluşturulan bilgi formlarının üçüncü kişilerle paylaşılmasına ilişkin onay alınmalı ve üniversite birimleri tarafından belirtilen şartlara uyulmalıdır. Bu kapsamda öğrenciler tarafından belirtilen şartların, öğrenci bilgilerinin aileleri ile paylaşımında da dikkate alınmasının gerektiği düşünülmektedir.

5.5. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN BİLGİ GÜVENLİĞİ ÖNLEMLERİ

Üniversite BİDB sorumluluğunda bulunan veri tabanları ve sunucu bilgisayarlar üzerinde bulunan kişisel veriler, mümkün olan en üst seviyede teknik önlemler alınarak korunmalıdır. Verilerin kötü amaçlı kişilerin eline geçse dahi gizliliğinin korunması önemlidir. Bunun en etkin yolu, McCumber bilgi güvenliği modelinde de belirtildiği gibi

verilerin kriptolanarak saklanmasıdır[130]. Mevcut durumda, üniversite bilgi işlem merkezlerinin %33,3'ünde sadece veri tabanı sisteminin sağlamış olduğu kriptolama işlemi ile sınırlı koruma sağlanmaktadır. Ancak araştırma esnasında üniversitelerde veri tabanında bulunmayan ve kişisel veriler içeren dosyalarında sayıca çok fazla olduğu bilgisi alınmıştır. Her ne kadar BİDB katılımcıları bu dosyaları da kriptolayarak saklama imkânlarının bulunduğunu belirtmiş olsalar da, bunun sağlanması için her üniversite birimi tarafından bir ön çalışma yapılması gerekmektedir. Çünkü üniversite birimleri elektronik depolama alanları üzerinde bulunan kişisel verileri diğer verilerden sınıflandırarak ayırmamaktadırlar. EBYS kullanımının üniversite birimlerinde yaygınlaştırılmasının da bu risklerin azaltılmasına katkı sağlayacağı düşünülmektedir.

Bilişim teknolojilerinin kullanımının üniversitelerde sayıca artması, doğrudan personel desteği gereken işlem ve denetimlerin zayıflamasına neden olmaktadır. Çok sayıda bilgisayar bulunan üniversitelerde oturum açma kayıtları gibi birtakım kayıtların incelenmesi ancak bir bilişim suçu gerçekleştiğinde yapılabilmektedir. Bununla birlikte, BİDB tarafından yapılacak bu tür inceleme ve denetimlerin sadece belirli idari birimlerde yapılması mümkün olabilmektedir. Özellikle domain yapısının kullanılmadığı üniversite akademik birimlerinde bu tür denetimlerin sağlanması "gereğinden fazla müdahale" olarak da algılanabilmektedir. Bu nedenle kullanıcı personelin farkındalığının arttırılması büyük önem taşımaktadır. Bunun için BİDB tarafından e-posta ile uyarılarda bulunulması, afiş ve ikaz notlarının kullanılması, toplantıların düzenlenmesi vb. yöntemler kullanılarak gerçekleştirilecek bilinçlendirme çalışmalarının mevcut risklerin azalmasında etkili olabileceği düşünülmektedir. Ayrıca, üniversite birimlerinde görevlendirilen bilgi işlem sorumluları ile BİDB arasında düzenli olarak iletişim sağlanması, güncel güvenlik önlemlerinin üniversite birimlerinde daha kısa sürede ve standart olarak uygulanmasına katkı sağlayacağı değerlendirilmektedir. Üniversitelerin %66,6'sında üst yönetim tarafından onaylanan ve birimlerin içeriği hakkında bilgi sahibi olmadığı ULAKBİM Kabul Edilebilir Kullanım Politikası sorumluluklarının da, bilgi işlem sorumluları aracılığıyla üniversite birimleri tarafından yerine getirilmesinin bilgi güvenliği önlemleri kapsamında gerekli olduğu düşünülmektedir.

[130] Detaylı bilgi için "2.2. Mccumber Bilgi Güvenliği Modeli Kapsamında Bilgi Güvenliği" isimli konuya bkz.

Bilginin durumuna (depolanma, transfer ve işleme) bağlı olarak karşılaşacağı risk seviyeleri ve alınacak güvenlik önlemleri farklı olabilmektedir. Bu nedenle, uygulanacak olan bilgi güvenliği önlemlerinin belirlenmesinde, bilginin içinde bulunduğu durum göz önüne alınmalıdır. Araştırmadan elde edilen verilere bağlı olarak; üniversitelerin tamamında teknik bilgi güvenliği önlemlerinin BİDB tarafından ihtiyacı karşılayacak en üst seviyede alındığı söylenebilir. Ancak araştırma kapsamında yer alan üniversitelerin tamamında, McCumber modelinin önemli bileşenlerinden biri olan ve AB ülkeleri üniversitelerinin web sayfaları üzerinden yapılan ön araştırmada da uygulandığına dair bulgular elde edilen "idari önlemlerin" ihmal edildiği görülmektedir. Türkiye'deki üniversitelere ilişkin web sayfaları üzerinden yapılan ön araştırmada elde edilen bulgularda da bu eksiklik görülmektedir. İdari önlemlerin alınmaması bilgi güvenliğinin sağlanması açısından olumsuz etki yarattığı gibi, bireylerin kişisel hak ve özgürlüğünün korunması konusunda da eksikliklere neden olmaktadır. BİDB tarafından alınan teknik önlemlerle, verinin gizliliğinin sınırlı olarak (kişilik hakları göz ardı edilerek) korunması sağlanabilmektedir. Bu yaklaşım, Whitman ve Mattord tarafından dikkat çekilen kişilik haklarının korunması ile bilginin gizliliğin korunması arasındaki bağın kurulamamasına (Whitman ve Mattord, 2011) ve alınan önlemlerin bir yönünün zayıf kalmasına neden olmaktadır. Teknik önlemlerin yanı sıra alınacak idari önlemlerin, tüm üniversite birimlerinde uygulanabilir genel güvenlik unsurlarını içerecek ve kişisel hakları koruyacak nitelikte olması gerekmektedir. Bu nedenle bilgi güvenliği konusu sadece BİDB'nin sorumluluğu olmanın ötesinde, üniversite üst yönetimi tarafından da ele alınması gereken konular arasında yer almalıdır. Üniversite üst yönetiminin yanı sıra, üniversite birimlerindeki yöneticilerin de etik ilkeler konusunda bilgi birikimlerinin olması ve kişisel verilerin korunmasına yönelik denetimlerde bulunmalarının süreci olumlu etkileyeceği düşünülmektedir. Üniversite üst yönetimi tarafından bilgi güvenliği konusunda gerekli adımların atılabilmesi için, her üniversitede koordinasyon görevini de üstlenecek bir bilgi güvenliği kurulunun oluşturulmasının önemli katkılar sağlayacağı ve üniversite içinde bilgi güvenliği kültürünün bu kurul aracılığıyla daha hızlı yaygınlaştırılabileceği düşünülmektedir.

Araştırmada üniversite BİDB katılımcılarının vermiş olduğu bilgiler; üniversitelerde de kapsamlı bir denetleme yapılması halinde, DDK tarafından çeşitli kurumlarda yapılmış

olan denetlemelerde elde edilen sonuçların (DDK, 2013) benzeriyle karşılaşılabileceğini göstermektedir. Üniversitelerde ve diğer kamu kurumlarında bilgi güvenliği ve kişisel verilerin korunmasına ilişkin denetimlerin yapılması kadar, bu denetimlerin standart olması ve gizliliğe önem verilmesi de önem taşımaktadır. Bu nedenle, üniversitelerde yapılacak bilgi güvenliği denetimleri; uluslararası standartlar, hukuksal düzenlemeler ve evrensel bilgi güvenliği ile kişisel verilerin korunmasına ilişkin temel ilkeler çerçevesinde oluşturulmuş bilgi güvenliği politikaları dikkate alınarak, kamu kaynaklı denetim kurumları tarafından ya da iç denetim şeklinde yapılmalıdır. Denetim sürecine ilişkin olarak, DDK raporlarında da önerildiği gibi (DDK, 2013) üniversitelere yönelik olarak güvenlik testi standardının geliştirilmesi ya da üniversitelerde oluşturulacak kapsamlı bilgi güvenliği politikaları çerçevesinde düzenli olarak yapılacak iç denetimler, kritik açıkların kapatılmasına ve farkındalığın oluşmasına katkı sağlayacaktır.

Verilerin korunmasına ilişkin hukuksal sorumluluklara bakıldığında; üniversitede personel kayıtlarının ve bilgi merkezlerinde bulunan kişisel verilerin korunmasıyla ilişkili olarak, veriyi işleyen personelin bu verileri koruma sorumluluğunu içeren düzenlemenin TCK'nın 258. Maddesi[131] ile yapıldığı görülmektedir. Kişisel verileri işleyen personelin görevi nedeniyle edindiği bilgilerin gizli kalmasını ve yetkisiz kişilere verilmemesini öngören bu madde ile kişisel veriler için dolaylı olarak koruma sağlanmaktadır. Ancak hukuksal sorumluluklara ilişkin güvenlik önlemlerinin eğitim ve farkındalığın oluşturulması ile sağlanabileceği değerlendirilmektedir. Üniversite birimlerinde kişisel verileri işleyen personelin seçilmesi de personel güvenliğiyle ilişkili olarak kişisel verilerin korunması sürecinin içinde yer almaktadır. Özellikle vakıf üniversitelerinde devlet memuru olmanın beraberinde getirdiği hukuksal sorumlulukları taşımayan personelin seçimi ve sözleşme içeriğinin hazırlanması büyük önem taşımaktadır. Personel ile yapılan sözleşmelerde kişisel verilerin korunması ve bu konuda ihlallerin olması halinde uygulanacak yaptırımlara yer verilmesinin, personel kaynaklı bilgi güvenliği risk ve zafiyetlerini büyük ölçüde ortadan kaldıracağı düşünülmektedir.

[131] **TCK, 258. Madde:** (1) Görevi nedeniyle kendisine verilen veya aynı nedenle bilgi edindiği ve gizli kalması gereken belgeleri, kararları ve emirleri ve diğer tebligatı açıklayan veya yayınlayan veya ne suretle olursa olsun başkalarının bilgi edinmesini kolaylaştıran kamu görevlisine, bir yıldan dört yıla kadar hapis cezası verilir.
(2) Kamu görevlisi sıfatı sona erdikten sonra, birinci fıkrada yazılı fiilleri işleyen kimseye de aynı ceza verilir.

5.6. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ÖNLEMLERİN STANDARTLAR VE YASALARA UYUMLULUĞU

10 üniversitenin BİDB sorumluluğunda olan veri tabanlarının ve bilgi sistemlerinin, her ne kadar düzenli ve planlı olmasa da güvenlik kontrol ve denetimlerinin kişisel verilerin de dikkate alınarak yapıldığı görülmektedir. AB KVKK'de de belirtilen "kişisel verilerin sistem güvenlik testinde kullanılmaması" konusunda BİDB katılımcılarının %86,7'sinin duyarlı olması ve veri tabanı üzerinde birim bazında ayrılmış olan kişisel verileri diğer verilerle aynı işlem sürecinden geçirmemeleri, BİDB birimlerinde kişisel verilere ve kişisel haklara gösterilen özeni ortaya koymaktadır. Ancak bu işlem, diğer üniversite birimlerinin verileri sınıflandırma konusunda göstermiş olduğu hassasiyet ile de ilişkilidir. Araştırma verilerine göre; üniversite birimleri tarafından verilerin sınıflandırılması halinde, BİDB tarafından bu verilerin farklı fiziksel ortamlar ya da farklı sanal ağlar kullanılarak diğer verilerden ayrılmasının da imkân dâhilinde olduğu görülmektedir. Kişisel verilerin diğer verilerden farklı sanal ağlar ya da veri depolama alanlarında bulunması, yetkisiz erişimlere karşı alınabilecek önlemler arasında ilâve maliyet gerektirmeyen ve en etkili uygulama yöntemlerinden biridir. Araştırmalar (Wolf ve diğerleri., 2011); maliyeti düşük ve etkinliği yüksek teknik önlemlerin öncelikli olarak alınması gerektiğini göstermektedir. Örneğin üniversitede kişisel verilerin kaydedildiği bilgi sistemlerinin mevcut altyapı üzerinde değişiklik yapılmaksızın (sanal ağlar ile) birbirinden ayrılması sağlanabiliyorsa, bu konuda hukuksal düzenlemelerin yapılması ya da tüm personelin bilinçlenmesi beklenmemelidir. Kontrol ve denetimlerin sadece sistemi tasarlayan ve yöneten kişiler tarafından yapılması, düzensiz aralıklarla yapılan işlemlerin kayıtlarının tutulmaması ve bazı üniversitelerde veri tabanları üzerinde kişisel veriler sınıflandırılmadığı için işlem sürecinde bu verilerin de kullanılması ise, bu konuda iyileştirilebilecek noktalar olarak göze çarpmaktadır.

Sistemi tasarlayan ya da yöneten kişilerin, sistemin açıklarını görememe olasılıklarının bulunması göz önünde tutulurken; dokuz BİDB katılımcısının bu tür sistemlerin denetim ve kontrollerini yaparak rapor sunabilecek kurumsal ve güvenilir kaynakların bulunmadığı yönündeki ifadeleri de dikkate alınmalıdır. Bu nedenle, denetim ve kontrol konusundaki eksikliklerin giderilmesi için, BİDB birimlerinin kendi personeli ile imkân

ve sınırları zorlaması dışında seçeneğinin olmadığı düşünülmektedir. Bununla beraber, iki üniversite dışında birimlerde yer alan bilgi sistemleri bu denetimlerin dışında kalmaktadır. Üniversitelerin PDB ve KDB birimlerinde de (sırasıyla %21,4 ve %33,3) üzerinde kişisel verilerin bulunduğu ve bu birimler tarafından işletilen sunucular bulunmaktadır. Üniversite birimlerinin %26'sında merkezi veri tabanlarına aktarılmayan bilgilerin bulunduğu bilişim sistemlerinin zincirin zayıf halkası olduğu düşüncesi tartışmaya açılarak, alınan önlemler içerisinde bu sistemler de göz önünde bulundurulmalıdır. Ayrıca üniversite birimlerinin tüm verileri merkezi sisteme aktarma çalışmaları devam ederken, araştırma bulgularına bağlı olarak PDB ve KDB birimlerinde kişisel verilerin işlendiği bilgisayarlar üzerinde de bu tür bilgileri içeren dosyaların olduğu bilinmektedir. Bu bilgisayarların denetimlerinin yapılması ya da kullanıcılarda farkındalığın arttırılmasının, birimlerde görevlendirilecek bilgi işlem sorumluları ile sağlanabileceği değerlendirilmektedir. Ancak her ne kadar birimlerde görevlendirilecek bilgi işlem sorumluları tarafından sistem güvenlik güncellemeleri BİDB ile koordineli olarak yürütülse de; denetim faaliyetlerine ilişkin olarak üniversite üst yönetiminin de sürece dâhil olmasını sağlayacak bir bilgi güvenliği kurulunun koordinatör olarak görev alması önem taşımaktadır. Üniversite birimlerinin mevcut şartlarda bilgi güvenliği açısından değerlendirmesinin yapıldığı çalışmalar bulunmamaktadır. Ancak bu çalışma kapsamında elde edilen verilere dayanarak, üniversite birimlerinde yapılacak denetim ve kontrollerde, diğer devlet kurum ve kuruluşlarında yapılan denetimlerde elde edilen sonuçlarla karşılaşma olasılığının bulunduğu söylenebilir[132].

Üniversite BİDB tarafından alınan bilgi güvenliği önlemleri, büyük ölçüde McCumber bilgi güvenliği modelinin teknik önlemleri içeren bölümünü adreslemektedir. Araştırma esnasında BİDB katılımcılarının %80'i, almış oldukları önlemlerin hukuksal dayanağının bulunmadığını ifade etmektedirler. Kişisel verilerin korunmasına ilişkin yönleriyle, bu konunun BİDB birimlerinin eksikliği ya da hukuksal düzenlemelerdeki eksikliklerle ilişkilendirerek tartışılması mümkündür. Ancak yaptığımız çalışma sonucuna göre, bu konudaki eksikliklerin her iki boyutunun da değerlendirilmesi gerektiği düşünülmektedir. BİDB, PDB ve KDB katılımcılarının %77'si, hukuksal düzenlemeler içinde bilgi

[132] Detaylı bilgi için "2.4.5. Kişisel Verilerin ve Bilgi Güvenliğinin Sağlanmasına İlişkin Denetim ve Koordinasyon Sisteminin Geliştirilmesi" isimli konuya bkz.

güvenliğinin sağlanmasına dayanak oluşturacak maddelerin çok dağınık olduğu ve bu nedenle konuya ilişkin çalışmalara ihtiyaç duyulduğu görüşünü öne sürmektedirler. Türk Hukuk Mevzuatında yer alan hukuksal düzenlemelerin üniversite BİDB tarafından incelenerek alınan teknik önlemlerin bu düzenlemelere dayandırılabilmesi için, konuya ilişkin uzman görüşünün de alınarak çalışma yapılması gerekmektedir. Çünkü 5651 Sayılı Kanun dışındaki hukuksal düzenlemelerde, kişisel verilerin korunmasına yönelik noktalara sınırlı ve dağınık olarak değinilmektedir. Öte yandan, katılımcılar tarafından hukuksal düzenlemelerin içeriğinin incelenmemiş olması önleyici tedbirlerin alınmasına yönelik eksiklik oluşturmamaktadır. Çünkü Türk Hukuk Mevzuatında yer alan düzenlemeler BİDB tarafından uygulanan önleyici tedbirlere yönelik olarak değil, gizliliğin ihlali sonrasında atılacak adımlara ilişkin hususları içermektedir.

Hukuksal düzenlemelerin yanı sıra üniversite birimlerinin dikkate aldıkları mesleki etik ilkeler bulunmaktadır. Ancak özellikle BİDB ve PDB katılımcılarının dikkate almış olduklarını belirttikleri üniversite etik ilkeleri ya da mesleki etik ilkelerinin içeriğinde kişisel verilerin korunmasına ilişkin hususların ne kadar belirgin ve yeterli olduğu tartışmalıdır. Kişisel verilerin korunmasına yönelik hukuksal düzenlemelerin yetersizliği göz önüne alındığında, mesleki etik kurallara olan ihtiyacın önemi daha fazla anlaşılmaktadır. Mesleki etik kurallarının yabancı hukuk mevzuatlarının ve etik kurallarının da dikkate alınarak oluşturulması, güncellenmesi ve belirli bir mesleki gruba duyurularak hayata geçirilmesinin hukuksal düzenlemelerden daha hızlı ve etkin olabileceği düşünülmektedir. Her ne kadar kişisel verilerin korunması ve bilgi güvenliğinin sağlanmasına yönelik yeterli düzeyde içeriğe sahip olmasa da, katılımcıların bu konulara ilişkin olarak mesleki etik ilkeleri takip ettiklerini belirtmeleri ve özellikle KDB katılımcılarının %45,5'inin etik ilkeleri hukuksal eksikliklerin giderilmesi için ikinci öncelikli kaynak olarak nitelendirmeleri önemlidir. Bu nedenle, hukuksal düzenlemelerin yetersiz kaldığı kişisel verilerin korunmasına ilişkin konulara mesleki etik ilkeleri içerisinde daha geniş yer verilmesinin uygulamaya yönelik önemli katkılar sağlayacağı değerlendirilmektedir.

5.7. KİŞİSEL VERİLERİN DEPOLANMASI VE KORUNMASINA İLİŞKİN SORUMLULUKLAR

Üniversite BİDB birimlerinin %60'ında bilgi güvenliğinin sağlanmasına yönelik olarak personel görevlendirilmemesi, bilgi güvenliğine yönelik politika ve eylem planlarının geliştirilmesinin ikinci planda kalmasına neden olmaktadır. Bununla beraber, personel yetersizliği nedeniyle bilgi güvenliğinin sağlanmasına ilişkin sorumlulukların bir personele ek görev olarak verildiği BİDB birimlerinde, bu konuya yönelik sorumlulukları üstlenen personelin %83,3'ünün uzmanlık alanının farklı olduğu görülmektedir. Sorunun temelinde üniversite BİDB birimlerinde bilgi güvenliğinin sağlanmasına ilişkin bir personel kadrosunun bulunmamasının olduğu düşünülmektedir. Özellikle vakıf üniversitelerinde personel eksikliğinin daha fazla olduğu görülmektedir. Devlet ve vakıf üniversitelerinde bilgi güvenliği önlemlerinin alınmasına ilişkin en büyük farklılık, iş yüküne oranla personel sayısının yeterliliği konusunda görülmektedir. Vakıf üniversitelerinin %90'ında personele birden fazla sorumluluk verilmesi nedeniyle, BİDB'de özel olarak bilgi güvenliği konusunda uzman personelin görevlendirilmesi ikinci planda kalmaktadır. Bilgi güvenliği politikalarının geliştirilmesi ve bu politikalara uygun önleyici tedbirlerin alınması uzmanlık ve bilgi birikimi gerektiren konulardır. Bu nedenle, üniversitelerde bu görev ve sorumluluğu üstlenen birimlerde görevli personelin uzmanlık alanına göre çalıştırılması önem taşımaktadır.

Araştırma verilerine göre, üniversitelerin büyük bölümünde (%73,3) üst yönetimin bilgi güvenliğinin sağlanmasına önem verdiği ve donanımsal gereksinimleri ivedilikle karşıladığı görülmektedir. Ancak bu bulgular sadece BİDB katılımcılarının bu konuya ilişkin beklentileri ve bu beklentilere karşılık olarak alınan sonuçları göstermektedir. BİDB birimlerinin %93,3'ünde bilgi güvenliğine ilişkin personel kadrosunun bulunmaması ve bilgi güvenliğine ilişkin idari önlemlerin alınacağı üniversite politikalarının bulunmaması da üniversite üst yönetiminin konuya ilişkin tutumunu yansıtmaktadır. Üniversitelerin yarısında (%46,7) bilgi güvenliği sorumluluğunun birimler arasında paylaşılmadığı, %60'ında bilişim faaliyetlerini düzenleyen bilişim komisyonunun bulunmadığı ya da gündem maddeleri arasında kişisel verilerin korunmasına yönelik önlemlerin bulunmadığı, üniversite birimlerinin %66,7'sinde

bilişim sorumlularının bulunmadığı ve üniversitelerin %73,3'ünde personelin görev tanımında kişisel verilerin korunması ve saklanmasına ilişkin sorumlulukların yer almadığı görülmektedir. Tüm bu eksikliklere ilişkin olarak; üniversite üst yönetiminin bilgi güvenliğinin sağlanmasına yönelik olarak alınacak önlemlere yeterince katkıda bulunmamalarının da payı olduğu düşünülmektedir. Araştırmadan elde edilen veriler; üniversitelerin %73,3'ünde üst yönetimin de BİDB'yi bilgi güvenliği konusunda tek yetkili ve sorumlu birim olarak gördüğü ve alınacak önlemlerin teknik uygulamalarla sınırlı olduğunu düşündüğünü göstermektedir.

Araştırma sonucunda elde edilen verilere göre, üniversitelerde BİDB dışındaki birimler sadece birim içinde sunucu bilgisayarların olması durumunda kişisel verilerin korunmasına ilişkin teknik önlemlerin alınması konusunda sorumluluklarının olduğunu düşünmektedirler. Oysa merkezi denetim ve kontrollerin yapılamadığı ve birimlerde bilgi işlem sorumlularının bulunmadığı üniversitelerin %80'inde, bireysel olarak da birtakım sorumlulukların üstlenilmesi gerekmektedir. Örneğin temel güvenlik önlemleri arasında yer alan anti virüs korumasının sağlanması, sistem güvenlik güncellemelerinin yapılması, kullanıcı hesabına ilişkin işlemler (şifre vd.), kişisel verilerin işlendiği bilgisayardaki sistem ve yazılım olay kayıtlarının tutulması ve BİDB ile koordineli olarak veri yedeklerinin alınması başlıca kullanıcı sorumlulukları arasında yer almaktadır. Bununla birlikte, üniversite birimlerinde kişisel verilerin işlendiği bilgisayarlar üzerinden yapılan erişimlerle, tüm güvenlik duvarlarının aşılması ve istenilen bilgilerin elde edilmesi mümkün olabilmektedir. Araştırma verileri, kişisel verilerin işlendiği yazılımların, yedekliliğin de sağlanması amacıyla birim içindeki tüm bilgisayarlara yüklendiğini göstermektedir. Veri tabanlarına erişim imkânı sağlayan yazılımların yüklü olduğu her bilgisayarın birim içindeki riskleri arttırması nedeniyle, sadece ihtiyaç duyulan bilgisayarlara yazılımların yüklenmesi önerilmektedir. Ayrıca, bu bilgisayarların kötü amaçlı kişiler tarafından uzaktan erişim aracı olarak kullanılma risklerinin azaltılabilmesi için, sistem güvenlik yamalarının güncellenmesi ve güvenlik duvarının etkinleştirilmesi gibi temel teknik önlemlerin alınması da önem taşımaktadır.

Üniversitelerin tamamında merkezi olarak BİDB sorumluluğunda bulunan verilerin yedeklenmesi konusunda profesyonel ve ihtiyaçlara cevap verecek nitelikte

uygulamaların bulunduğu görülmektedir. Verilerin yedeklenmesi, her sistemin bir gün mutlaka faaliyet dışı kalabileceği düşüncesine bağlı olarak, en önemli bilgi işlem sorumlulukları arasında yer almaktadır. McCumber bilgi güvenliği modelinde de bilginin kullanılabilirliğinin, erişim kolaylığının ve sürekliliğinin sağlanması açısından verilerin yedeklenmesi işleminin özel bir yeri bulunmaktadır. Yedekleme işlemlerinin sık aralıklarla yapılması, herhangi bir veri ihlali ya da yetkisiz erişim sonrasında verilerin mümkün olan en son bozulmamış haline ulaşabilmeyi sağlamaktadır. Bu nedenle özellikle ödünç verme kayıtları gibi anlık değişim gösteren üniversite bilgi merkezi verilerinin sık aralıklarla yedeklenmesi önem taşımaktadır. Üniversite BİDB sorumluluğunda bulunan verilerin belirli bir yazılı yedekleme planı çerçevesinde yapılması ve yedekleme kayıtlarının tutulması ise, bilişim suçları ile mücadele ve adli işlemler esnasında üniversite için önemli başvuru kaynakları sağlayacaktır. Üniversitelerde merkezi veri depolama ünitelerinin yedeklenmesi konusunda sistem donanımı ve personelin bilinçliliği açısından endişe duyulacak eksiklikler bulunmazken; üniversite birimlerindeki bilgisayarlar üzerinde bulunan verilerin nasıl ve kimin sorumluluğunda yedekleneceğine ilişkin belirsizlikler bulunmaktadır. Bu belirsizliklerin ortadan kaldırılabilmesi için, üniversitenin kurumsal bilgi güvenliği politikasına bağlı olarak tüm üniversite birimleri için veri yedekleme politikalarının geliştirilmesi ve birimlerin bilgi işlem sorumluları tarafından veri yedekleme faaliyetlerinin yürütülmesi sağlanmalıdır.

Araştırmadan elde edilen sonuçlara göre, üniversite birimlerinin sadece %40,25'inde olası ihlallere karşı uygulanacak yaptırımların belirlendiği görülmektedir. Bununla beraber, yaptırımların belirlenmiş olduğu üniversitelerde; yazılı ya da sözlü uyarı, disiplin soruşturmaları ve cezaları, idari para cezası ve işten uzaklaştırma gibi yaptırımların uygulanabileceği ifade edilmektedir. Bu yaptırımların bir personelin kişisel verisinin açığa çıkması ya da kötü amaçlı olarak kullanılması karşısında ne kadar yeterli ve etkili olacağı tartışmalıdır. Ancak Türk Hukuk Mevzuatı incelendiğinde, kişisel verilerin korunması konusunda önleyici tedbir olarak tanımlanabilen ve üniversiteler tarafından uygulanabilecek farklı yaptırımların da bulunmadığı görülmektedir. Hukuksal düzenlemelerin bilgi depolama yöntemleri ve bilgi sistemlerindeki gelişimin gerisinde kalması nedeniyle, AB 2010 yılında yeni bir veri koruma direktifi üzerinde çalışmaya

başlamış ve geçen süre içinde alınan kararlarla ilerlemeler sağlamıştır. Bu nedenle, üniversitelerde kişisel verilerin depolanması ve korunmasına ilişkin politikalar geliştirilirken, AB'nin mevcut veri koruma direktifi üzerinde yapmış olduğu reform çalışmalarının da dikkate alınmasının faydalı olacağı değerlendirilmektedir.

5.8. RİSK FAKTÖRLERİ, RİSK YÖNETİMİ VE ALTERNATİF PLANLAR

Her kurum ve kuruluşun alabileceği risklerin boyutu ve türleri farklıdır. Ancak hassas ve kişisel verilerin korunması söz konusu olduğunda, bu tür verilerin kötü amaçlı kişiler tarafından ele geçirilmesi halinde dahi özel hayatın gizliliğinin korunması öncelikli ortak hedefler arasında bulunmaktadır. Bu nedenle planlama aşaması içinde yer alan bilgi güvenliği politikalarının da oluşturulduğu süreçte korunan bilgi varlığının niteliğinin göz önüne alınması, tüm sürecin doğru işlemesinin ön şartıdır. Bilgi güvenliği yaşam döngüsünün üniversitelerde kişisel verilerin korunmasına yönelik olarak uygulanması, sürekliliğin sağlanması açısından önemlidir. Bu süreç, üniversitelerin bilgi varlıklarını ve önemini fark etmelerine de katkı sağlamaktadır. Bununla beraber, kontrol etme ve önlem alma süreçlerinin uluslararası bilgi güvenliği standartları ve McCumber modelinde yer alan bilgi güvenliği önlemleri çerçevesinde kapsamlı olarak ele alınmasıyla, sürecin etkinliğinin arttırılabileceği değerlendirilmektedir.

Üniversitelerde veri tabanlarına yönelik olarak yapılan iç ve dış saldırıların yoğunluğu (%64,3), tüm kurum ve kuruluşlar gibi üniversitelerin de risk ve siber tehdit altında olduğunu göstermektedir. Bununla birlikte, kişisel verilerin işlendiği üniversite birimlerindeki bilişim sistemlerinin hemen hemen tamamının (%93,1) internete bağlı olarak çalışması risk oranını arttırmaktadır. Buna karşın, büyük bölümünde (%60) bilgi varlıklarının değerlendirmesi yapılmayan, risk analiz raporu bulunmayan ve yazılı eylem planı olmayan üniversitelerin risk ve tehditler karşısında sistematik olarak mücadele edebilme gücünün bulunmadığı değerlendirilmektedir. Üniversitelerde risk değerlendirmesinin yapılmış olması da tek başına yeterli olmamaktadır. Elde edilen ve korunan bilgiler için yapılan risk değerlendirmesi sık aralıklarla güncellenmediği sürece, geliştirilen ya da uyarlanan bilgi güvenliği politikalarının da zaman içerisinde bilgi güvenliğini sağlamada yetersiz kalacağı düşünülmektedir.

Araştırmadan elde edilen bulgulara göre, üniversitelerin %86,6'sında ISO 27001 gibi risk analizine yönelik standartların gerektirdiği koşulları sağlamanın ve bunu muhafaza etmenin zor olduğu görülmektedir. Çünkü bu tür standartların içeriği ile üniversitenin özünde yer alan ve akademik birimlerde daha fazla görülen esnek çalışma şartları tam olarak örtüşmemektedir. Diğer taraftan bu tür standartların sadece idari birimlerde sağlanması da gerekli sertifikasyon süreci için yeterli olmamaktadır. Araştırmadan elde edilen veriler, üniversitelerde risk yönetimine ilişkin bu tür standartların satın alınması yerine; içeriğinin alınması, değerlendirilmesi ve üniversiteye uyarlanmasıyla daha verimli sonuçların alınabileceğini göstermektedir. ISO 27001 gibi uluslararası standartlar, risk analizi yapılmamış üniversitelerde analizin yapılması ve raporlandırılması işlemleri için de rehber niteliği taşımaktadır. Risk analizinin yapılması ve raporlandırılması, olası felaketlerde ya da veri ihlalinde uygulanacak eylem planının oluşturulması için de temel teşkil etmektedir. Üniversitelerin birçoğunda (%86,6) bu tür eylem planlarının olmadığı görülmektedir. Bu nedenle büyük tehdit ve saldırılar karşısında teknik işlemlerin dışında atılması gereken adımların (adli işlem süreci vb.) doğru sırayı takip etmesinde sorunların yaşanabileceği değerlendirilmektedir.

Höne ve Eloff'un belirttiği gibi, organizasyonlar için en önemli ve aynı zamanda yazılması zor dokümanlardan biri olan bilgi güvenliği politikalarının geliştirilmesi esnasında faydalanılan ve referans gösterilen öncelikli kaynaklar arasında uluslararası bilgi güvenliği standartları da yer almaktadır (Höne ve Eloff, 2002). Ancak her üniversitenin kendi özel yönetim ve denetim sistemi olması nedeniyle, üniversitelerin geliştirecekleri bilgi güvenliği politikalarının yerini alması mümkün değildir. Ayrıca devlet üniversiteleri, kamu kurum ve kuruluşlarının dışarıdan yapılacak denetimlerinin, veri koruma kanunu ile kapsamı belirlenerek devletin denetiminde ve bağımsız bir denetim mekanizması ile yapılması gerekmektedir. HKSAR'nin (Hong Kong Special Administrative Region) bilgi güvenliği standartlarına ilişkin raporunda belirtildiği gibi; uluslararası standartların üniversite yapısıyla örtüşen bölümlerinden uyarlanarak geliştirilen bilgi güvenliği politikalarının, bilgi sistem yöneticileri ve tüm kullanıcıların katılımıyla uygulanarak bilgi güvenliği kültürü oluşturulması halinde, bilgi güvenliğinin sağlanmasına yönelik katkısının daha fazla olacağı düşünülmektedir (HKSAR, 2008).

Bilgi sistemleri yönetiminde risklere ilişkin olarak göz önünde bulundurulan ve genel kabul gören düşünce; her sistemin bir gün tehditler, yetkisiz erişimler, yazılım hataları ya da donanım ömrünün tamamlanması nedeniyle kullanım dışı kalabileceğidir. Bu nedenle bilgi işlem merkezleri olası felaketlerin önüne geçilemediği durumlarda, mümkün olan en az zararla sistemi yeniden aktif hale getirmeyi amaçlamaktadırlar. Üniversite bilgi işlem merkezlerinin tamamında mevcut risklerin göz önünde bulundurulmuş ve olası felaketlerde sistemi en geç 24 saat içerisinde yeniden aktif hale getirebilecek önlemlerin alınmış olması, risk ve tehditlere karşı önemli bir aşamanın kat edildiğini göstermektedir. Ancak olası felaketlere karşı üniversite birimlerinde ise aynı ölçüde önlemlerin alındığını ve kaybolan verinin telafisinin olabileceğini söylemek güçtür. Araştırma kapsamında yer alan ve kendi sunucularını işleten sekiz üniversite biriminin (üç PDB ve beş KDB) altısında veri yedekleri alınırken; birim içinde bulunan ve üzerinde kişisel bilgilerin de tutulduğu bilgisayarların veri yedeklerinin alınmadığı görülmektedir. Bu nedenle üniversite birimlerinde işlenen verilerin merkezi veri depolama birimlerine aktarılmasının, veri güvenliği ve yedekliliğinin sağlanması açısından da önem taşıdığı düşünülmektedir.

Üniversitelerde veri güvenliğinin sağlanmasına ilişkin önemli risk unsurlarından biri de dışarıdan teknik destek alınma sürecidir. Yaptığımız çalışma sonuçlarına göre, bilgisayar sayısının çok fazla olduğu ve bilgi işlem personelinin yetersiz kaldığı üniversitelerde dışarıdan teknik destek alınmasının zorunlu hale geldiği görülmektedir. Ancak bu desteğin alınmasına ilişkin olarak belirlenen şartlar, üniversitenin bilgi güvenliğine ilişkin risk düzeyini doğrudan etkilemektedir. Üniversitelerin %80'inde merkezi sistemlerin bakım ve onarım ihtiyaçları için dışarıdan destek alınmamaktadır. Ancak merkezi sistemler için dışarıdan destek alan üniversiteler için bu desteğin gözetim altında alınması ve yüklenen her yazılımın kontrol edilmesi hayati önem taşımaktadır. Araştırma verileri, dışarıdan destek alınan üniversitelerde, teknik desteğe ihtiyacı olan birimlere BİDB tarafından anlaşma yapılan firmaların doğrudan yönlendirilebildiğini ya da üniversite birimleri tarafından zaman zaman ilgili firmalar ile iletişim kurularak teknik destek alınabildiğini göstermektedir. McCumber modelinde önemle vurgulanan ve bilgi güvenliğinin tamamlayıcı unsurlarından biri olan kullanıcı bilinçliliğinin arttırılması

unsurunun önemi, üniversite birimlerinin doğrudan dışarıdan destek alması gibi durumlarda daha fazla hissedilmektedir. Bu konuya ilişkin sadece üniversite idari birimleri tarafından değil, öğretim elemanları tarafından da hassasiyet gösterilmesi önem taşımaktadır. Zira öğretim elemanlarının kullanmış olduğu bilgisayarların veri depolama birimlerinde de üzerinde uzun süre çalışılan patent, proje, tez, makale, kitap vd. korunmaya değer belgeler bulunabilmektedir. Dışarıdan teknik destek alan üniversite birimlerinin, her ne kadar ilgili firmalar ile belirli sözleşmeler yapılmış ve güvenlik araştırmaları yapılmış olsa da, veri güvenliğinin sağlanmasına ilişkin risk ve sorumluluğu ortadan kalkmamaktadır. Teknik destek alan üniversite birimlerinin, ilgili firmaların yaptığı tüm işlemleri kontrol etme yükümlülüğü bulunmaktadır. Bu nedenle, yazılım problemlerinin yerinde ve kullanıcı gözetiminde giderilmesi önem taşımaktadır. Bilgi sistemlerinde donanım problemlerinin olması ve sorunun yerinde giderilememesi halinde ise, verilerin işlendiği sabit disklerin sökülerek dışarıdan teknik destek sağlayan şirkete verilmemesi önem taşımaktadır. Bu hususların ve ilâve olarak kurumsal bilgi güvenliği politikasına uyma yükümlülüğünün, ilgili firma ile yapılan yazılı sözleşmeye de dâhil edilmesi gerektiği düşünülmektedir.

Üniversitelerde bilgi güvenliğine ilişkin risk alanlarından biri de arşivlerdir. Birçok üniversitenin birimlerinde yazılı-basılı evraklara kolay erişim sağlanması ve saklama sorumluluklarının farklı olması nedeniyle bağımsız arşivlerin oluşturulduğu görülmektedir. Bu arşivlerin güvenliği söz konusu olduğunda, Devlet Arşiv Hizmetleri Hakkında Yönetmelikte de belirtildiği gibi (T.C. Başbakanlık, 1988); yangın, su baskını, rutubet, hırsızlık ve haşaratın tahriplerine karşı alınacak fiziksel önlemlere ilişkin yükümlülüklerin yerine getirilmesi yeterli olabilmektedir. Bu nedenle gerekli önlemlerin alınması üniversite birimleri tarafından sağlanabilmektedir. Ancak elektronik bilgilerin korunması söz konusu olduğunda; sadece fiziksel önlemlerin alınması yeterli olmadığı gibi, her birim için ayrı ayrı alınacak önlemlerin kapsamı üniversite birimlerinin imkân ve koşullarını zorlamaktadır. Araştırma esnasında bu konuya ilişkin olarak görüş bildiren altı BİDB katılımcısı, geleneksel veri saklama yöntemlerinin değişmesi nedeniyle farklılıkların değerlendirilmesi ve sorumluluk sahiplerinin yeniden tanımlanmasının gerekli olduğunu vurgulamaktadır. Üniversitelerde elektronik arşivlere yönelik risklerin azaltılabilmesi için, mevcut arşivlerin tek bir çatı altında ve bir belge yönetim biriminin

koordinatörlüğünde birleştirilerek, yazılı olarak belirlenmiş güvenlik politikaları kapsamında erişim yetkilerinin "bilmesi gereken prensibine" uygun olarak düzenlenmesi gerektiği değerlendirilmektedir.

5.9. KİŞİSEL VERİLERİN İMHA EDİLMESİ VE SİSTEM KAYITLARININ TEMİZLENMESİ

Araştırmadan elde edilen bulgular, üniversitelerin tamamında yazılı-basılı belgelerin imhası için kâğıt kırpma makineleri gibi yardımcı araçların kullanıldığı ve geri dönüşüm risklerinin göz önünde bulundurulduğu görülmektedir. Ancak aynı hassasiyetin elektronik bilgiler için gösterilmediği anlaşılmaktadır. Araştırma kapsamında yer alan üniversite BİDB ve kişisel verilerin işlendiği diğer birimlerde, elektronik verilerin kalıcı olarak silinmesine ve bu işlemlerde hangi standartların kullanılacağına ilişkin politikalar bulunmamaktadır. Elektronik verilerin imhasına ilişkin eksikliklerin temelinde, üniversite birimleri arasında bu sorumluluğun paylaşılmamış olmasının da yer aldığı düşünülmektedir. Üniversite BİDB birimlerinin %46,7'si verilerin imhası konusunda verileri işleyen birimin sorumlu olduğunu düşünürken; PDB ve KDB birimlerinin %78,3'ü bu konuda sadece BİDB'nin sorumluluğunun olduğunu ya da bilgi sahibi olmadıklarını ifade etmektedirler. Bu noktada değerlendirilmesi gereken soru, bilgisayar sayısının çok fazla olduğu üniversitelerde BİDB'nin bu sorumluluğu alması halinde mevcut BİDB personeli ile gerekli işlemleri yapıp yapamayacağıdır. Çünkü bilgisayar ve kullanıcı sayısı çok fazla olan üniversiteler, üniversite birimlerinde kişisel verilerin işlendiği bilgi sistemlerine yönelik teknik desteğin verilmesi konusunda dahi personel yetersizliğinden kaynaklanan zorlukların olduğunu ifade etmektedirler. Öte yandan, elektronik verilerin imha işlemi üniversite birimlerinde çalışan herhangi bir personel tarafından yapılabilecek bir işlem olmadığı gibi, BİDB personeli tarafından da bu tür işlemlerin uygun standartlarda yapılabilmesi için özel bilgi, uzmanlık ve zamana ihtiyaç duyulmaktadır. Araştırma verileri ışığında BİDB personel yeterliliği de göz önüne alındığında; üniversite BİDB tarafından verilerin imhasına ilişkin olarak birimlere verilebilecek desteğin sınırlı olabileceği değerlendirilmektedir.

Üniversite BİDB tarafından imha sürecine ilişkin olarak diğer birimlere doğrudan destek verilemediği düşünüldüğünde, üniversiteler için bir veri imha politikasının geliştirilmesi ve tüm birimler tarafından uygulanması daha fazla önem taşımaktadır. Ancak üniversitelerin %93,3'ünde henüz taslak halinde dahi veri imha politikasının bulunmaması, alınması gereken bilgi güvenliği önlemleri içinde henüz bu konuya yer verilmediğini göstermektedir. Veri imha politikalarının geliştirilmesi ve bu kapsamda üniversite birimleri arasındaki sorumlulukların belirlenerek uygulanmasının, üniversite birimlerinde kişisel verileri işleyen personel üzerindeki farkındalığı ve konuya olan ilgisini de arttıracağı değerlendirilmektedir. Üniversite PDB ve KDB katılımcılarından elde edilen araştırma verileri, PDB ve KDB birimlerinde elektronik verilerin nasıl, neden ve hangi yöntemlerle imha edileceğine ilişkin düşünceler arasında da büyük farklılıkların olduğunu ve bu konuda personelin %75,9'unun herhangi bir bilgilendirme toplantısına katılmamış olduğunu göstermektedir. Bu konuya ilişkin olarak, kurumsal bilgi güvenliği politikası çerçevesinde bir veri imha politikasının geliştirilerek veri imha standartlarının ve sorumluluklarının belirlenmesi ve BİDB bünyesinde veri imha işlemlerini belirlenen standartlara uygun olarak yapabilecek ve üniversite birimlerine destek sağlayacak bir birimin oluşturulması gerektiği düşünülmektedir.

Üniversite birimlerinde tamamen kullanım dışı kalan bilgi sistemlerinin üzerindeki bilgilerle birlikte çöpe atılması, bu sistemler üzerinde işlenmiş olan veriler için silinmiş olsa dahi risk oluşturmaktadır. Kullanım ömrü dolan sabit disklere yapılan işlemlere ilişkin araştırma verileri dikkate alındığında; üniversite birimlerinde "bilgi sahibi değilim" ya da "bu işlemler BİDB sorumluluğunda yapılıyor" düşüncesinde olan PDB ve KDB katılımcılarının oranının yüksekliği (sırasıyla %73,3 ve %83,3) dikkat çekicidir. Ancak araştırmadan elde edilen verilere göre, üniversitelerin büyük bölümünde (%93,3) BİDB içinde bu tür özel imha işlemlerinin yapılmadığı bilinmektedir. Bu risklerin tamamen ortadan kalkması, kalıcı silme işlemi ve sonrasında mümkün olması halinde fiziksel imhasının yapılmasıyla sağlanabilmektedir. Bunun için üniversitenin tüm birimlerinde gerekli yazılım, donanımın ve bu işlemleri yapabilecek personelin bulunması öngörülmemektedir. Ancak tamamen kullanım dışı kalan bilgi sistemlerinin bu tür işlemlere tabi tutulması gerektiği bilincinin üniversite birimlerinde veri işleyen tüm personelde oluşturulması gerekmektedir. Araştırma verileri, tüm üniversitelerde bu

bilince sahip birim personeli tarafından işlem ve yardım talebi olması halinde, BİDB tarafından gerekli desteğin sağlanabileceğini göstermektedir. Bu konuda üniversite birimlerinde görevlendirilen bilgi işlem sorumluları aracılığıyla gerekli koordinasyonun sağlanabileceği düşünülmektedir.

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

5.10. BİLGİ GÜVENLİĞİNİN SAĞLANMASINA İLİŞKİN EĞİTİM VE FARKINDALIK

Türk Hukuk Mevzuatında yer alan düzenlemelerin kişisel verileri korumaya yönelik ihtiyacı karşılamaması nedeniyle eğitim ve farkındalığın arttırılması konusu daha önemli hale gelmiştir. Ancak eğitim ve farkındalığa ilişkin faaliyetler bilgi güvenliği önlemlerinin bir unsuru olarak görüldüğü ve diğer güvenlik önlemleri ile koordineli olarak yürütüldüğü sürece başarılı olabilmektedir. Bu nedenle, bilgi güvenliği ve risk yönetimini bir bütün olarak kapsayan bilgi güvenliği modellerinden faydalanılması, güçlü bir güvenlik ağının oluşturulması açısından önem taşımaktadır. Teknik önlemlerle en yüksek seviyede korunan bilgilere dahi sosyal mühendislik yöntemleriyle kolaylıkla erişilebilmektedir. Bu nedenle, üniversitelerde de eğitim ve farkındalığın diğer güvenlik önlemleri içindeki ağırlığı artmakta ve ihmal edilmesi halinde bilgi güvenliği açısından zincirin en zayıf halkasını veriyi işleyen kullanıcılar oluşturmaktadır. Bu çalışmanın kapsamının belirlenmesinde yararlanılan McCumber bilgi güvenliği modelinde de eğitim ve farkındalık, bilgi güvenliği önlemlerinin önemli unsurlarından biridir. Bununla birlikte

araştırma kapsamında katılımcıların tutumlarını değerlendirmek amacıyla geliştirilen anket soruları titizlikle hazırlanarak; bilgi güvenliği konusundaki bilgi seviyesini etkileyen eğitim ve bilgi düzeyi ile davranışları etkileyen farkındalık düzeyinin ayrı ayrı ölçülmesi sağlanmıştır.

Farkındalığın arttırılmasına yönelik olarak, birim yöneticileri ve verileri işleyen personele tehditler ve tehditlere karşı alınacak önlemlere ilişkin eğitimlerin verilmesi gerekmektedir. Ancak üniversite PDB ve KDB birimlerinin %75,9'unda görev yapan birim yöneticilerine ya da verileri işleyen personele bilgi varlıklarının korunmasına yönelik her iki eğitimin de verilmediği görülmektedir. Bu konuda duyarlı olan dört PDB katılımcısı ise, kendi istek ve imkânları doğrultusunda dışarıdan eğitim alma yolunu seçmişlerdir. Ortaya çıkan bu tablo ve katılımcıların görüşleri değerlendirildiğinde, üniversitelerde bilgi güvenliğine ilişkin farkındalık eğitimlerine ihtiyaç duyulduğu görülmektedir. Üniversitelere yönelik tehdit türleri ve yetkisiz erişim yöntemleri arasında farklılık olmamasına karşın, üniversite birimlerindeki farkındalık eğitimine duyulan ihtiyaçlarda farklılıklar bulunmaktadır. Özellikle kişisel verilerin yoğun olarak işlendiği PDB gibi birimlerde düzenli aralıklarla bilinçlendirme eğitim ya da toplantılarının yapılmasının, risk ve tehditlerin ortadan kaldırılmasına önemli ölçüde katkı sağlayacağı değerlendirilmektedir.

Araştırmadan elde edilen verilere göre, üniversitelerde herhangi bir veri ihlali olması durumunda; BİDB, PDB ve KDB katılımcılarının büyük bölümü (sırasıyla %86,7, %92,9 ve %66,7) öncelikle idari amire bilgi verileceğini belirtmektedirler. Bilgi güvenliğinin sağlanması ve gerekli önlemlerin alınması konusunda idari tedbirlerin önemi ile katılımcıların vermiş oldukları cevaplar arasındaki ilişki bu noktada daha kolay fark edilebilmektedir. Katılımcılar karşılaşmış oldukları diğer günlük problemlerde olduğu gibi, veri ihlali konusunda da öncelikle idari amirlerine başvurma ve görüş alma yolunu seçmektedirler. TCK'da yer alan "bildirim yapılmasına" ilişkin düzenleme ile yetkili makamlara haber verme işleminin ilk adımı olması açısından bu tercihin kabul edilebilir olduğu düşünülmektedir. Zira bildirimde ihmal ya da gecikme olması halinde, TCK'nın

279. Maddesi[133] gereğince cezai yaptırım uygulanması öngörülmektedir. Katılımcıların verilerin ihlal edilmesi durumunda öncelikle idari amirlere haber verilmesine ilişkin tutumları, bilgi güvenliğinin sağlanmasına yönelik farklı çıkarımlarda bulunulmasına da imkân sağlamaktadır. Buna göre, alınan bilgi güvenliği önlemlerinin ve uygulanan politikaların idari amirler ve üniversite üst yönetimi tarafından benimsenerek birimlere uygulanmasının, personelin algısı üzerinde daha etkili olacağı ve daha kısa sürede davranışa dönüşeceği değerlendirilmektedir.

Üniversitelerde veri ihlali olması durumunda haber vermeksizin sistemin yeniden aktif hale getirilmesini tercih eden BİDB, PDB ve KDB birimi yöneticisinin bulunmaması, bu konudaki farkındalığın olumlu göstergelerinden biridir. Sistemin yeniden aktif hale getirilmesi konusunda zamanı iyi kullanma ve doğru adımların atılması arasındaki dengenin kurulması, meydana gelebilecek zararın boyutunu da etkilemektedir. Yetkisiz erişimler sonrasında meydana gelen zararın boyutunun çoğu zaman ilk aşamada görülemeyeceği ve sistem üzerinde yapılan değişikliklerin, zararın hukuksal girişimlerle telafi edilme olasılığını da ortadan kaldırabileceği değerlendirilmektedir.

Araştırma bulguları ve katılımcıların görüşleri birlikte değerlendirildiğinde, üniversite BİDB, PDB ve KDB birimlerinde kişisel verilere yönelik ihlallerle ilgili olarak veri sahibine de bilgi verilmesi gerektiği düşüncesinin bulunması, bu konudaki olumlu ve yapıcı davranışın birimlerde yerleşmiş olduğunu göstermektedir. Ancak hangi verilerin sorumluluğunun hangi birimde olduğu konusundaki belirsizlikler, bu konudaki tutum ve davranış üzerinde de etkili olmaktadır. Bu nedenle BİDB, PDB ve KDB katılımcılarının herhangi bir veri ihlali olması halinde veri sahibine bilgi verilmesi konusundaki yanıtlarında (sırasıyla %53,3, %64,3 ve %20) farklılıklar bulunmaktadır. KDB katılımcılarının yanıtlarındaki belirgin farklılığın (%20) nedeni, verilerin diğer birimler tarafından elde edilmiş olmasından kaynaklanmaktadır. Ancak bu anlayışın temelde yanlış olan bazı noktaları bulunmaktadır. Öncelikle, verinin elde edilmesi ve kullanılmasına ilişkin hukuksal sorumluluklar arasında farklılık bulunmaktadır. Her ne

[133] **TCK, 279. Madde:** (1) Kamu adına soruşturma ve kovuşturmayı gerektiren bir suçun işlendiğini göreviyle bağlantılı olarak öğrenip de yetkili makamlara bildirimde bulunmayı ihmal eden veya bu hususta gecikme gösteren kamu görevlisi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır.

(2) Suçun, adlî kolluk görevini yapan kişi tarafından işlenmesi halinde, yukarıdaki fıkraya göre verilecek ceza yarı oranında artırılır.

kadar veriler diğer birimler tarafından elde edilse de, verilere erişim sağlayan ve kullanan birimlerin de bu verileri koruma yükümlülükleri bulunmaktadır. Üniversite bilgi merkezleri tarafından erişilen ya da kullanılan verilere yönelik ihlalin bulunması halinde, bu verilere erişim sağlayan tüm birimlerle koordineli olarak bilgi merkezlerinin de atılacak adımları içeren eylem planını uygulaması gerekmektedir. Kişisel veri ihlalinin bilgi merkezinde gerçekleşmiş olması halinde, veri sahibinin bilgilendirilmesi sorumluluğunun bilgi merkezinde olduğu değerlendirilmektedir. Üniversite birimlerinde uygulama standardının oluşabilmesi için, öncelikle verilerin korunmasına yönelik olarak üniversite birimlerinin sorumlulukların belirlenmesi ve kurumsal bilgi güvenliği politikalarında veri sahibinin haklarına ilişkin unsurlara yer verilmesi gerekmektedir. AB Hukuk Mevzuatı kapsamında yapılan reform çalışmaları ve KVKKT üzerinde, veri koruma otoritesi ve veri sahibini bilgilendirmeye yönelik düzenlemelere de yer verilmektedir (Wong, 2013).

Üniversitelerde hassas ve kişisel verilerin korunabilmesi için, bu verileri işleyen personelin kişisel veri algısının nasıl olduğu da önem taşımaktadır. AB Hukuk Mevzuatında kişisel verilerin tanımı ve hangi verilerin kişisel veri olarak nitelendirileceğinin açık olmasına karşın; Türk Hukuk Mevzuatında bu tanım henüz tasarı aşamasındaki (KVKKT) düzenlemelerde görülmektedir. Bu nedenle, tüm kurum ve kuruluşlarda olduğu gibi üniversitelerde de standart bir kişisel veri algısının bulunduğunu söylemek güçtür. Bununla beraber üniversite PDB ve KDB birimlerinde iletişim ve kimlik bilgilerinin korunması gerektiği konusunda tereddüt bulunmazken; IP adresi, akademik özgeçmişe ilişkin veriler, bilgi merkezi kullanıcılarının araştırma konuları ve ödünç alınan yayınlara ilişkin bilgilerin neden korunması gerektiği konusunda katılımcıların en az %33'ünde tereddütler bulunmaktadır.

Üniversite bilgi merkezlerinde bilgi erişim olanaklarının geliştirilmesi ve bilgi kaynaklarının ihtiyaca cevap verecek şekilde zenginleştirilmesi amacıyla, kullanıcıların bilgi davranışlarına ait kayıtlar tutulmaktadır. Bu kayıtlar içinde veri tabanlarının kullanımı ve bilgi kayıtlarının ödünç alınma istatistikleri gibi kullanıcı ilgi alanlarını ve eğilimlerini gösteren hassas veriler bulunmaktadır. Bu bilgiler, bireyin düşüncesinin kayıtlara yansıması olarak değerlendirilmektedir. Bazı ülkelerde kütüphane kayıtlarının

incelenmesine ilişkin hukuksal düzenlemelerin yapılması ve toplumsal olaylar sonrasında soruşturmaların bilgi merkezi kayıtlarına başvurularak şekillendirilmesi de bu düşünceyi desteklemektedir (Starr, 2004). Kullanıcılara ait bu tür bilgilerin kendi iradesi dışında açığa çıkması, Anayasanın 25. ve 26. Maddesi kapsamında düşünceyi açıklama ve yayma hürriyetinin ihlali çerçevesinde de değerlendirilebilir. Bu konuda özellikle KDB katılımcılarının %56'sının, kullanıcıların yaptıkları araştırmaların ve yararlandıkları ya da ödünç aldıkları bilgi kaynaklarının kişisel veri kapsamında korunmasına ilişkin olarak tereddüt etmeleri dikkat çekicidir. Çünkü KDB katılımcıları, kişisel verilerin korunmasına yönelik olarak hukuksal düzenlemelerde eksikliklerin bulunduğu gerekçesiyle mesleki etik ilkeleri dikkate aldıklarını belirtmektedirler. Bilgi hizmetleri alanında çalışanların uyması gereken norm, kural ve davranışları belirlemeye yönelik olarak Türk Kütüphaneciler Derneği (TKD) tarafından kabul edilen "Mesleki Etik İlkelerinin" 7. Maddesinde[134] (TKD, 2010), TKD tarafından kabul edilen "Düşünce Özgürlüğü Bildirgesinin" 8. Maddesinde[135] (TKD, 2008) ve IFLA (International Federation of Library Associations and Institutions) tarafından yayınlanan "İfade Özgürlüğü ve İyi Kütüphaneciliğin İlkelerinin" 8. Maddesinde[136] (IFLA, 2014) ise bu bilgilerin gizliliğinin kişisel veriler ve özel yaşamın gizliliği kapsamında korunacağı açık olarak belirtilmektedir. Bu tereddütlerin, bilgi varlıklarının korunması ve hangi verilerin kişisel veri kapsamında değerlendirileceğine ilişkin farkındalık eğitiminin yapılmamasının bir yansıması olduğu düşünülmektedir. Araştırma esnasında katılımcılarla kimlik, kişilik ve kişinin hayat görüşüne ilişkin birçok bilgiye ulaşılmasını sağlayan hassas verilerin önemine ilişkin kısa bilgi alış verişi yapılması sonrasında katılımcıların konuya bakış açısının değişmesi de bu görüşü desteklemektedir.

Bilgi merkezlerindeki kişisel veri algısı, bilgi hizmetlerinin sunulmasındaki önceliklere ilişkin görüşü de etkilemektedir. Araştırma verilerine göre, bilgi hizmetlerinin sunulmasında hukuksal ve etik önlemlerin alınması düşük öncelik (%54,5) sırasında yer

---

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

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

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

almaktadır. Kişisel verilerin korunmasına yönelik risk algısının düşük olması ve bilgi ihlallerinin yaratacağı sonuçlara ilişkin endişe duyulmamasının bu sonuçta etkili olduğu düşünülmektedir. Bilgi merkezleri varlık nedenlerini "kullanıcının en kısa sürede bilgi ile buluşturulması" gibi mesleki ilkelerle açıklamaktadırlar. Ancak sorumluluklara ilişkin olarak elde edilen araştırma verileri değerlendirildiğinde; bilgi merkezlerinin %66,7'sinde "kullanıcıların bilgi ile *güvenli olarak* buluşturulması" konusunda sorumluluğun bulunmadığı düşünülmektedir. Bu düşüncenin temelinde öğretiden kaynaklanan kabullenmenin bulunduğu düşünülebilir. Öğretideki "düşünce ve erişim özgürlüğüne" vurgu yapılarak açıklanan bilgi hizmetlerinin sunulması ile uygulamadaki bilgi varlıklarının korunması ve sorumlulukların üstlenilmesi dengesinin sağlanmasında eksikliklerin olduğu değerlendirilmektedir. Bilgi merkezlerinde kullanıcı ile bilginin buluşturulması sürecinde güvenlik önlemlerinin farklı bir birim tarafından alınması ya da bu sorumluluğun üstlenilmesinin teknik ve hukuksal açıdan da mümkün olmadığı göz ardı edilmektedir. Bununla birlikte, güvenlik önlemlerinin alınması gerekçe gösterilerek dışarıdan yapılacak bu tür müdahalelerin kullanıcı erişim haklarını daha fazla sınırlandıracağı değerlendirilmektedir.

Araştırma bulgularına göre, üniversite PDB ve KDB birimlerinin %96,4'ünde kişisel verilerin işlendiği bilgisayarlara erişim sağlama konusunda gerekli hassasiyetin bulunduğu görülmektedir. Ancak özellikle merkezi veri tabanı üzerinde çalışmayan bilgisayarlar üzerinde yapılan işlem ve kayıtların tutulmasına ilişkin denetimlerin yapılmadığı görülmektedir. Bu bilgisayarlarda yapılan işlemlerin kim tarafından ve ne zaman gerçekleştirildiğine ilişkin kayıtlarının tutulması, gerektiğinde geriye dönük bilgi alınabilmesi açısından önem taşımaktadır. Üniversitelerde bu konuya ilişkin eksiklikler genel olarak kuruluş aşamasında görülmektedir. Yeterli altyapı, yazılım ve bilgisayar desteği sağlanmadan faaliyete geçen üniversite bilgi merkezlerinde, kolaylıkla yetkisiz erişimlerin yapılabildiği ya da ortak kullanıcı hesabı kullanımının daha yaygın olduğu görülmektedir. Bu aşamada bilgi güvenliği zafiyetlerinin daha fazla olabileceği açıktır.

Araştırma verileri değerlendirildiğinde, üniversite birimlerinin kişisel verilerin korunmasına ilişkin önceliklerinde farklılıkların olduğu görülmektedir. PDB ve KDB katılımcılarının bu konudaki birinci önceliği "hukuksal düzenlemeler kapsamında

korunması" iken (sırasıyla %71,4 ve %72,7); PDB katılımcıları için ikinci önceliğin "idari önlemlerin alınması" (%50), KDB katılımcıları için ise ikinci önceliğin "etik ilkeler çerçevesinde korunması" (%45,5) olduğu görülmektedir. Bu noktada kişisel verilerin öncelikle "hukuksal düzenlemeler kapsamında korunması" gerektiği düşüncesinin hâkim olması dikkat çekicidir. PDB ve KDB katılımcılarının belirtmiş oldukları ikinci önceliğe ilişkin farklılığın nedenini ise; KDB katılımcılarının hukuksal düzenlemelerdeki eksikliklerin etik değerlerle giderilebileceği yönündeki düşünceleri oluşturmaktadır. Bu bulgulara göre, uygulanabilir nitelikte hukuksal düzenlemelerin yapılması halinde, bu düzenlemelerin kısa sürede üniversitelerde benimsenerek uygulamaya dönüşmesinin sağlanabileceği söylenebilir. Üniversitelerde kişisel verilerin korunmasına ilişkin teknik önlemlerin alınmasının üçüncü öncelikte olması ise dikkat çekicidir. Oysa yapılan farklı araştırma sonuçlarında da görüldüğü gibi (Wolf ve diğerleri., 2011); şifre değişimi vd. güvenlik önlemlerin alınması konusunda mümkün olduğu ölçüde teknik önlemlerin alınması, zorlayıcı olması yönüyle alınan önlemleri daha etkili hale getirebilmektedir. Araştırmaya katılan dört katılımcı ise; hukuksal, etik, teknik ve idari önlemlerin aynı anda ve eşit düzeyde alınması gerektiğini belirterek sıralama yapmamıştır. Bu katılımcıların görüşleri de farklı bir yaklaşımı ve bu konuya ilişkin farkındalığın diğer boyutunu göstermesi açısından değerlidir. Araştırmadan elde edilen bulgular üniversitelerde hukuksal ve idari önlemlerin alınmasına ne kadar değer verildiğinin görülmesi açısından önemli olduğu gibi; teknik önlemler ve etik değerlerle bu konudaki eksikliklerin giderilebileceğine ilişkin farkındalığı ortaya çıkarması açısından da önem taşımaktadır.

Araştırma verileri dikkate alındığında; üniversite veri tabanlarına yönelik saldırıların içinde iç saldırı olarak nitelendirilen saldırılar da olduğu ve genellikle bilişimle ilgili bölümlerin öğrencileri ya da mezunları tarafından gerçekleştirildiği görülmektedir. Bu grubun faaliyetleri her ne kadar kötü niyetli olmasa da, bilişim suçları arasında yer alan yetkisiz erişim, sistemin işleyişini engelleme, verileri bozma ve yok etme gibi zararlı faaliyetler olarak nitelendirilmektedir. Bu noktada McCumber bilgi güvenliği modelinin önemli unsurlarından biri olan eğitim ve farkındalık boyutunu farklı bir açıdan değerlendirmekte fayda bulunmaktadır. Eğitim ve farkındalığın oluşturulması bilgi güvenliği önlemlerinin tamamlayıcı unsurlarından biri olmakla birlikte, sadece veriyi işleyen ya da saklanmasından sorumlu personel ile sınırlandırılmamalıdır. Üniversitelerin

bilgisayar mühendisliği bölümleri ve bilişim enstitüleri başta olmak üzere, bilişimle ilgili tüm eğitim programlarının içinde bilişim hukukuna ilişkin bilgilere de yer verilmelidir. Böylece sadece üniversite bilgi işlem merkezlerine değil, tüm kamu kurum ve kuruluşlarına yönelik kötü niyetli olmadığı halde kayıplara neden olan yetkisiz erişimlerin azaltılabileceği düşünülmektedir. Ayrıca, üniversite bilişim sistemlerinin güvenlik açıklarının tespit edilmesine yönelik uygulanan testlerin yanı sıra, ulusal siber güvenlik tatbikatına üniversitelerin de katılım sağlamasının ya da sadece üniversitelerin katılım sağladığı siber güvenlik tatbikatlarının organize edilmesinin yararlı olacağı değerlendirilmektedir. Bir yarışma ortamında gerçekleştirilecek bu tür tatbikatların, siber güvenlik konusunda yetişmiş eleman ihtiyacının karşılanmasına da katkı sağlayacağı düşünülmektedir.

5.11. GELECEKTE YAPILMASI ÖNERİLEN ARAŞTIRMALAR

Bilgi güvenliğinin kişisel verileri korumaya ilişkin yönü kapsamında yapılan bu çalışma, konunun çok kapsamlı olması nedeniyle genel çerçevenin çizilmesi ile sınırlı kalmıştır. Çalışmanın alt başlıklarında yer alan her konu (örneğin risk yönetimi gibi), kendi içinde detayları olan ve derin araştırma yapılabilecek konulardır. Bu nedenle, kişisel verilerin korunmasına yönelik her bilgi güvenliği önlemi için farklı alanlarda da (sağlık, eğitim, özel sektör vd.) araştırmaların yapılmasının, bu konuda kişisel hak ve özgürlüğün sağlanmasına önemli katkıları olacağı değerlendirilmektedir.

Üniversitelerde işlenen ve saklanan bilgilerin büyük bölümü elektronik ortamlarda işlenmekte ve saklanmaktadır. Hukuksal sorumluluklar açısından elektronik arşivlere aktarılan bilgiler de yazılı-basılı ortamda yer alan bilgilerle aynı niteliktedir. Ancak hukuksal düzenlemelerde elektronik arşivlerin korunmasına yönelik olarak yer alan ve fiziksel güvenlik ile sınırlı olan koruma yükümlülükleri, elektronik arşivlerde yer alan bilgilerin korunması için yeterli değildir. Bu çalışmada elde edilen veriler, birkaç üniversite dışında elektronik ortamda yer alan bilgilerin geleceğine ilişkin politikaların bulunmadığı ve bu konuda gerekli çalışma ve koordinasyonu sağlayabilecek belge yönetim ve arşiv merkezlerinin henüz kurulmadığını göstermektedir. Üniversite birimlerindeki tüm elektronik bilgilerin sınıflandırılarak merkezi bir birime güvenli

iletişim yöntemleriyle (sanal özel ağ ve e-imza kullanımı gibi) aktarılmasının sağlanması ve elektronik arşivlerin tüm yönleriyle (iletişim altyapısı, yazılım ve fiziksel olarak) korunması için kapsamlı elektronik arşiv politikalarının geliştirilmesine ihtiyaç duyulmaktadır. Bunun için sadece birkaç üniversitede örneği bulunan kurumsal belge yönetim ve arşiv merkezinin de çalışmalarının incelendiği kapsamlı projeler oluşturularak, konuya ilişkin temel ilkelerin tüm üniversitelerde uygulanabilir hale getirilmesi sağlanmalıdır.

6. BÖLÜM

ÜNİVERSİTE BİLGİ GÜVENLİĞİ POLİTİKA ÖNERİSİ

Üniversite içinde toplanan, işlenen, depolanan ve diğer kurum ya da kuruluşlara transfer edilen bilgi varlıklarının gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunması; üniversitenin misyonu ve üniversitede gizlilik derecesi bulunan verileri işleyen herkesin sorumluluğu olarak görülmektedir. Üniversite bilgi varlıklarına yetkisiz olarak müdahale edilmesi, değiştirilmesi ya da ifşa edilmesi, maddi zararların yanı sıra üniversitenin saygınlığına da zarar veren sonuçlara neden olmaktadır.

Bu çalışma kapsamında üniversiteler için geliştirilen bilgi güvenliği politikalarının tüm üniversiteler tarafından uygulanabilir olması amacıyla, Ankara'da bulunan 15 üniversiteden 44 daire başkanının (15 BİDB, 14 PDB ve 15 KDB) katılımıyla gerçekleştirmiş olduğumuz araştırma bulgularından teknik, idari ve hukuksal boyutlarıyla yararlanılmıştır. Çalışma kapsamında yapılan araştırma ile ilişkili maddeler, Ankara'da bulunan 15 üniversiteden elde edilen bulgulara dayanmaktadır. Çalışma kapsamında kişisel verilerin korunmasına yönelik Türk Hukuk Mevzuatı ve AB Hukuk Mevzuatında yer alan önleyici bilgi güvenliği tedbirleri irdelenerek politikaların içinde bu unsurlara yer verilmiş ve bilgi güvenliği politikasının hukuksal dayanağı oluşturulmuştur. Ayrıca; uluslararası bilgi güvenliği standartlarında yer alan temel unsurlar ve bu standartlar çerçevesinde DDK tarafından diğer kurum ve kuruluşlarda yapılan denetimlerin sonucunda oluşturulan raporlar da dikkate alınmıştır. Üniversite üst yönetimi tarafından takip edilen, tüm üniversite birimlerine sorumluluklar yükleyen ve birimler arasında koordinasyonun sağlanmasını öngören bu güvenlik politikası ile üniversite birimleri ve veri sahiplerinin uymaları istenen esaslar düzenlenmektedir. Bilgi güvenliğine yönelik sorumlulukların üniversite üst yönetimi ve tüm üniversite birimleri tarafından paylaşılmasıyla, iş süreçlerinin de kolaylaştırılması amaçlanmıştır.

6.1. AMAÇ

Madde 1

(1) Bu bilgi güvenliği politikasıyla üniversiteler için hukuksal, idari ve teknik bilgi güvenliği önlemlerini içeren, önleyici nitelikte, temel hak ve özgürlüklerin korunmasını öncelikler arasında belirleyen ve hukuksal düzenlemeleri dikkate alan bir bilgi güvenliği çatısının oluşturulması amaçlanmıştır.

(2) Belirlenen bilgi güvenliği önlemleriyle, üniversite birimlerinde işlenen tüm gizlilik değeri bulunan bilgiler ve/veya gizlilik/öncelik/hassasiyet derecesine göre sınıflandırılmış verilerin depolandığı ortamların gizliliği ve kullanılabilirliğinin sağlanması, risklerin kabul edilebilir seviyeye düşürülerek bilgi varlıkları için gerekli güvenlik standardının karşılanması, sorumlulukların ve yetkilerin belirlenerek, verilerin yetkisiz müdahale, değişim ve ifşa edilerek kurumun zarara uğratılmasının önlenmesi hedeflenmektedir.

6.2. KAPSAM

Madde 2

(1) Üniversite bilgi güvenliği politikası, üniversite birimlerinde elde edilen, işlenen, depolanan, dağıtılan ve imha sürecinde olan tüm bilgiler için uygulanır. Politika içinde yer alan temel ilkelerin bir bölümü; AB Hukuk Mevzuatında yer alan direktifler, uluslararası sözleşmeler ve Türk Hukuk Mevzuatında yer alan kanun ve/veya tasarı halinde olan düzenlemelerden alınmıştır. Bu nedenle üniversite gizlilik politikaları açısından önem taşıyan ve bu politika içinde yer verilen hassas ve kişisel verilere ilişkin unsurların bir bölümü, aynı zamanda hukuksal koruma altında bulunmaktadır.

(2) Hukuksal düzenlemeler çerçevesinde alınacak bilgi güvenliği önlemlerine ilişkin unsurlar belirlenirken, araştırma kapsamında Ankara'da bulunan 15 üniversitenin bilgi işlem daire başkanları, personel daire başkanları ve kütüphane ve dokümantasyon daire başkanları ile yapılan görüşmeler sonucunda elde edilen bulgular dikkate alınarak, uygulanabilir nitelikte bir bilgi güvenliği politikasının geliştirilmesi sağlanmıştır. Politika kapsamında belirlenen amaca ulaşılabilmesi

için üniversitede alınacak bilgi güvenliği önlemleri yapılandırılırken; ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardının sağlanabilmesi için gerekli ön şartlardan biri olan ve "risk seviyesinin düşürülmesine" ilişkin kontrolleri içeren ISO/IEC 27002 standardının içeriği de dikkate alınmıştır.

(3) Güvenlik politikaları içinde bulunan kişisel verileri korumaya yönelik esaslar, kişisel verileri işlenen gerçek kişiler ile bu verileri kısmen ya da tamamen elektronik ya da yazılı-basılı veri depolama ortamına kaydetmek üzere işleyen üniversite birimlerine uygulanır. Anonimleşmiş verilere ve kişisel verilerin gerçek kişiler tarafından sadece kişisel faaliyetlerine ilişkin olarak işlenmesi halinde uygulanmaz.

(4) Bu politika, üniversite içinde faaliyet gösteren ve/veya üniversitede verilerin işlendiği bilgisayarların bulunduğu ortamlarda çalışan personelin faaliyetlerini de kapsamaktadır. Üniversite bilgi güvenliği politikası, tüm üniversite fakülteleri, öğrenciler, personel ve belirli sözleşmeler çerçevesinde üniversite birimlerinde işlenen verilere erişim yetkisi tanınmış şirket çalışanlarına uygulanır.

6.3. KISALTMA VE TANIMLAR

Madde 3

(1) Bu politikada adı geçen;

a) Anonim Hale Getirme: Kişisel verilerin belirli veya kimliği belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek ya da kaynağı belirlenemeyecek hale getirilmesidir.

b) BEHK: Bilgi Edinme Hakkı Kanunu

c) BİDB: Üniversite Bilgi İşlem Daire Başkanlığı

d) Bilgi Güvenliği Politikası: Bilgi ve bilgi sistemlerine yetkisiz erişim, bilginin kullanımı, ifşa edilmesi, bozulması, değiştirilmesi veya bilginin gizlilik, bütünlük ve kullanılabilirliğine zarar vermek için yapılan kötü niyetli girişimlere karşı sağlanacak risk odaklı korumaya ilişkin politikadır.

e) Kişisel Veri[137]: Belirli veya kimliği belirlenebilir gerçek kişilere ilişkin bütün bilgilerdir.
f) Kurul: Üniversite Bilgi Güvenliği Kurulu
g) Hassas Veri[138]: Açıklanması halinde kişinin toplum içinde ayrımcılığa uğramasına ya da ötekileştirilmesine neden olabilecek inanç, politik görüş, sağlık bilgileri, cinsel yaşamı, etnik kökeni vb. bilgilerdir.
h) Rıza Beyanı: İlgili kişinin kendisiyle ilgili veri işlenmesi fiiline, "tereddüde yer bırakmayacak şekilde", özgürce, konuyla ilgili yeterli bilgi sahibi olarak verdiği ve sadece o işlemle sınırlı onay beyanıdır.
i) Üçüncü Kişi: Veri sorumlusu ile kişisel verileri işleyen kişilerin dışında kalan gerçek ve tüzel kişi, kamu kurum veya kuruluşudur.
j) Üniversite Bilgi Güvenliği Kurulu: Bilgi güvenliğinin sağlanmasına ilişkin teknik, hukuksal ve idari konularda çalışma ve denetim sorumlulukları bulunan, personel arasından seçilen ve yetkileri üniversite üst yönetimi tarafından belirlenen kuruldur.
k) Üniversite Birimi Bilgi İşlem Sorumlusu: Üniversite birimlerindeki bütün bilgi işlem faaliyetlerinin yürütülmesi ve BİDB ile koordineli olarak belirlenen güvenlik ve gizlilik politikalarının uygulanmasını sağlamak amacıyla yazılı olarak görevlendirilmiş personeldir.
l) Verilerin İşlenmesi: Verilerin elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi ya da imha edilmesi, yeniden düzenlenmesi, sınıflandırılması, açıklanması ve üçüncü kişilere aktarılması gibi bu veriler üzerinde gerçekleştirilen işlemlerdir.
m) Veri Sorumlusu: Birim ya da kurumda veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan ve/veya kişisel verilerin işlenme araç ve amaçlarını birlikte ya da tek başına belirleyen kişilerdir.
n) Veri Sahibi: Hakkında hassas ya da kişisel veri işlenen gerçek kişilerdir.

---

[137] Başlıca kişisel bilgiler arasında; telefon bilgileri, kimlik bilgileri, adres bilgileri, e-posta adresi, fotoğraflar, vatandaşlık numarası, kurum/öğrenci kimlik numarası, eğitim bilgileri, çevrimiçi kullanıcı hesapları, sosyal paylaşım siteleri üzerinden yapılan gönderiler, banka bilgileri ile sağlık kayıtları gibi kesin teşhis sağlayan bilgiler ve dolaylı da olsa kişiyi belirlenebilir kıldığı için, isim, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri ve genetik bilgiler bulunmaktadır (Avrupa Komisyonu, 2012c).

[138] Başlıca hassas (özel nitelikli) veriler arasında; kişilerin ırk, siyasî düşünce, felsefî inanç, din, mezhep veya diğer inançları, dernek, sendikal bağlantıları, sağlık bilgileri, cinsel yaşamları, ahlaki eğilimleri ve mahkûmiyetleri ile ilgili bilgiler bulunmaktadır (T.C. Başbakanlık, 2008b; TCK, 2004).

6.4. YETKİ VE SORUMLULUKLAR

6.4.1. Üniversite Bilgi Güvenliği Kurulunun Çalışma Esasları, Yetkileri ve Sorumlulukları

Madde 4

(1) Üniversite Rektörlüğü tarafından yetkilendirilen "Üniversite Bilgi Güvenliği Kurulu"; üniversite bilgi güvenliği politikalarının içeriğinin oluşturulması, güncellenmesi, yeniden değerlendirilmesi ve uygulanmasından sorumludur.

(2) Üniversite Rektörlüğü tarafından alınan kararla, Kurulun üye sayısı, üniversite birimlerini temsil oranı, görev süresi ve toplanma zamanları belirlenir.

(3) Üniversite Bilgi Güvenliği Kurulu;

a) Kişisel verilerin korunmasına ilişkin çalışma ve karar alma sürecinde hiçbir üniversite organı, makamı ya da kişiden emir ve talimat almaz. Yetkilerini bağımsız olarak kullanır.

b) Üniversite birimleri arasında sorumlulukların paylaşılması ve politikaların uygulanması için gerekli koordinasyonu sağlama yetkisine sahiptir.

c) BİDB bilgi güvenliği birimi ve/veya diğer üniversite birimlerinde bulunan bilgi işlem sorumluları ile de doğrudan koordinasyon kurma ve gerektiğinde bilgi güvenliğinin sağlanmasına yönelik görevler verme yetkisine sahiptir.

d) Veri sahibi açısından telâfisi mümkün olmayan bir zararın oluşma ihtimali bulunması halinde, geçici bilgi güvenliği önlemleri almaya yetkilidir.

e) Üniversitenin bilgi güvenliği danışma, koordinasyon ve denetim merkezi konumundadır. Üniversite bilgi güvenliği politikalarının uygulanmasına ilişkin olarak resen ya da başvuru üzerine denetim faaliyeti başlatabilir.

f) Üniversite birimlerinin kendi uygulama ve hizmetlerine ilişkin olarak geliştireceği detaylı gizlilik politikalarının üniversite bilgi güvenliği politikasına uyumluluğunun kontrol ve denetimini yapar.

g) Üniversitenin belirlemiş olduğu etik davranış ilkelerine aykırı davranış ve bilgi güvenliğinin ihlaline neden olabilecek uygulamalar hakkında, resen veya yapılacak başvurular üzerine, gerekli inceleme ve araştırmayı yapmaya yetkilidir.

h) Bireylerin, kişisel verilerin işlendiği üniversite idari birimlerine yönelik olarak kişilik haklarının ihlâl edildiği gerekçesiyle yapmış oldukları şikâyetleri inceler.

i) Bilgi güvenliğinin sağlanmasına ilişkin olarak, veri koruma hukuku alanındaki gelişmeleri takip ederek, ihtiyaç duyulması halinde diğer kurum ve kuruluşlar ile de işbirliği ve ortak çalışmalar yapabilir.

j) Üniversite birimleri için bilgi güvenliği raporlarının hazırlanması ve risk yönetimine ilişkin rehberlik hizmetlerinin sunulmasına katkı sağlar.

(4) Kurul üyelerinin çalışma ve denetleme sürecinde elde etmiş oldukları bilgileri üniversitenin yetkili organlarından başkasına açıklamama ve kendi yararına kullanmama yükümlülüğü bulunmaktadır. Bu yükümlülük, kurul üyelerinin görevden ayrılmaları halinde de devam eder.

(5) Kurul, açıklık ilkesinin gereği olarak; her yıl faaliyetlerine ve vermiş olduğu kararlara ilişkin olarak rapor hazırlar ve bu raporların erişime açılmasını sağlar.

(6) Kurul tarafından alınan kararlar ve/veya yapılan değişiklikler genel duyuru mekanizmaları ile duyurulur.

6.4.2. Üniversite Birimleri ve Veri Sorumlularının Yükümlülükleri

Madde 5

(1) Üniversite birimleri, Kurul tarafından incelenmesi amacıyla istenen bilgi ve belgeleri göndermek ve yerinde inceleme yapılabilmesi için gerekli şartları sağlamakla yükümlüdür.

(2) Kurul tarafından yapılan inceleme sonrasında üniversite bilgi güvenliği politikasının ihlal edildiğinin anlaşılması halinde, ilgili üniversite birimi verilerin bu politikalara uygun olarak işlenmesini sağlamakla yükümlüdür. Hukuka aykırı olarak kişisel veri işlenmesi halinde, ilgili kişisel verilerin işlenmesinin durdurulmasına yönelik olarak Kurul tarafından verilen karar uygulanır.

(3) Üniversite birimlerinde hassas ve kişisel verileri işleyen personel, bu verilerin işlenmesi esnasında gizliliğinin korunmasını sağlamakla yükümlüdür.

(4) Üniversite birimleri, güvenliğinin sağlanmasından sorumlu oldukları bilgilerin üniversite bilgi güvenliği politikası ve hukuksal düzenlemeler kapsamında

istenmesi halinde, talep edilen bilgilerin yetkili makamlara (kimlik kontrolü yapılma şartıyla) doğru ve eksiksiz verilmesinden sorumludurlar.

(5) Veri sorumlusu, kişisel verilerin tedbirsizlikle veya hukuka aykırı amaçlarla yok edilmesini, kaybolmasını, değiştirilmesini, yetkisiz olarak açıklanmasını veya aktarılmasını ve başka şekillerdeki tüm hukuka aykırı işlenmelerini önlemek için; korunacak verinin niteliği, teknolojik imkânlar ve uygulama maliyetine göre uygun teknik ve idarî tedbirleri almak zorundadır.

(6) Dışarıdan bilişim hizmeti sunan şirketler tarafından veri ihlali yapılması halinde, hizmeti alan üniversite biriminin de oluşan zarara ilişkin yükümlülüğü bulunmaktadır.

(7) Üniversite bilgi güvenliği politikalarına uyma yükümlülüğü bulunan tüm üniversite fakülteleri, öğrenciler, personel ve belirli sözleşmeler çerçevesinde üniversite birimlerinde işlenen verilere erişim yetkisi tanınmış şirket çalışanlarının; bu politikada belirtilen ilkelere aykırı uygulama ya da bilgi güvenliği ihlallerini Kurula bildirme sorumluluğu bulunmaktadır.

6.5. BİLGİ GÜVENLİĞİ RİSK YÖNETİM STRATEJİSİNİN GELİŞTİRİLMESİ

6.5.1. Üniversite Birimlerinde Risk Yönetimi Stratejisinin Geliştirilmesi Sürecinde Dikkate Alacak Unsurlar[139]

Madde 6

(1) Risk yönetim sürecinin ilk aşamasında bilgi varlıklarının tanımlanması ve envanterinin oluşturulması işlemleri yapılmalıdır.

(2) Bilgi varlıkları değerlendirilmeli ve öncelikleri belirlenerek sınıflandırılmalıdır.

(3) Üniversite birimlerinin karşılaşabileceği olası tehditler[140] önceliklerine bağlı olarak incelenmeli ve bu tehditlerin her birinin üniversite birimleri üzerinde oluşturacağı etki değerlendirilmelidir.

---

[139] Bu bölüm (Whitman ve Mattord, 2011) kaynağından uyarlanmıştır.

[140] Bilgi güvenliğine yönelik tehditler 14 kategori altında toplanmaktadır. Bunlar; 1.Fikri mülkiyet, 2.Yazılım saldırıları, 3.Servis kalitesine yönelik saldırılar, 4.Casusluk, 5.Doğal felaketler, 6.İnsan hataları, 7.Bilginin gasp edilmesi, 8.Bilginin kaybedilmesi, 9.Ağ kontrollerinin kaybedilmesi, 10.Sabotaj, 11.Hırsızlık, 12.Donanımsal arızalar, 13.Teknik yazılım hataları ve 14.Teknoloji eskimesidir. Detaylı bilgi ve kaynak için bkz. (Whitman ve Mattord, 2011)

(4) Özel bilgi varlıkları için karşılaşılabilecek olası riskleri gösteren risk derecesinin belirlenmesi için, risk değerlendirmesi yapılmalıdır.
(5) Güvenlik eksikliklerinin derecelendirilerek tanımlanması sonrasında, bu eksikliklerden kaynaklanan risklerin kontrol edilebilmesi için strateji geliştirilmelidir[141].
(6) Bilgi varlıklarının korunması için gereken maliyet ile bilginin karakteristik özelliklerinin değeri (bilgi varlığının değeri) arasındaki dengenin korunmasını amaçlayan uygulanabilirlik çalışması yapılmalıdır.
(7) Risklerin kabul edilebilir seviyeye düşürülmesini amaçlayan bir risk yönetim stratejisi oluşturulmalıdır.

6.5.2. Üniversite Birimlerinde Risk Yönetimi Kapsamında Göz Önünde Bulundurulacak ve Uygulanacak Genel Unsurlar

Madde 7

(1) Hassas ve kişisel verilerin bulunduğu veri depolama alanlarının ve bilgi sistemleri ortamının fiziksel güvenliğine ilişkin risk değerlendirmesi yapılarak, hırsızlık ve doğal felaketlere karşı gerekli önlemler alınmalıdır.
(2) Merkezi olarak verilerin depolandığı sunucuların bulunduğu sistem odalarına yapılan fiziksel erişimlerin kayıtları tutulmalı ve bu kayıtların güvenli olarak saklanması için gerekli önlemler alınmalıdır.
(3) Uygulanacak güvenlik seviyesinin belirlenmesi ve kripto kullanımı vb. üst düzey güvenlik önlemlerinin nerelerde kullanılacağının belirlenmesi için idari ve teknik seviyede risk değerlendirmesi yapılmalıdır.
(4) Hassas ve kişisel verilerin bulunduğu bilgi sistemlerine uzaktan erişim ile ilgili riskler belirlenmeli ve erişim hakkı verilmeden önce bu risklere yönelik önlemler alınmalıdır.
(5) Kişisel verilerin işlendiği veri depolama ortamlarına üniversite birimlerinin erişim, kullanım ve değiştirme yetkileriyle ilgili riskler tanımlanmalı ve personelin görev tanımına bağlı olarak sistem kullanım kayıtlarının tutulması sağlanmalıdır.

[141] Geliştirilecek olan risk kontrol stratejisi, savunma, transfer, azaltma, kabul etme ya da kaçınma üzerine kurulmalıdır.

(6) Kişisel verilerin işlendiği sistemlerin tasarımı esnasında ve verilerin işlenmesi sırasında teknik ve kurumsal önlemler alınırken, korunacak verilerin yapısı, risk durumu ve maliyetler de dikkate alınmalıdır.
(7) Sistem güncelleme ve yükseltme çalışmaları öncesinde, meydana gelebilecek yeni riskler gözden geçirilmeli ve sistem yedekleri alınmalıdır.
(8) Kişisel verilerin işlendiği birimlerde bulunan bilgisayarlara yeni yazılımların yüklenmesine ilişkin risk değerlendirmesi yapılmalı ve gerekli kısıtlamalar uygulanmalıdır.
(9) Kişisel verilerin işlendiği birimlerde bulunan bilgi sistemlerinin dış bağlantı riskleri gözden geçirilerek, dosya alış verişine ilişkin kısıtlamalar yapılmalıdır.
(10) Kişisel verilerin işlendiği birimlerde diz üstü bilgisayar gibi taşınabilir cihazların ve veri depolama ortamlarının kullanımına ilişkin risk değerlendirmesi yapılmalıdır.
(11) Kişisel verilerin bulunduğu sistemlere yönelik kötü amaçlı yazılımların oluşturabileceği riskler gözden geçirilmeli ve gerekli önlemler alınmalıdır.
(12) Herhangi bir bilgi güvenliği ihlalinin meydana getireceği etkilere ilişkin risk analizi yapılarak gerekli önlemler alınmalıdır.
(13) Üniversite bilgi sistemlerine yönelik olarak dışarıdan destek veren şirket ya da kişilere yönelik riskler belirlenmeli ve bir kontrol mekanizması geliştirilmelidir.

6.6. GENEL BİLGİ GÜVENLİĞİ ÖNLEMLERİ

6.6.1. Üniversite Bilgi Sistemleri ve Bilgisayar Ağında Bilgi Güvenliğinin Sağlanmasına İlişkin Olarak Alınacak Önlemler

Madde 8

(1) Üniversite birimlerinde işlenen veriler belirlenmiş kurallar, politikalar ve yönergeler çerçevesinde yetkilendirilmeli ve bu yetkilendirme amacını aşmamalıdır.
(2) Üniversite birimlerinde hassas ve kişisel verilerin işlendiği bilgisayarlarda üniversite BİDB tarafından sunulan ve/veya önerilen işletim sistemleri ve yazılımlar kullanılmalıdır.

(3) Üniversite birimleri tarafından işlenen verilerin merkezi olarak tutulduğu sunucular üzerinden verilen servislere ilişkin kayıtlar tutulmalı ve veri yedekleme politikasına[142] uygun olarak yedeği alınmalıdır.

(4) Üniversite birimleri sunmuş oldukları kablosuz ağ servisinin teknik ve idari sorumluluğunu taşımaktadırlar. Ağ erişim cihazı üzerinden geçen veri trafiği kayıtları, servisi veren üniversite birimi tarafından 5651 Sayılı Kanuna uygun olarak tutulmalı ve veri yedekleme politikasına uygun olarak yedeklenmelidir.

(5) 5651 Sayılı Kanun kapsamında "erişim sağlayıcı" ve "yer sağlayıcı" olarak tutulan trafik bilgilerinin doğruluğu, bütünlüğü ve gizliliği üst seviyede güvenlik önlemleri (kriptolama vd.) alınarak korunmalıdır.

(6) Üniversite birimleri, sorumlu oldukları sunucu ve çalışma bilgisayarları üzerindeki hassas ve kişisel verilerin ağ üzerinden iletimi, yetkisiz erişim, değiştirme ve kazara ya da yasa dışı yöntemlerle yapılacak tahribe karşı gerekli teknik ve kurumsal önlemleri BİDB ile koordineli olarak almalıdır.

(7) Üniversite birimleri, kendi bünyelerinde bulunan sunucuların yazılım ve donanım güvenliğini sağlamak için gerekli fiziksel ve teknik önlemleri almalıdır.

(8) Elektronik imza kullanımına yönelik olarak yapılandırılan sistem erişim yetkilendirmeleri birim bazında daraltılarak yapılmalıdır.

(9) Hassas ve kişisel verilerin işlendiği ve verilerin depolandığı tüm bilgi sistemlerinin sistem kayıtları BİDB tarafından ve/veya BİDB ile koordineli olarak önceden belirlenmiş politikalar kapsamında alınmalıdır.

(10) Hassas ve kişisel veriler taşınabilir veri depolama ünitelerine (USB bellek, CD/DVD vd.) kopyalanmamalı ve gerekli izinler alınmaksızın üniversite bilgi sisteminden çıkartılmamalıdır. Sağlanabilmesi halinde, kişisel verilerin işlendiği bilgisayarlar üzerine taşınabilir veri depolama ünitelerinin bağlandığı port ve sürücüler kullanıma kapatılmalıdır.

(11) Hassas ve kişisel verilerin üniversite içindeki birimler arasındaki transferinde, her ne sebeple (sistem arızası vb.) olursa olsun internet altyapısı ve internet ortamında çalışan yazılımlar kullanılmamalıdır[143].

---

[142] **Veri Yedekleme Politikası:** Üniversite birimleri ya da BİDB sorumluluğunda bulunan veri ve sistem yedeklerinin oluşturulma ve saklama usul ve esaslarını içeren politikadır.

[143] Konuya ilişkin riskler ve detaylı bilgi için bkz. (Külcü ve Henkoğlu, 2014)

(12) Üniversitenin belirlemiş ve onaylamış olduğu veri sınıflandırmasına[144] göre üzerinde risk değeri yüksek gizlilik dereceli bilgiler bulunan bilgisayar ya da veri depolama ortamlarına, sadece yerel alan ağı üzerinden erişim sağlanabilmesi için gerekli önlemler alınmalıdır. Teknik imkânların bulunması halinde, üniversite bilgisayar ağı dâhili ve harici etki alanlarına bölünmeli ya da üniversite birimlerinin erişim alanlarına bağlı olarak farklı sanal ağların oluşturulması sağlanmalıdır.

(13) Kişisel ve hassas veriler içeren e-posta gönderimi için üniversitenin sağlamış olduğu kurumsal e-posta servis ve altyapısının kullanılması sağlanmalıdır.

(14) Kişisel verilerin e-posta ile kriptolu olarak gönderilmesi sağlanmalıdır.

(15) Üniversite birimleri tarafından kullanılan, ancak sistem altyapısı BİDB tarafından sağlanan EBYS vb. projeler için bilgi güvenliğinin sağlanmasına ilişkin gerekli koordinasyon ve sorumluluk paylaşımı yapılmalı ve veri tabanı erişim yetkilendirmelerinin ilgili birimler tarafından düzenlenmesine imkân sağlanmalıdır.

(16) BİDB sorumluluğundaki veri tabanlarında yer alan ve erişim yetkilendirmeleri veriyi üreten birimlere yöre yapılandırılmış verilerin arşiv özelliği kazanması sonrasındaki erişim yetkilendirmelerinin nasıl olacağı da dikkate alınmalıdır. Bunun için kurumun arşiv işlerini yürüten birim ile BİDB arasında gerekli koordinasyon sağlanmalıdır.

(17) Elektronik Belge Standartları hakkındaki 2008/16 Sayılı Genelge[145] gereğince, üniversitede elektronik belgelerin korunmasına ve erişimine imkân sağlayacak tedbirler, TSE 13298 no'lu standarda göre elektronik belge yönetim sistemlerinin tasarım aşamasında ele alınmalıdır.

(18) Kişisel verileri yetkisiz erişimler, zararlı kodlar, kötü niyetli çalışanlar ve veri ihlallerine neden olan diğer bilişim suçlarına karşı etkin bir şekilde korumak amacıyla şu temel önlemler[146] alınmalıdır;

---

[144] Üniversitelerde verilerin sınıflandırılmasına ilişkin örnek için bkz. (http://security.harvard.edu/files/it-security-new/files/data_classification_table_abridged_7.23.13_0.pdf)

[145] Detaylı bilgi ve kaynak için bkz (T.C. Başbakanlık, 2008a)

[146] Detaylı bilgi ve kaynak için bkz. (Hanks, 2013)

a) Üniversite birimlerinde kişisel verileri işleyen personel alınan bilgi güvenliği önlemleri ve politikaları konusunda bilgilendirilerek, bilgi güvenliğine ilişkin olarak belirlenen usul ve esaslara uymaları sağlanmalıdır.
b) Zararlı kodlar kullanılarak işlenen bilişim suçlarına karşı temel teknik önlemlerin (güvenlik duvarı, anti virüs yazılımları vd.) alınması sağlanmalıdır.
c) Hassas ve kişisel verilerin işlendiği ve verilerin depolandığı sistemlere erişim sağlayan personel için; bireysel parola kullanımı, güçlü parola kullanımı, parolanın belirli aralıklarla değiştirilmesi, sisteme ilk girişte geçici parolanın değiştirilmesi ve eski parolaların kullanımına engel olunması gibi zorunlulukları getiren teknik önlemler alınmalıdır.
d) Bilgisayarlarda şifre koruması bulunmalı ve bilgisayarlar uzun süre kullanılmadığında kullanıcı oturumunun şifre ekranına dönmesi sağlanmalıdır.
e) Bilgisayarlarda lisanssız yazılım kullanılmamalı ve sistem güvenlik yamaları günlük olarak yapılmalıdır.
f) Hassas ve kişisel verilerin yanlış kişilerin eline geçmesi halinde dahi kötü amaçlı kullanımının önlenmesi için, bu tür veriler kriptolanarak saklanmalı ve/veya transfer edilmelidir.
g) Kişisel verilerin yasal düzenlemeler çerçevesinde iletişim ağları üzerinden transferi yapılırken; SSL[147], VPN (Sanal özel ağ)[148], yetkilendirme ve kriptolama gibi güvenlik teknolojilerinin kullanılması sağlanmalıdır.
h) Hassas ve kişisel verilerin yanlışlıkla ya da kasıtlı olarak silinmesi, değiştirilmesi veya bu verilerin bulunduğu depolama ortamlarının arızalanması halinde verilerin yeniden erişilebilir ve kullanılabilir hale getirilmesi için, farklı depolama ortamlarına periyodik ve kriptolu olarak yedeklenmelidir.
i) Veri tabanı dışında bulunan hassas ve kişisel veriler üzerinde yetkisiz erişimler vb. nedenlerle meydana gelen değişikliklerin takip edilebilmesi için,

[147] **Secure Socket Layer (Güvenli Yuva Katmanı):** 1994 yılında Netscape tarafından geliştirilen ve internet üzerinden şifreli veri iletişimi sağlayan güvenlik protokolüdür. SSL 3.0 sürümü tüm web tarayıcılar tarafından desteklenmektedir.
[148] **Sanal Özel Ağ (VPN- Virtual Private Network):** İnternet gibi ortak ağlar üzerinde uçtan uca ya da çok noktadan çok noktaya güvenli veri aktarımı sağlayan bağlantılardır. VPN bağlantılarda kapsülleme, kimlik doğrulama ve veri şifreleme özelliği bulunmaktadır.

üniversite birimleri tarafından bu veriler sınıflandırılarak diğer verilerden ayrılmalı ve teknik imkânların sağlanabilmesi halinde "hash" değerleri hesaplanarak kontrol mekanizması geliştirilmelidir.

j) Saklama süresi sona eren ya da kullanım amacı bulunmayan hassas ve kişisel veriler, geri dönüşüm olasılığını ortadan kaldıracak teknik yöntemlerle kalıcı olarak silinmelidir.

k) Üniversite bilgi sistemleri ağ yöneticisi tarafından düzenli aralıklarla güvenlik risklerini belirlemek amacıyla sistem taraması yapılmalıdır.

6.6.2. Fiziksel Güvenlik Önlemleri Kapsamında Alınacak Önlemler

Madde 9

(1) Bilgi ve bilgi sistemlerine yönelik tehditlerin en aza indirilebilmesi için risk düzeylerine göre kontrollü alanlar belirlenmeli ve bu çerçevede fiziksel güvenlik önlemleri alınmalıdır.

(2) Üniversite birimleri bilişim servislerinin sunulması ve verilerin saklanmasına ilişkin olarak, öncelikle BİDB tarafından üst düzeyde güvenlik önlemleri alınarak korunan merkezi olanaklar değerlendirilmelidir. Gizlilik derecesi bulunan yazılı-basılı bilgi kaynakları ise kilitli dolaplarda ve sağlanabilmesi halinde kamera sistemi ile desteklenerek muhafaza edilmelidir.

(3) Üzerinde kişisel ya da gizlilik dereceli veri bulunduran sistem bilgisayarlarına sistem yöneticileri dışında fiziksel erişim kısıtlanmalı ve bu sistemler üzerinde kullanılan veri depolama ünitelerinin kullanım süresi sonunda imha politikasına uygun olarak imha edilmesi sağlanmalıdır.

(4) Gizlilik dereceli verilerin işlendiği kontrollü alanlara kayıt cihazlarının girmesine izin verilmemeli ve bu alanlarda yapılan çalışmalara nezaret edilmelidir.

(5) Sistem odalarının fiziksel güvenliğinin sağlanması için güvenli anahtarların kullanılmasının yanı sıra alarm ve kamera sistemleriyle de desteklenmelidir.

(6) Hırsızlık, yangın, su baskını, toz, elektrik kesintileri ve elektromanyetik radyasyona ilişkin riskleri azaltmak için gerekli önlemler alınmalıdır.

(7) Fiziksel etki ve dinleme faaliyetlerine karşı, üniversite birimlerinde gizlilik dereceli verilerin işlendiği bilgisayarlar ve merkezi olarak verilerin saklandığı

sunucuların güç ve iletişim hatları birbirinden ayrılmalıdır. İmkân bulunması halinde fiber optik iletişim hatlarının kullanımı tercih edilmelidir.

(8) Hassas ve kişisel verilerin işlendiği tüm üniversite birimlerinde iş sürekliliği ve felaket kurtarma politika ve senaryoları geliştirilmelidir.

(9) Hassas ve kişisel verilerin işlendiği ya da depolandığı bilgisayarlara ve sistem ağ kablolarına erişim konusunda, her birim bilgi işlem sorumlusunun kontrolünde gerekli fiziksel güvenlik önlemlerini almalıdır.

(10) Hassas ve kişisel verilerin işlendiği ve/veya depolandığı bilgisayarların üzerine etiketlendirme ve ikaz notları yerleştirilerek, sadece yetkili kullanıcılar tarafından kullanılabileceği belirtilmelidir.

(11) Yazılı-basılı ortamda ve/veya taşınabilir veri depolama ortamlarında yer alan kişisel veriler, sadece erişim yetkisi olan kişiler tarafından erişilebilir olacak şekilde kontrollü alanlarda muhafaza edilmelidir. Fiziksel güvenliği sağlanmış bölgelere yabancıların girmesine müsaade edilmemelidir.

6.6.3. Doküman Güvenliğinin Sağlanması Amacıyla Alınacak Önlemler

Madde 10

(1) Üniversitede merkezi olarak saklanan verilere yetkisiz ve/veya izinsiz olarak erişim, üçüncü kişilere/kuruluşlara dağıtılması ya da bu verilere zarar verici girişimlerin engellenmesi amacıyla gerekli güvenlik önlemleri alınmalıdır.

(2) Bilgi kaynaklarının kullanımına ilişkin delil niteliğindeki bilgiler (IP adresi, web ziyaret tarih/zaman bilgileri, kaynak arama/erişim bilgileri vd.) sınıflandırılmalı ve korunması için gerekli güvenlik önlemleri sağlanmalıdır.

(3) Kişisel verilerin işlendiği üniversite birimlerinde fotokopi makinası, yazıcı ve tarayıcılar kullanılarak; kim tarafından, ne zaman ve hangi belgenin kopyalandığını gösteren kayıtların tutulmasını sağlayan yazılımlar kullanılmalıdır.

(4) Kişisel veri içeren belgeler kullanımı sonrasında çalışma masaları üzerinde bırakılmamalıdır.

(5) Risk derecesi yüksek olan kişisel ve/veya gizlilik dereceli bilgiler, üniversite birimlerindeki bilgisayarların dışında işlememeli ve depolanmamalıdır.

(6) Üniversite birimlerinde bulunan güvenlik görüntü kayıtları ve turnike kayıtlarının, hukuka aykırı olarak başkalarına verilmesine ilişkin önlemler alınmalıdır.

6.6.4. Personel Güvenliğinin Sağlanması Kapsamında Alınacak Önlemler

Madde 11

(1) Üniversite birimleri tarafından belirlenen bilgi işlem sorumluları Kurula ve BİDB'ye bildirilmelidir. Bilgi işlem sorumlularının Kurul ve BİDB ile koordineli olarak çalışması sağlanmalıdır.

(2) Üniversite birimlerinde hassas ve kişisel verilerin işlendiği bilgisayarlarda çalışan personel belirlenerek, bu personelin dışında bilgisayarlara fiziksel ve/veya uzaktan erişimin engellenmesi için gerekli önlemler alınmalıdır. Bu bilgisayarlarda çalışan personelin de sadece yetkilendirilmiş olarak bilgilere erişimi sağlanmalıdır.

(3) Üniversite birimlerine yeni atanan ve kişisel verilere erişim yetkisi verilmesi öngörülen personele, öncelikle üniversite bilgi güvenliği politikası ve bu kapsamdaki sorumluluklara ilişkin bilgilendirme yapılmalıdır.

(4) Analizlere esas olan temel verilerin doğrudan ya da dolaylı olarak insan katılımcılardan (üniversite birimlerinde çalışan personel vd.) elde edildiği araştırmalar için etik kurul değerlendirmesinin yapılması sağlanmalı ve insanlardan veri toplamayı gerektiren araştırmaların, kişi hak ve özgürlüklerine saygılı ve evrensel etik ilkelere uygun olup olmadığı incelenmelidir.

(5) Üniversite idari birimlerinde kişisel verilerin korunmasına ilişkin olarak uygun idari personel istihdam edilmeli ve güvenlik soruşturmalarına ilişkin bilgiler güncel olarak bulundurulmalıdır.

(6) Üniversite birimlerinde kişisel verileri işleyen personel ile yapılan sözleşmelerde kişisel verilerin korunması ve bu konuda ihlallerin olması halinde uygulanacak yaptırımlara yer verilmelidir.

(7) Üniversite birimlerinde çalışan ve gizlilik dereceli belgelere erişim yetkisi bulunan personelin güvenlik belgeleri düzenli (yıllık) olarak güncellenmeli ve her dönemde personel için bilgi güvenliği konusunda bilgilendirme toplantıları yapılmalıdır.

(8) Hassas ve kişisel verilerin işlendiği birimlerde çalışan personelin görevden ayrılması durumunda, çalışma esnasında edinmiş olduğu bilgilerin gizliliğinin korunması konusundaki sorumluluklara ilişkin ayrılış bilgilendirmesi yapılmalıdır.

(9) Belirli bir süre için üniversite birimleri tarafından işlenen verilere dışarıdan erişim yetkisi verilen ya da görevden ayrılan personelin, belirlenen ya da ilişik kesme işleminin gerçekleştiği tarihin sonunda erişim yetkileri sonlandırılmalıdır.

(10) Üniversite birimlerine dışarıdan bilişim hizmeti sunan şirketlerle gizlilik sözleşmesi ve personeline yönelik güvenlik araştırması yapılmalıdır.

6.7. HUKUKSAL DÜZENLEMELER VE TEMEL İLKELER KAPSAMINDA KİŞİSEL VERİLERİN VE BİREYİN KORUNMASI

6.7.1. İdari İşlemler Kapsamında Hassas ve Kişisel Verileri Korumak Amacıyla Alınacak Önlemler [149]

Madde 12

(1) Kişisel verileri işleme ve saklama sorumluluğu bulunan üniversite birimleri, kişisel verilerin tedbirsizlikle veya hukuka aykırı amaçlarla yok edilmesini, kaybolmasını, değiştirilmesini, yetkisiz olarak açıklanmasını ya da aktarılmasını ve diğer tüm hukuka aykırı işlemleri önlemek için; korunacak verinin niteliği, teknolojik imkânlar ve uygulama maliyetine göre uygun teknik ve idarî tedbirleri almalıdırlar.

(2) Üniversite birimleri tarafından idari işlemler kapsamında alınan güvenlik önlemlerinin koruma düzeyi, üniversite bilgi güvenliği politikalarından daha düşük seviyede olmamalıdır.

(3) Bilgisayar olaylarına karşı BİDB biriminde bilgisayar olaylarına müdahale ekibi oluşturularak, bu ekibin diğer üniversiteler ve kurumlarla da ortak çalışmalar yapabilmesi için imkân sağlanmalıdır.

[149] Detaylı bilgi ve kaynak için bkz. (Avrupa Komisyonu, 2001b)

(4) BİDB tarafından yapılan sözleşme çerçevesinde dışarıdan teknik destek alınması sürecine ilişkin olarak, ilgili şirket ve görevlendireceği personel hakkında güvenlik araştırması yapılmalıdır.

(5) Üniversitede merkezi veri depolama alanlarının bulunduğu ya da üniversite birimlerinde üzerinde kişisel verilerin bulunduğu bilgi sistemleri için BİDB tarafından yapılan sözleşmelere bağlı olarak dışarıdan teknik destek alınması halinde, ilgili birim ya da kullanıcının gözetimi altında işlem yapılmalıdır. Yerinde giderilemeyen donanımsal problemlerin olması halinde, bilgi sistem cihazlarının üzerinden veri depolama üniteleri sökülerek sistemle birlikte teslim edilmemesi sağlanmalıdır.

(6) Üniversite üst yönetimi tarafından ağ ve bilgi güvenliğinin sağlanmasına yönelik gerekli teknoloji desteği sağlanmalıdır.

(7) Üniversite için yeni sistemlerin alınması ya da mevcut sistemlerin iyileştirilmesine ilişkin ihtiyaçlar belirlenirken güvenlik gereksinimleri de göz önünde bulundurulmalı ve bu konuda ayrıca BİDB bilgi güvenliği biriminin görüşü alınmalıdır.

(8) Üniversite Bilgi Güvenlik Kurulu tarafından bilgi güvenliği standartları düzenli olarak gözden geçirilmeli ve bu kapsamda belirlenen ihtiyaçların giderilebilmesi için hazırlanacak programlar üniversite üst yönetimi tarafından desteklenmelidir.

(9) BİDB tarafından siber suçlara yönelik çalışmalar yapılmalı ve bilgi ve iletişim sistemlerine ilişkin güvenlik gereksinimleri karşılanmalıdır.

(10) BİDB bünyesinde bulunan bilgi güvenliği birimi tarafından tespit edilen bilgi güvenliği ihlalleri, yetkisiz erişimler ve kötü niyetli yazılımlar hakkında aylık rapor hazırlanmalı ve bu raporlar Kurul ile paylaşılmalıdır. Gerekli görülmesi halinde bu raporlar üniversite birimlerinde görevli bilgi işlem sorumluları ile de paylaşılarak sistem açıklarının en kısa sürede kapatılması sağlanmalıdır.

(11) Üniversite Bilgi Güvenlik Kurulunun bilgi güvenliğinin sağlanması konusunda uluslararası organizasyonlarla diyalog ve işbirliğine yönelik çalışmaları desteklenmelidir.

(12) Üniversite Bilgi Güvenliği Kurulu öncülüğünde ağ ve bilgi güvenliği kültürü oluşturulmalı ve kişisel verileri işleyen personelin bilgi güvenliğine ilişkin

eğitimlere katılmaları amacıyla ilgili üniversite birimleri ya da kurumlarla koordinasyon sağlanmalıdır.

6.7.2. Üniversitelerde Hassas ve Kişisel Verilerin İşlenmesi ve Hukuksal Düzenlemelerle İlişkili Önlemler[150]

Madde 13

(1) Kanunilik ilkesi gereğince, kişisel veriler ancak kanunlarda öngörülen hallerde işlenmelidir. Bununla beraber, TCK'nın 135. Maddesinde[151], kişisel verilerin hukuka aykırı olarak kaydedilmesine ilişkin ceza yaptırımı düzenlenmiştir.

(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgiler, kişisel veri olarak kaydedilmemelidir. TCK'nın 135. Maddesinde bu konuya ilişkin ceza yaptırımı düzenlenmiştir.

(3) Kişisel verilerin hukuka aykırı olarak açıklanması, yayılması, bir başkasına verilmesi ya da aktarılmasına ilişkin olarak önlemler alınmalıdır. TCK'nın 136. Maddesinde[152] bu konuya ilişkin ceza yaptırımı düzenlenmiştir. Bu suçların kamu görevlisi tarafından işlenmesi ve/veya mesleğin sağladığı kolaylıktan faydalanılması halinde, TCK'nın 137. Maddesinde düzenlenen "suçun nitelikli haline" ilişkin ceza yaptırımı öngörülmektedir.

(4) Kişisel verilerin kullanılması, değiştirilmesi, imhası, yetkisiz olarak erişimi, açıklanması ve kaybolması risklerine karşı uygun güvenlik önlemleri alınmalıdır.

(5) Kişisel veriler meşru ve yasal olarak belirlenen amaçlar için elde edilmeli ve işlenmelidir.

---

[150] 108 Sayılı "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşmenin" 5. ve 6. Maddeleri, 95/46/EC Sayılı "Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki Direktifi", KVKKT'de dikkate alınan rehber ilkeler ve 95/46/EC Sayılı Direktif üzerinde yapılan güncelleme çalışmalarından uyarlanmıştır.

[151] **TCK, Madde 135-** (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. (2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.

[152] **TCK, Madde 136-** (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

(6) Kişisel veri toplama amacı belirgin olmalı, sonraki kullanımlar bu amaca uygun olmalı, kişinin rızası ya da kanunun yetki verdiği haller hariç olmak üzere kişisel veriler toplanma amacının dışında kullanılmamalı ve açıklanmamalıdır.

(7) Kişisel veriler veri sahibinin bilgisi ya da rızası ile elde edilmeli ve işlenmelidir. Veri sahibinin rızası dışında işlenen veriler için kanunun öngördüğü bir zorunluluk bulunmalı, veri sahibi hakkında bağlayıcı bir sözleşme yerine getirilmeli ya da veri sahibinin meşru menfaati bulunmalıdır. Kişisel verilerin veri sahibi dışındaki bir kaynaktan elde edilmesi halinde de veri sahibi bilgilendirilmelidir.

(8) Elde edilen bilgiler tam, doğru, güncel, amacı ile bağlantılı ve amacı ile sınırlı olmalıdır. Yanlış ve eksik bilgilerin düzeltilmesi ya da silinmesi için gerekli işlemler yapılmalıdır.

(9) Veriler toplanma amacına uygun olarak ve belirlenen süre içinde saklanmalıdır.

(10) İstatistiksel bilgilerin kişi ile ilişkili olarak kullanılması zorunluluğu bulunmuyor ise (örneğin en çok erişilen veri tabanları listesi) anonim hale getirilerek işlenmeli ve saklanmalıdır. Kişi ile ilişkili olarak kullanılması zorunluluğu bulunan istatistiksel bilgiler için, bilgi güvenliği politikasında belirtilen gizlilik ve saklama koşulları sağlanarak kişisel haklar korunmalıdır.

(11) Üniversite birimleri ve BİDB tarafından tutulan sistem kayıtları ve trafik bilgileri, yasal olarak belirlenen veri saklama sürelerinden daha uzun süre tutulmamalıdır.

(12) Üniversite birimlerinde işlenen kişisel veriler üzerinde zorunlu olmadığı (zaman sınırı vb. nedenler) ve görüşmeler kayıt altına alınmadığı sürece telefon aracılığıyla güncelleme yapılmamalı ya da kimlik doğrulaması sonrasında işlem yapılmalıdır.

(13) Üniversite birimlerinin danışma hizmetlerinde elde edilen veriler, haberleşme aracının türüne (e-posta, anlık mesajlaşma, telefon vd.) bakılmaksızın korunmalı ve bu bilgiler hukuksal gerekçeler olmadığı sürece paylaşılmamalıdır.

(14) İhtiyaç duyulmayan ve koruma tedbiri ya da ispat amacıyla muhafaza edilmesi gerekli olmayan veriler anonim hale getirilmeli ya da imha edilmelidir.

(15) Kullanım ve saklama süresi sona eren verilerin imha edilmesi sağlanmalıdır. Kullanım süresi sona eren ve kanunların belirlediği sürelerin geçmiş olmasına

rağmen verilerin imha edilmesi sorumluluğunu yerine getirmeyenler için, TCK'nın 138. Maddesinde[153] ceza yaptırımı düzenlenmiştir.

(16) Elektronik ortamda yer alan verilerin imha edilmesinde (kalıcı silme işlemi için) üniversite tarafından uygulama esas ve usulleri belirlenmiş veri imha politikalarında öngörülen standartlar (DoD 5220.22-M vb.) kullanılmalıdır.

(17) Üniversite birimlerinin BİDB tarafından yerine getirilmesini istediği işlemleri "bilgi işlem yardım masasından" talep etmesi ve bu taleplerin kayıt altına alınması sağlanmalıdır.

(18) TCK'nın 243. ve 244. Maddeleriyle düzenlenen bilişim suçlarıyla ilişkili olarak üniversite birimlerinde herhangi bir veri ihlali olması durumunda, en kısa sürede yetkili makamlara bildirimde bulunulmalıdır.

(19) Üniversite personeli ve öğrencilerin ilk kayıt ya da atama esnasında oluşturulan bilgi formlarının üçüncü kişilerle paylaşılmasına ilişkin onay alınmalı ve üniversite birimleri tarafından belirtilen şartlara uyulmalıdır. Bu kapsamda öğrenciler tarafından belirtilen şartlar, öğrenci bilgilerinin aileleri ile paylaşımında dikkate alınmalıdır.

6.7.3. Bireyin Hak ve Özgürlüğünün Korunmasına Yönelik Olarak Alınacak Önlemler

Madde 14

(1) Veri sahibinin kişisel hak ve özgürlüğünü koruyacak önlemler, hukuksal düzenlemeler ve üniversite bilgi güvenliği politikası kapsamında alınmalıdır.

(2) Üniversite birimleri arasında kişisel verilerin serbest akışına izin verildiği gibi, bireylerin temel hakları da güvence altına alınmalıdır. Yeterli düzeyde güvenlik önlemlerinin alınamadığı birimlere kişisel verilerin transferi kontrollü olarak sağlanmalıdır.

(3) Veri sahibi Anayasa'nın 20. Maddesinde yer verilen[154], kendisiyle ilgili kişisel verilerin korunmasını isteme, kendisiyle ilgili olarak kaydedilen kişisel verilerin

---

[153] **TCK, Madde 138-** (1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

[154] **Anayasa, Madde 20 -** (Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların

neler olduğunu öğrenme, bu bilgileri talep etme, eksik ya da gerçeğe aykırı olması halinde düzeltilmesini isteme, hukuka aykırı olması halinde silinmesini, imha edilmesini ve aktarımının engellenmesini isteme hakkına sahip olmalıdır.

(4) Kişisel verilerin elde edilmesi sırasında veri sahibi; verilerin hangi amaçla işleneceği, kimlere aktarılabileceği, toplanan verilerin hukuksal dayanağı, elde edilen kişisel verilerin içeriğini öğrenme ve bu bilgilerin eksik ya da gerçeğe aykırı olması halinde düzeltme hakkının olduğu konusunda bilgilendirilmelidir.

(5) Veri sahibinin verinin kaynağını bilme ve hukuka aykırı işlemlere karşı kanun yollarına başvurma hakkı bulunmalıdır. Üniversite birimleri tarafından elde edilen kişisel veriler üniversite veri tabanından alınmasa dahi, veri sahibine elde edilen verilere ilişkin bilgi verilmelidir.

(6) Kişisel verileri veri sahibinden elde eden üniversite birimleri, bu bilgilerin üniversite bilgi güvenliği politikası kapsamında korunacağı ve izinsiz olarak paylaşılmayacağına ilişkin olarak veri sahibine yazılı taahhütte bulunmalıdırlar.

(7) Yasal zorunluluklar nedeniyle soruşturma/kovuşturma kapsamında paylaşılan bilgilerin dışında diğer kişi, kurum ve kuruluşlarla paylaşılan kişisel bilgilere ilişkin olarak veri sahibinin bilgilendirilmeyi isteme hakkı bulunmalıdır.

(8) Kişisel bilgi veya belgeler özel hayatın gizliliği kapsamında değerlendirilerek; kamu yararı ve veri sahibinin yazılı izni bulunmadığı sürece 4982 Sayılı Bilgi Edinme Hakkı Kanunu kapsamında açıklanmamalıdır.

(9) Bireylerin bilgi edinme hakkını kullanmasına yardımcı olunarak, 4982 Sayılı Bilgi Edinme Hakkı Kanununda belirlenen istisnalar dışında, usulüne uygun olarak bilgi verilmelidir.

(10) Veri depolama alanları üzerinde oluşan güvenlik ihlali ile ilgili durumlarda veri sahibi zaman kaybetmeksizin bilgilendirilmelidir.

(11) Üniversite bilgi merkezleri ve diğer birimler, merkezi veri tabanı üzerinden (PDB personel kayıtları gibi) elde ettikleri kişisel verileri sadece kullanıcı hesabı açmak ya da güncellemek gibi belirlenmiş sınırlı işlemler için kullanmalıdırlar.

---

düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir.

(12) Bilişim kaynaklarını kullanıma sunan birimler, kullanıcı ya da personel bilgilerinin gizliliğini korumalıdırlar. Bu kaynaklar hukuksal düzenlemelere ve üniversite bilgi güvenliği politikalarına aykırı olarak kullanılmamalıdır.

(13) 5651 Sayılı Kanun kapsamında "içerik sağlayıcı" sorumluluğunu taşıyan üniversite birimleri, şeffaflık ilkesi gereğince yapılan ilanlarda kişisel bilgilerin korunmasına özen göstermelidirler.

(14) Bilgi hizmetleri kalitesinin arttırılması amacıyla tutulan ve düzenli olarak yayınlanan istatistiksel raporlar kişisel veri içermemelidir. Kişisel veriler, araştırma, planlama ve istatistiksel amaçlı olarak anonim hale getirilmek şartıyla işlenmelidir.

(15) Üniversite birimlerinde danışma hizmetleri kapsamında kullanıcıların sözlü ya da sosyal medya üzerinden yöneltmiş olduğu sorular ve sağlanan hizmete ilişkin bilgiler, kişi ile ilişkilendirilerek kayıt altına alınmamalı ve üçüncü kişi ve/veya kurum/kuruluşlarla paylaşılmamalıdır.

(16) Hukuksal zorunluluklar ve verilerin istatistiksel amaçlı olarak anonimleştirilerek kullanılması gibi bu politikada belirlenen istisnai durumlar nedeniyle belirli bir süre için saklanan verilerin dışındaki kişisel verilere ilişkin olarak; bireylerin üniversite bilgi sistemleri ağı üzerindeki veri koruma haklarını yönetebilmesine imkân tanıyan "unutulma hakkı" [155] sağlanmalıdır.

(17) Üniversitelerde veri işleme sistemleri insana hizmet etmek üzere tasarlanmalı ve kişilerin gizliliği ile temel hak ve özgürlüğünü korumalıdır.

(18) Önceden belirlenmiş bazı özel durumlar (tıbbi verilere erişimin sağlık uzmanları ile sınırlandırılması gibi) dışında, veri sahibinin, kendisine ait kişisel verilerin doğruluğunu onaylayabilmesi için, bu verilere erişimi ya da ilgili birim personeli aracılığıyla kontrolü sağlanmalıdır.

[155] Detaylı bilgi ve kaynak için bkz. (Avrupa Komisyonu, 2011c)

6.7.4. İstisnalar

Madde 15

(1) Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaati, suçların önlenmesi, ilgili şahsın korunması ve başkasının hak ve özgürlüğü için zorunlu olması halinde; Kurul tarafından verilen kararlar çerçevesinde bilgi güvenliğinin sağlanmasına ilişkin olarak alınacak önlemlerin kapsamı daraltılabilir[156]

(2) Kişisel veriler, kanun gereği zorunlu olması halinde; bir hakkın tespiti, korunması, suçun önlenmesi ya da soruşturulması için ilgili kamu kurum ve kuruluşları ile paylaşılabilir.

(3) Hukuksal düzenlemeler çerçevesinde yürütülen soruşturma/kovuşturma kapsamında paylaşılan kişisel verişlere ilişkin olarak, soruşturma/kovuşturmanın gizliliği nedeniyle veri sahibine bilgi verilmeyebilir.

(4) Üniversite birimleri, veriyi işleyen personel ya da veri sahipleri arasında doğabilecek her türlü ihtilaf durumunda, üniversite yönetimi doğrudan taraf olma hakkını saklı tutar.

6.8. EĞİTİM PROGRAMLARI, VERİ İHLALİ YÖNETİM PLANI VE DENETİMLERE İLİŞKİN HUSUSLAR

6.8.1. Personelin Farkındalığını Arttırmaya Yönelik Eğitim ve Eğitim Programının İçeriğinde Yer Alacak Konular

Madde 16

(1) Personelin farkındalığını arttırmaya yönelik olarak, çalışmaya başladığı ilk haftalar içinde bilgi güvenliğinin sağlanmasına ilişkin önlemler ve kurumsal bilgi güvenliği politikası hakkında genel bilgi verilmeli ve yılda bir defadan az olmamak koşuluyla, düzenli aralıklarla bilgilendirme toplantıları yapılmalıdır. Bu toplantılarda;

[156] Detaylı bilgi ve kaynak için bkz. (Avrupa Konseyi, 1995) ve (Avrupa Komisyonu, 1981)

a) Bilgi sistemleri güvenliği, fiziksel güvenlik, doküman güvenliği ve personel güvenliğine ilişkin genel hususlar,
b) Kullanıcı şifrelerinin seçilmesi, kullanımı ve değiştirilmesine ilişkin resmi prosedürler ile şifrelerin diğer kullanıcılarla paylaşılmaması ve diğer kullanıcıların şifreleriyle oturum açılmamasına ilişkin hususlar,
c) Bilgisayar ekranı ve klavye üzerinden şifre elde etmek amacıyla kullanılan yetkisiz gözetim yöntemlerine ilişkin hususlar,
d) Kullanıcı erişim hakları, bu hakların düzenli aralıklarla kontrol edilmesi ve güncellenmesine ilişkin hususlar,
e) Herhangi bir veri ihlali gerçekleşmesi halinde uygulanacak eylem planına ilişkin hususlar,
f) "Temiz masa" ve "temiz ekran" politikalarına uygun olarak çalışma masaları, yazıcı, tarayıcı ve fotokopi makinalarının üzerinde gizlilik dereceli belgelerin bırakılmaması, bilgisayar ekranlarının çalışılmayan zamanlarda kilitlenmesi ve çalışma odaları terk edilirken dikkat edilecek hususlar ve
g) "Bilmesi gereken prensibi" çerçevesinde alınacak önlemler ve erişim yetkilendirmelerine ilişkin esaslar hakkında genel bilgiler verilerek, personelin bilinçlendirilmesi sağlanmalıdır.

(2) Personelin farkındalığını arttırmaya yönelik eğitim programlarında;
a) Hassas ya da kişisel verilerin toplanması, kullanımı, transferi ve hangi verilere işlem yapılacağına ilişkin hususlar,
b) EBYS'ye ilişkin mevzuat ve standartlar
c) Personelin kişisel verileri hukuksal düzenlemeler çerçevesinde koruma yükümlülükleri,
d) Veri korumaya ilişkin temel ilkeler ve hukuksal düzenlemeler çerçevesinde alınan önlemler,
e) Yetkisiz erişimleri engellemek için kullanılan yöntemler ve aldatma yöntemlerine (phishing vb.) karşı alınan önlemler,
f) Zararlı yazılımlara (virüs, trojan vd.) karşı alınan teknik önlemlerin güncelliğinin korunması,
g) Soruşturma ve kovuşturma evrelerinde yazılı olarak talep edilen kişisel bilgilere ilişkin sorumluluklar,

h) Kişisel verilere yönelik yetkisiz erişimler ve siber saldırılar sonucunda herhangi bir güvenlik ihlali oluşması halinde, veri sahibine ve ilgili makamlara durumun bildirilmesine dair yükümlülükler,
i) Veri saklama süreleri, imha sorumluluğu ve politikalarına ilişkin hususlar,
j) Verilerin yedeklenmesine ilişkin hususlar,
k) Bilişim kaynakları kullanım ve gizlilik politikaları ve
l) Bilişim servisleri işletim ilkeleri ve sorumlulukları yer almalıdır.

6.8.2. Kişisel Verilerin Korunmasına Yönelik Olarak Uygulanacak İhlâl Yönetim Planında Yer Alacak Unsurlar[157].

Madde 17

(1) Hassas ve kişisel verilerin işlendiği üniversite birimlerinde risk değerlendirmesi yapılarak; yetkisiz erişimler, zararlı kodlar ve kötü niyetli çalışanlar tarafından gerçekleşebilecek olası bir ihlâl durumunda veri sahibine yönelik olarak meydana gelebilecek olumsuz sonuçlar değerlendirilmelidir.
(2) Meydana gelen veri ihlâli ile ilgili olarak kimlerin (Kurul, savcılık, veri sahibi vd.), hangi öncelik sırasına göre ve neden bilgilendirileceğine dair plan yapılmalıdır.
(3) Meydana gelen ihlâlin nedenleri ve alınan önlemlerin değerlendirilmesine yardımcı olacak bir olay müdahale planı oluşturulmalıdır.
(4) Bilgi güvenliği olayları nedeniyle gerçekleşebilecek kesintilerin etkilerine ilişkin risk analizleri ve iş sürekliliğinin sağlanması amacıyla alınacak önlemleri (sorumlulukların, hasarların ve onarım prosedürlerinin belirlenmesi) içeren iş sürekliliği yönetim stratejisi belirlenmelidir.
(5) Kaybedilen verilerin yedeklenen en son haliyle yeniden elde edilebilmesi amacıyla veri kurtarma planı oluşturulmalıdır.

[157] Detaylı bilgi ve kaynak için bkz. (Johnston, 2011)

6.8.3. Bilgi Güvenliğinin Sağlanması İle İlişkili Olarak, Kişisel Verilerin Korunması Konusunda Yapılacak Denetim ve Kontrollerde Dikkate Alınacak Unsurlar[158]

Madde 18

(1) Hassas ve kişisel verilerin korunmasına ilişkin olarak yapılan iç denetimler, hukuksal düzenlemeler ve kurumsal bilgi güvenliği politikasına uyumlu olmalıdır.

(2) Denetimler, BİDB bünyesinde oluşturulan bilgi güvenliği birimi, BİDB'de bilgi güvenliğinin sağlanması amacıyla özel olarak görevlendirilmiş personel ve/veya üniversite birimlerinde görevli bilgi işlem sorumluları ile koordineli olarak, Bilgi Güvenliği Kurulu tarafından yapılmalıdır.

(3) Üniversite birimlerinde kişisel verilerin korunması ve bilgi güvenliğinin sağlanmasına ilişkin sürecin yürütülmesi için sorumluluklar belirlenmiş olmalı ve personelin görev tanımlarında bu sorumluluklar yer almalıdır.

(4) Aktif veri tabanı testlerinde kişisel ve diğer hassas veriler kullanılmamalı ve test için kullanılması gerektiğinde canlı sistem bilgilerinin içindeki gizlilik dereceli bilgiler çıkartılmalıdır.

(5) Üniversite birimlerinde kişisel verileri işleyen personel, üniversitenin oluşturmuş olduğu kurumsal bilgi güvenliği politikası ve bilgi güvenliğinin sağlanması amacıyla oluşturulan organizasyon yapısı hakkında bilgi sahibi olmalıdır.

(6) Üniversite birimleri tarafından alınan önlemler ve uygulanan politikalar, hukuksal düzenlemeler ve üniversite bilgi güvenliği politikasına uyumlu olmalıdır.

(7) Üniversite birimleri; bilgi sistemleri güvenliği, fiziksel güvenlik, doküman güvenliği ve personel güvenliğine ilişkin yükümlülüklerin yerine getirilmesi için gerekli önlemleri almalıdırlar.

6.9. YAPTIRIMLAR

Madde 19

(1) Üniversite bilgi güvenliği politikalarında belirtilen ilkelere aykırı olarak işlem yapılması ve/veya bu kapsamda gerekli önlemlerin alınmaması nedeniyle bilgi

[158] Detaylı bilgi ve kaynak için bkz. (Ottekin, 2008).

güvenliği ihlaline sebep olunması halinde; meydana gelen zararın boyutuna ve tekrarına bakılarak aşağıda yer alan işlemlerin biri ya da birden fazlası uygulanabilir;

a) Bilgi güvenliği ihlaline sebep olan birim ya da personel sözlü ve/veya yazılı olarak uyarılır.
b) Üniversite bünyesindeki akademik/idari soruşturma mekanizmaları harekete geçirilir.
c) Adli yargı mekanizmaları harekete geçirilerek hukuk mevzuatında belirtilen cezaların uygulanması sağlanır.

(2) Bu politikada tanımlanmayan ya da tanımlanan ilkelerin yetersiz kaldığı bilgi güvenliği ihlallerinin gerçekleşmesi halinde, meydana gelen zararın niteliğine bağlı olarak Üniversite Bilgi Güvenliği Kurulu tarafından değerlendirme yapılır.

6.10. İLGİLİ POLİTİKALAR VE YOL HARİTASI

Madde 20

(1) Bilgi varlıklarının en üst seviyede korunabilmesi amacıyla geliştirilen üniversite bilgi güvenliği politikalarındaki temel esaslar oluşturulurken, uzun süre güncelliğini koruyabilecek ve teknolojideki gelişmeler karşısında kapsamında daralmaya neden olmayacak ifadelere yer verilmiştir. Üniversite birimlerinde geliştirilecek diğer servis kullanım politikalarının, bilgi güvenliği politikasına bağlı olarak ilgili konularda eksikliklere yer bırakmayacak detayda hazırlanması ve yıllık ve/veya gerekli görüldüğü zamanlarda güncellenmesi sağlanmalıdır.

(2) Üniversite bilgi güvenliği politikası, üniversite birimlerinin uygulama ve hizmetlere bağlı olarak geliştirecekleri politikaların temel ilkelerini belirlemektedir. Üniversite birimleri kendi iç dinamikleri ve uygulamalarına bağlı olarak, bilgi güvenliği politikasında yer alan temel ilkeler kapsamında kendi hizmet politikalarını detaylı olarak yapılandırmalı ve uygulamalıdır. Üniversite birimleri tarafından geliştirilecek bu politikalar, üniversite bilgi güvenliği politikalarına aykırı maddeler içermemelidir.

(3) Bu bilgi güvenliği politikası dikkate alınarak üniversite birimleri tarafından geliştirilmesi öngörülen diğer gizlilik ve bilgi güvenliği politikaları şunlardır;

a) Bilişim kaynakları kullanım ve gizlilik politikaları
b) Veri yedekleme ve gizlilik politikası
c) Veri imha ve gizlilik politikası
d) Yardım masası çalışma esasları ve gizlilik politikası
e) Üniversite yerel alan ağında 5651 Sayılı Kanun kapsamında uyulması gereken kurallar
f) Üniversite yerleşkesinde bilişim servisleri işletim ilkeleri ve gizlilik politikaları
g) E-Posta, FTP, WEB, DNS, DHCP, veri tabanı işletim ilkeleri ve gizlilik politikaları
h) Veri ihlali yönetim ve eylem planı
i) Üniversite yerleşkesinde kablosuz ağ kullanımı kuralları ve gizlilik politikası
j) PC salonları kullanım kuralları, sorumlulukları ve gizlilik politikaları
k) Üniversite enformatik hizmetleri servis ve gizlilik politikaları

(4) Bu belge yayınlandığı tarihten itibaren geçerlidir.

KAYNAKÇA

5651 Sayılı Kanun. (2007). İnternet Ortamında Yapılan Yeyınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. 17 Kasım 2013 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf adresinden erişildi.

6518 Sayılı Kanun. (2014). Aile ve sosyal politikalar bakanlığının teşkilat ve görevleri hakkında kanun hükmünde kararname ile bazı kanun ve kanun hükmünde kararnamelerde değişiklik yapılmasına dair kanun. 19 Mart 2014 tarihinde http://www.resmigazete.gov.tr/eskiler/2014/02/20140219.pdf adresinden erişildi.

6533 Sayılı Kanun. (2014). Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun. 11 Kasım 2014 tarihinde http://www.tbmm.gov.tr/kanunlar/k6533.html adresinden erişildi.

AB Adalet Divanı. (2014a). C-131/12: Google Spain v AEPD and Mario Costeja Gonzalez. 12 Kasım 2014 tarihinde http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf adresinden erişildi.

AB Adalet Divanı. (2014b). The Court of Justice declares the Data Retention Directive to be invalid. 13 Nisan 2014 tarihinde http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf adresinden erişildi.

AİHM. (2009). Uslu / Türkiye Davası (No.2). 8 Aralık 2013 tarihinde http://www.hukukturk.com/fractal/hukukTurk/pages/findAihm0_n.jsp?pLayerOk=1&pPageDestination=findAihm0_n.jsp%3FpSMode4&pSMode=4&pObjectId=609&pMevzuatId=19007&pBasvuruNo=23815%2F04&i1.x=-391&i1.y=-240 adresinden erişildi.

Akipek, J., Akıntürk, T. ve Karaman, D. A. (2012). *Türk Medeni Hukuku: Başlangıç hükümleri - Kişiler hukuku*. İstanbul: Beta Yayınevi.

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

Anayasa Mahkemesi. (2008). Özel hayatın gizliliği ve korunması. 29 Ekim 2013 tarihinde http://www.hukukturk.com/fractal/hukukTurk/pages/find_n.jsp?pLayerOk=1&pObjectId=509&pViewId=486&pMainCategoryId=Anayasa&pEsasNo1=2006&pEsasNo2=167&pMerciId=4091&i1.x=16&i1.y=7 adresinden erişildi.

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

Anayasa Mahkemesi. (2014). 5651 sayılı Kanunun 8/5. ve 8/16. maddelerinin Anayasanın 2., 13., ve 20. maddelerine aykırılığı nedeniyle iptali. 6 Ocak 2015 tarihinde http://www.resmigazete.gov.tr/eskiler/2015/01/20150101-16.pdf adresinden erişildi.

Avrupa Adalet Divanı. (2003). Criminal proceedings against Bodil Lindqvist (Case C-101/01). Publication of personal data on the internet. 4 Ocak 2014 tarihinde

http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=623399 adresinden erişildi.

Avrupa Komisyonu. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. 8 Kasım 2013 tarihinde http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm adresinden erişildi.

Avrupa Komisyonu. (2000). 2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland. 6 Ocak 2014 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0518:EN:HTML adresinden erişildi.

Avrupa Komisyonu. (2001a). 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC. 25 Aralık 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:181:0019:0031:EN:PDF adresinden erişildi.

Avrupa Komisyonu. (2001b). Network and Information Security: Proposal for A European Policy Approach. 12 Ocak 2014 tarihinde http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf adresinden erişildi.

Avrupa Komisyonu. (2002). 2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act. 6 Ocak 2014 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002D0002:EN:HTML adresinden erişildi.

Avrupa Komisyonu. (2003). 2003/490/EC: Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina. 6 Ocak 2014 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003D0490:EN:HTML adresinden erişildi.

Avrupa Komisyonu. (2004a). 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries. 25 Aralık 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF adresinden erişildi.

Avrupa Komisyonu. (2004b). The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce. 26 Kasım 2013 tarihinde http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf adresinden erişildi.

Avrupa Komisyonu. (2008). 2008/49/EC: Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data. 26 Aralık 2013 tarihinde http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:013:0018:0023:EN:PDF adresinden erişildi.

Avrupa Komisyonu. (2010a). 2010/87/EU: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. 26 Aralık 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF adresinden erişildi.

Avrupa Komisyonu. (2010b). European Commission sets out strategy to strengthen EU data protection rules. 22 Aralık 2013 tarihinde http://europa.eu/rapid/press-release_IP-10-1462_en.pdf adresinden erişildi.

Avrupa Komisyonu. (2010c). MEMO/10/542: Data protection reform – frequently asked questions. 22 Aralık 2013 tarihinde http://europa.eu/rapid/press-release_MEMO-10-542_en.pdf adresinden erişildi.

Avrupa Komisyonu. (2011a). 2011/136/EU: Commission Recommendation of 1 March 2011 guidelines for the implementation of data protection rules in the Consumer Protection Cooperation System (CPCS). 26 Aralık 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:057:0044:0053:EN:PDF adresinden erişildi.

Avrupa Komisyonu. (2011b). *Action 28: Reinforced Network and Information Security Policy*. 22 Aralık 2013 tarihinde http://ec.europa.eu/digital-agenda/en/content/action-28-reinforced-network-and-information-security-policy adresinden erişildi.

Avrupa Komisyonu. (2011c). How will the data protection reform affect social networks? 23 Aralık 2013 tarihinde http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf adresinden erişildi.

Avrupa Komisyonu. (2011d). How will the EU's data protection reform benefit European businesses? 23 Aralık 2013 tarihinde http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/7_en.pdf adresinden erişildi.

Avrupa Komisyonu. (2011e). How will the EU's data protection reform make international cooperation easier? 23 Aralık 2013 tarihinde http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/5_en.pdf adresinden erişildi.

Avrupa Komisyonu. (2011f). How will the EU's data protection reform simplify the existing rules? 23 Aralık 2013 tarihinde http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/6_en.pdf adresinden erişildi.

Avrupa Komisyonu. (2011g). How will the EU's data protection reform strengthen the internal market? 23 Aralık 2013 tarihinde http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/4_en.pdf adresinden erişildi.

Avrupa Komisyonu. (2011h). How will the EU's reform adapt data protection rules to new technological developments? 23 Aralık 2013 tarihinde http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf adresinden erişildi.

Avrupa Komisyonu. (2011i). Why do we need an EU data protection reform? 23 Aralık 2013 tarihinde http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf adresinden erişildi.

Avrupa Komisyonu. (2012a). Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for

businesses. 22 Aralık 2013 tarihinde http://europa.eu/rapid/press-release_IP-12-46_en.pdf adresinden erişildi.

Avrupa Komisyonu. (2012b). How does the data protection reform strengthen citizens' rights? 22 Aralık 2013 tarihinde http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf adresinden erişildi.

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

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

Avrupa Komisyonu. (2013). *Action 12: Review the EU data protection rules*. 22 Aralık 2013 tarihinde http://ec.europa.eu/digital-agenda/en/pillar-i-digital-single-market/action-12-review-eu-data-protection-rules adresinden erişildi.

Avrupa Konseyi. (1992a). *92/242/EEC: Council Decision of 31 March 1992 in the field of security of information systems*. 18 Aralık 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31992D0242:EN:NOT adresinden erişildi.

Avrupa Konseyi. (1992b). Council Decision of 31 March 1992 in the field of security of information systems. 23 Aralık 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1992:123:0019:0025:EN:PDF adresinden erişildi.

Avrupa Konseyi. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 24 Kasım 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF adresinden erişildi.

Avrupa Konseyi. (1997). Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. 23 Aralık 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML adresinden erişildi.

Avrupa Konseyi. (2001a). Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows. 23 Aralık 2013 tarihinde http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm adresinden erişildi.

Avrupa Konseyi. (2001b). Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. 25 Aralık 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:EN:PDF adresinden erişildi.

Avrupa Konseyi. (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. 23 Aralık 2013 tarihinde http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML adresinden erişildi.

Avrupa Konseyi. (2003). Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security. 26 Aralık 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2003:048:0001:0002:EN:PDF adresinden erişildi.

Avrupa Konseyi. (2004a). Decision of the European Parliament and of the Council on establishing a multiannual Community programme on promoting safer use of the Internet and new online technologies. 25 Aralık 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0091:FIN:EN:PDF adresinden erişildi.

Avrupa Konseyi. (2004b). Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. 26 Aralık 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML adresinden erişildi.

Avrupa Konseyi. (2005). Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies. 23 Aralık 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0001:0013:EN:PDF adresinden erişildi.

Avrupa Konseyi. (2006). Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. 24 Aralık 2013 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF adresinden erişildi.

Avrupa Konseyi. (2012). Proposal for a Regulation of theEuropean Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

Avrupa Konseyi. (2013a). Consultative committee of the convention for the protection of ındividuals with regard to automatic processing of personal data. 04 Ocak 2014 tarihinde http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2014)WP_en_final.pdf adresinden erişildi.

Avrupa Konseyi. (2013b). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: Status as of: 21/11/2013. 21 Kasım 2013 tarihinde http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=21/11/2013&CL=ENG adresinden erişildi.

Avrupa Konseyi. (2013c). Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013, repealing Regulation (EC) No 460/2004. 26 Aralık 2013 tarihinde http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF adresinden erişildi.

Avrupa Konseyi. (2014). Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows. CETS No.: 181. 9 Kasım 2014 tarihinde http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=8&DF=&CL=ENG adresinden erişildi.

Avrupa Parlamentosu, Avrupa Konseyi ve Avrupa Komisyonu. (2000). Avrupa Birliği Temel Haklar Şartı. 27 Kasım 2013 tarihinde http://ekutup.dpt.gov.tr/ab/hukuk/temelhak.pdf adresinden erişildi.

Backhouse, J., Bener, A., Chauvidul, N., Wamala, F. ve Willison, R. (2005). Risk management in cyberspace. *Cyber Trust & Crime Prevention Project*, 349-379.

Barker , W. C. (2003). Guideline for Identifying an information system as a national security system: Information security. 24 Ekim 2013 tarihinde http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf adresinden erişildi.

BEHK. (2003). 4982 Sayılı Bilgi Edinme Hakkı Kanunu. 16 Kasım 2013 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.4982.pdf adresinden erişildi.

Bil.Güv.Müh. ABD. (2013). *Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Anabilim Dalı hakkında*. 15 Ocak 2014 tarihinde http://fbe-infosec.gazi.edu.tr/posts/view/title/hakkimizda-83050 adresinden erişildi.

BMD. (2007). *Bilgi güvenliğine AB kriteri*. 21 Aralık 2013 tarihinde http://www.bmd.org.tr/bilgi-guvenligine-ab-kriteri.html adresinden erişildi.

BTK. (2005). Elektronik İmza Kanununun Uygulanmasına İlişkin Usul Ve Esaslar Hakkında Yönetmelik. 16 Kasım 2013 tarihinde http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.7224&MevzuatIliski=0&sourceXmlSearch= adresinden erişildi.

California Information Practices Act. (2012). *Security Breaches Involving Personel Information*. 14 Ekim 2013 tarihinde http://cnc.ucr.edu/securitybreaches/ adresinden erişildi.

Cambridge University. (2012). *Privacy Policy for the Cambridge University Data Network*. 2 Şubat 2014 tarihinde http://www.ucs.cam.ac.uk/privacy/cudnprivacy adresinden erişildi.

Cambridge University. (2013). *Data Protection Act 1998*. 2 Şubat 2014 tarihinde http://www.admin.cam.ac.uk/univ/information/dpa/ adresinden erişildi.

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

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

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

CISCO. (2009). CCNA Security. 11 Ocak 2014 tarihinde http://www.cs.rpi.edu/~kotfid/secvoice10/powerpoints/CCNA_Security_01.ppt adresinden erişildi.

Cole, C. (2014). *Information security operations policy*. 11 Ekim 2014 tarihinde http://www.howard.edu/technology/docs/InformationSecurityOperationsPolicy_v3_UPC.pdf adresinden erişildi.

Constitution.eu. (2013). *Constitutions of Europe in English*. 28 Ekim 2013 tarihinde http://www.constitution.eu/ adresinden erişildi.

Crouhy, M., Galai, D. ve Mark, R. (2006). The Essentials of Risk Management. New York: McGraw-Hill.

Danagher, L. (2012). An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data? *European Journal of Law and Technology, 3*(3).

Data Protection Unit of the Directorate-General for Justice. (t.y.). Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries. 25 Aralık 2013 tarihinde http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf adresinden erişildi.

Davenport, T. H. ve Prusak, L. (2000). *Working knowledge*. Boston: Harvard Business Review Press.

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

Decker, L. G. (2011). *Factors affecting the security awareness of end-users: A survey analysis within institutions of higher learning.*: ProQuest.

Doğan, Y. H. (2005). Özel hayata ve hayatın gizli alanına karşı suçlar. 11 Kasım 2013 tarihinde http://www.ceza-bb.adalet.gov.tr/makale/146.doc adresinden erişildi.

Elektronik İmza Kanunu. (2004). 5070 sayılı Elektronik İmza Kanunu. 16 Kasım 2013 tarihinde http://www.tbmm.gov.tr/kanunlar/k5070.html adresinden erişildi.

ENISA. (2009). Cloud computing information assurance framework. 20 Aralık 2013 tarihinde http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport adresinden erişildi.

ENISA. (2011). *ENISA ad hoc Working Group on National Risk Management Preparedness*. Members of the ad-hoc Working Group, ENISA and ExecIA LLP.

ENISA. (2012). Consumerization of IT: Risk mitigation strategies - Responding to the emerging threat environment. 20 Aralık 2013 tarihinde http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/COITMitigationStategiesPublishedVersion.pdf adresinden erişildi.

ENISA. (2013). *ENISA Threat Landscape 2013: Overview of current and emerging cyber-threats*.

Erola, A., Castellà-Roca, J., Viejo, A. ve Mateo-Sanz, J. M. (2011). Exploiting social networks to provide privacy in personalized web search. *Journal of Systems and Software, 84*(10), 1734-1745.

Feiler, L. (2011). *Information Security Law in the EU and the U.S.: A Risk-Based Assessment of Implicit and Explicit Regulatory Policies*. 12 Ocak 2014 tarihinde http://fsi.stanford.edu/research/information_security_law_in_the_eu_and_the_us

_a_riskbased_assessment_of_implicit_and_explicit_regulatory_policies adresinden erişildi.

FERPA. (1974). Family educational and privacy rights. 2 Aralık 2013 tarihinde http://www.gpo.gov/fdsys/pkg/USCODE-2011-title20/pdf/USCODE-2011-title20-chap31-subchapIII-part4-sec1232g.pdf adresinden erişildi.

Filippi, P. ve Belli, L. (2012). The law of the cloud v the law of the land : Challenges and opportunities for innovation. *European Journal of Law and Technology, 3*(2), 1-23.

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

Fowler, K. L., Kling, N. D. ve Larson, M. D. (2007). Organizational preparedness for coping with a major crisis or disaster. *Business & Society, 46*(1), 88-103.

Garigue, R. (2007). Understanding the new information risks: The requirement for a new information security conceptual framework. *EDPACS: The EDP Audit, Control & Security Newsletter, 35*(3), 1-9.

Gillon, K., Branz, L., Culnan, M., Dhillon, G. ve Hodgkinson, R. (2011). Information Security and Privacy - Rethinking Governance Models. *Communications of the Association for Information Systems*, 561-570.

Google. (2014). *Aramada içerik kaldırmaya ilişkin Avrupa gizlilik talepleri*. 12 Kasım 2014 tarihinde http://www.google.com/transparencyreport/removals/europeprivacy/ adresinden erişildi.

Grama, J. L. (2010). *Legal Issues in Information Security*. Sudbury: Jones & Bartlett Learning.

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108. *Edinburgh School of Law Research Paper*(12), 1-34.

Greenleaf, G. (2013a). Global Tables of Data Privacy Laws and Bills. *UNSW Law Research Paper*, 1-10.

Greenleaf, G. (2013b). Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories. *Journal of Law, Information & Science*.

Hafızoğulları, Z. ve Özen, M. (2009). Özel hayata ve hayatın gizli alanına karşı suçlar. *Ankara Barosu Dergisi*(4), 9-22.

Hanks, N. (2013). *What small businesses need to know about information security*. 8 Ocak 2014 tarihinde http://www.smallbusinessbc.ca/growing-a-business/what-small-businesses-need-know-about-information-security adresinden erişildi.

Hannover University. (2014). *Data protection*. 2 Şubat 2014 tarihinde http://www.tib.uni-hannover.de/en/service/data-protection.html adresinden erişildi.

Harvard Infosec. (2013). Data classification and examples. 11 Ekim 2014 tarihinde http://security.harvard.edu/files/it-security-new/files/info_security_data_classification_table_abridged_8.12.14_3.pdf adresinden erişildi.

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

Henkoğlu, T. ve Külcü, Ö. (2013). Evaluation of Conditions Regarding Cloud Computing Applications in Turkey, EU and the USA. *Beyond the Cloud: Information… Innovation… Collaboration…*, 4.

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

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

HKSAR. (2008). *An overview of information security standarts*. The Government of the Hong Kong Special Administrative Region.

Höne, K. ve Eloff, J. H. P. (2002). Information security policy - what do international information security standards say? *Computers & Security, 21*(5), 402-409.

HÜ. BİDB. (2013). Hacettepe Üniversitesi elektronik imza kullanma rehberi. 16 Kasım 2013 tarihinde http://www.bidb.hacettepe.edu.tr/eimza/index.php adresinden erişildi.

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

Indiana University. (2012). Red-Hot Data: A guide to safe handling of critical information. 23 Ocak 2014 tarihinde https://protect.iu.edu/sites/default/files/SensitiveDataFlippyBook2012.pdf adresinden erişildi.

INVISUS. (2014). *Information security laws and regulations that affect your business*. 8 Ocak 2014 tarihinde http://www.invisus.com/is_security_regs.php adresinden erişildi.

ISO/IEC. (2008). ISO/IEC 27001:2005. 8 Aralık 2013 tarihinde http://www.iso.org/iso/catalogue_detail?csnumber=42103 adresinden erişildi.

Johnston, L. (2011). Guidelines on information security. 26 Ekim 2013 tarihinde http://www.belb.org.uk/downloads/foi_guidelines_on_information_security.pdf adresinden erişildi.

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

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

Kaya, M. (2010). Telekomünikasyon alanında kişilik haklarının korunması. *Ankara Barosu Dergisi, 68*(4), 279-334.

Kayrak, M. (2012). Bilgi kriterleri çerçevesinde bilişim teknolojileri denetimi. (87) 143-167.22 Aralık 2013 tarihinde http://dergi.sayistay.gov.tr/icerik/der87m7.pdf adresinden erişildi.

Ketizmen, M. (2008). *Türk Ceza Hukukunda Bilişim Suçları*. Ankara: Adalet Yayınevi.

Kılıçoğlu, A. (2013). *Şeref, haysiyet ve özel yaşama basın yoluyla yapılan saldırılardan hukuksal sorumluluk*. Ankara: Turhan Kitabevi.

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

Kurbanoğlu, S. (2004). *Kaynak gösterme el kitabı*. Ankara: ÜNAK.

Külcü, Ö. ve Henkoğlu, T. (2014). Privacy in social networks: An analysis of Facebook. *International Journal of Information Management, 34*(6), 761-769.

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

Küzeci, E. (2011). Anayasal bir hak: Kişisel verilerin korunması. *Bilişim Dergisi*(128), 142-149.

Landwehr, C. E. (2001). Computer security. *International Journal of Information Security, 1*(1).

Maconachy, W. V., Schou, C. D., Ragsdale, D. ve Welch, D. (2001). A model for information assurance: An integrated approach. 12 Ocak 2014 tarihinde

http://it210web.groups.et.byu.net/lectures/MSRW%20Paper.pdf adresinden erişildi.

Margulis, S. T. (1977). Conceptions of Privacy: Current Status and Next Steps. *Journal of Social Issues, 33*(3), 5-21.

McCumber, J. (2005). *Assessing and managing security risk in IT systems: A structured methodology*. Florida: CRC Press LLC.

MEB. (2014). Kişisel verilerin korunması. 12 Şubat 2014 tarihinde http://afyon.meb.gov.tr/2014/02/11/595433.pdf adresinden erişildi.

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

Mitnick, K. D. ve Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley Pub.

Netherlands Constitution. (2008). The Constitution of the Kingdom of the Netherlands. 28 Ekim 2013 tarihinde http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2008/10/20/the-constitution-of-the-kingdom-of-the-netherlands-2008/07br2008g109.pdf adresinden erişildi.

NIST. (2009). Recommended security controls for federal information systems and organizations. 21 Ocak 2014 tarihinde http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf adresinden erişildi.

NSTISSI. (1994). National Training Standard for Information Systems Security (INFOSEC) Professionals. 18 Ocak 2014 tarihinde http://www.scis.nova.edu/documents/nstissi_4011.pdf adresinden erişildi.

ODTÜ BİDB. (2008). ODTÜ yerel alan ağında 5651 Sayılı Kanun uyarınca uyulması gereken kurallar. 17 Kasım 2013 tarihinde http://www.metu.edu.tr/5651/files/5651_sayili_kanunun_uygulanma_kurallari_v1.0.pdf adresinden erişildi.

OECD. (2002). OECD Guidelines for the security of information systems and networks: Towards a culture of security. 26 Aralık 2013 tarihinde http://www.oecd.org/sti/ieconomy/15582260.pdf adresinden erişildi.

Ottekin, F. (2008). TS ISO/IEC 27001 Denetim Listesi. 7 Aralık 2013 tarihinde https://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys0013-iso-iec-27001-denetim-listesi/download.html adresinden erişildi.

Oxford University. (2013). *University Policy on Data Protection*. 2 Şubat 2014 tarihinde http://www.admin.ox.ac.uk/councilsec/compliance/dataprotection/policy/ adresinden erişildi.

Özdemirci, F. (2012). Üniversitelerde e-İmza Kullanımı ve Elektronik Belge Yönetim Sistemi (EBYS) Uygulamaları: Ankara Üniversitesi Deneyimi. 16 Kasım 2013 tarihinde http://beyas.ankara.edu.tr/dosyalar/Sunumlar_ve_seminerler/1_Kamu_SM_Fahrettin_sunum22_11_2012 adresinden erişildi.

Özenç Uçak, N. (2010). Bilgi: Çok yüzlü bir kavram. *Türk Kütüphaneciliği, 24*(4), 705-722.

Privacy International. (2013). *Data protection and privacy laws*. 21 Ekim 2013 tarihinde https://www.privacyinternational.org/issues/data-protection-and-privacy-laws adresinden erişildi.

PrivacyRightsClearinghouse. (2014). *Chronology of data breaches: Security breaches 2005 - Present*. 19 Kasım 2014 tarihinde https://www.privacyrights.org/data-breach adresinden erişildi.

Reding, V. (2013). Data protection reform: restoring trust and building the digital single market. 22 Aralık 2013 tarihinde http://europa.eu/rapid/press-release_SPEECH-13-720_en.pdf adresinden erişildi.

Rhee, H.-S., Ryu, Y. ve Kim, C.-T. (2005). I am fine but you are not: Optimistic bias and illusion of control on information security. *ICIS 2005 Proceedings*, 381-394.24 Ocak 2014 tarihinde http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1238&context=icis2005 adresinden erişildi.

Rubin, A. ve Babbie, E. R. (2011). *Research methods for social work* (7 ed.). Belmond: Cengage Learning.

Sasse, M. A., Brostoff, S. ve Weirich, D. (2001). Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122-131.

Schartum, D. W. (2008). Designing and formulating data protection laws. *International Journal of Law and Information Technology, 18*(1), 1-27.

Schwartz, P. M. (2012). The E.U.-US Privacy Collision: A Turn to Institutions and Procedures. 25 aralık 2013 tarihinde http://www.harvardlawreview.org/symposium/papers2012/schwartz.pdf adresinden erişildi.

Simitis, S. (1995). From the market to the polis: The EU Directive on the Protection of Personal Data. *80 Iowa Law Review*, 445-470.

Simpson, J. J. ve Endicott-Popovsky, B. (2010). A systematic approach to information systems security education. 15 Ocak 2014 tarihinde http://systemsconcept.org/static_files/2010/CISSE10_SAISSE.pdf adresinden erişildi.

Solomon, M. G. ve Chapple, M. (2005). *Information Security Illuminated* London: Jones and Bartlett Publishers.

STA. (2007). Ergun Özbudun'un hazırladığı anayasa taslağı. 28 Ekim 2013 tarihinde http://www.siviltoplumakademisi.org.tr/index.php?option=com_content&id=387:ergun-ozbudun&Itemid=130 adresinden erişildi.

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

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

Stoneburner, G., Goguen, A. ve Feringa, A. (2002). Risk management guide for information technology systems. 24 Ekim 2013 tarihinde http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf adresinden erişildi.

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

Stutzman, F., Gross, R. ve Acquisti, A. (2012). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Condentiality, 4*(2), 7-41.

Şimşek, O. (2008). *Anayasa Hukukunda kişisel verilerin korunması*. İstanbul: Beta Yayınevi.

T.C. AB Bakanlığı. (2003). 2003 Yılı Ulusal Program Dökümanları. 19 Kasım 2013 tarihinde http://www.ab.gov.tr/files/UlusalProgram/UlusalProgram_2003/Tr/pdf/IV-24.pdf adresinden erişildi.

T.C. AB Bakanlığı. (2010). Türkiye'nin AB müktesebatına uyum programı (2007-2013): Yargı ve temel haklar. 18 Kasım 2013 tarihinde http://www.abgs.gov.tr/files/Muktesebat_Uyum_Programi/23_YargiveTemelHaklar.pdf adresinden erişildi.

T.C. AB Bakanlığı. (2011). *23. Fasıl: Yargı ve temel haklar*. 27 Kasım 2013 tarihinde http://www.abgs.gov.tr/index.php?p=88&l=1 adresinden erişildi.

T.C. AB Bakanlığı. (2013). Avrupa Birliği müzakere sürecinde yargı ve temel haklar faslı. 28 Kasım 2013 tarihinde http://www.abgs.gov.tr/files/yargivetemelhaklar/yargi_ve_temel_haklar_kitap.pdf adresinden erişildi.

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

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

T.C. Başbakanlık. (2008a). Elektronik belge standartları. 19 Ekim 2014 tarihinde http://www.resmigazete.gov.tr/eskiler/2008/07/20080716-7.htm adresinden erişildi.

T.C. Başbakanlık. (2008b). Kişisel Verilerin Korunması Kanun Tasarısı ve Gerekçesi. 25 Kasım 2013 tarihinde http://www2.tbmm.gov.tr/d23/1/1-0576.pdf adresinden erişildi.

T.C. Başbakanlık. (2011). AB Antlaşması ve AB'nin İşleyişi Hakkında Antlaşma. 30 Kasım 2013 tarihinde http://www.abgs.gov.tr/files/pub/antlasmalar.pdf adresinden erişildi.

T.C. Başbakanlık. (2014a). Kişisel Verilerin Korunması Kanun Tasarısı ve Gerekçesi. 30 Aralık 2014 tarihinde http://web.tbmm.gov.tr/gelenkagitlar/metinler/362939.pdf adresinden erişildi.

T.C. Başbakanlık. (2014b). Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı. 10 Kasım 2014 tarihinde http://www2.tbmm.gov.tr/d24/1/1-0966.pdf adresinden erişildi.

T.C. Kalkınma Bakanlığı. (2013). Bilgi Toplumu Stratejisinin Yenilenmesi Projesi: İhtiyaç Tespiti ve Öneriler Raporu. 2 Aralık 2013 tarihinde http://www.bilgitoplumustratejisi.org/download/docfile/8a32476640e074570140e4c3388b0004 adresinden erişildi.

TCK. (2004). Türk Ceza Kanunu. 29 Ekim 2013 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf adresinden erişildi.

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

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

TÜBİTAK UEKAE. (2014). Kamu Sertifikasyon Merkezi Nitelikli Elektronik Sertifika Raporu. 25 Eylül 2014 tarihinde http://rpr.kamusm.gov.tr/GenelRaporlar/rdPage.aspx adresinden erişildi.

Uludağ Üniversitesi. (2013). Üniversaite, e-evrakla hem hızlandı hem de tasarruf etti. 16 Kasım 2013 tarihinde http://www.uludag.edu.tr/haberler/oku/dn/771 adresinden erişildi.

Waguespack, L. J. (2013). Computer security primer: Systems architecture, special ontology and cloud virtual machines. *Proceedings of the Information Systems Educators Conference*.

Warren, S. D. ve Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5).

Westervelt, R. (2013). *The 10 Biggest Data Breaches Of 2013*. 08 Ocak 2014 tarihinde http://www.crn.com/slide-shows/security/240159149/the-10-biggest-data-breaches-of-2013-so-far.htm?pgno=1 adresinden erişildi.

White, A. (1997). Control of Transborder Data Flow: Reactions to the European Data Protection Directive. *International Journal of Law and Information Technology, 5*(2), 230-247.

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

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

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

Wong, R. (2013). *Data Security Breaches and Privacy in Europe*. London: Springer.

Yüksel, M. (2003). Mahremiyet hakkı ve sosyo-tarihsel gelişimi. *Ankara Üniversitesi SBF Dergisi, 1*(58), 181-213.

Zevkliler, A., Gökyayla, E. ve Acabey, B. (2000). *Medeni hukuk: Giriş, başlangıç hükümleri, kişiler hukuku, aile hukuku*. Ankara: Seçkin Yayıncılık.

EK 1. Üniversite Bilgi İşlem Daire Başkanlığı Değerlendirme Anketi

Aşağıda, akademik bir çalışmada kullanılmak üzere hazırlanmış anket soruları yer almaktadır. Kapsamlı bir bilgi güvenliği politikasının oluşturulabilmesi ve üniversitelerde kişisel verilerin daha üst düzeyde korunmasının sağlanabilmesi amacıyla yapılan bu çalışmada, düşünce ve önerileriniz bizim için son derece önemlidir. Bu çalışma kapsamında elde edilen araştırma verileri büyük bir gizlilik içinde saklanarak kişi, kurum ve kuruluşlarla paylaşılmayacak ve çalışma içinde üniversite isimleri belirtilmeyecektir.

(Anket İçinde Kullanılan Kısaltmalar: PDB: Personel Daire Başkanlığı, BİDB: Bilgi İşlem Daire Başkanlığı)

1.	Üniversite birimlerinde hangi bilgisayarlar üzerinde kişisel verilerin işlendiği bilinmekte midir?	☐ Evet	☐ Hayır	☐ Fikrim Yok
2.	Aşağıdakilerden hangileri BİDB sorumluluğundaki sunucularda merkezi olarak tutulmaktadır? (*Birden fazla seçeneği işaretleyebilirsiniz*) ☐ PDB tarafından işlenen personel bilgileri ☐ Bilgi merkezi tarafından işlenen kullanıcı bilgileri ve veri tabanı erişim kayıtları ☐ BİDB tarafından işlenen kullanıcı bilgileri kapsamında elde edilen veriler ☐ Üniversite web sayfasına yapılan erişimlere ilişkin kayıtlar ☐ Diğer (……..)			
3.	Üniversitenin yayımlamış olduğu bir yazılı bilgi güvenliği politikası var mı? Cevabınız "*EVET*" ise bu politikalara nereden erişilebilir?	☐ Evet (……) ☐ Hayır ☐ Fikrim Yok		
4.	Bilgi güvenliği politikası kapsamlı teknik ve hukuksal önlemleri içeriyor mu?	☐ Evet	☐ Hayır	☐ Fikrim Yok
5.	Bilgi güvenliği politikası kişisel verilerin korunmasına ilişkin hususları içeriyor mu?	☐ Evet	☐ Hayır	☐ Fikrim Yok
6.	Verilerin imha işleminin nasıl yapılacağına ilişkin belirlenmiş bir politika bulunmakta mıdır?	☐ Evet	☐ Hayır	☐ Fikrim Yok
7.	Kişisel verilerin korunmasına ilişkin bilgi güvenliği politikalarının olması iş süreci ve sorumluluğun tanımlanmasını kolaylaştırır mı?	☐ Evet	☐ Hayır	☐ Fikrim Yok
8.	Bilgi güvenliği konusunda özel olarak görevlendirilmiş personel bulunuyor mu? *Cevabınız "*EVET*" ise eğitim durumu nedir? *Cevabınız "*HAYIR*" ise bu konuda uzman personele ihtiyaç duyuluyor mu?	☐ Evet (……..……) ☐ Hayır (……..)		
9.	Bilgi güvenliği amacıyla "kriptolama" yöntemi kullanılıyor mu?	☐ Evet	☐ Hayır	
10.	Kişisel verilerin bütünlüğü için "hash" değeri hesaplanıyor mu?	☐ Evet	☐ Hayır	
11.	Alınan bilgi güvenliği önlemleri verinin gizliliğini koruyor mu?	☐ Evet	☐ Hayır	
12.	Alınan bilgi güvenliği önlemleri bireylerin kişisel hak ve özgürlüğünü koruyor mu?	☐ Evet	☐ Hayır	
13.	Kişisel verilerin işlendiği ya da depolandığı bilgisayarların oturum açma kayıtları tutuluyor mu?	☐ Evet	☐ Hayır	
14.	Üzerinde kişisel bilgi bulunan bilgisayarlar uygun etiketlendirme ve ikaz notları ile işaretleniyor mu?	☐ Evet	☐ Hayır	
15.	Üzerinde kişisel bilgi bulunan bilgisayarların güvenlik denetimleri yapılıyor mu? Cevabınız "*EVET*" ise bu denetimler kim tarafından ve hangi sıklıkta yapılıyor? ☐ Evet (……..……..) ☐ Hayır			

16. Kişisel verilerin korunmasına yönelik ne tür teknik ve idari önlemler alınıyor?
(……
……)

17. Sistem güvenlik testleri yapılıyor mu? Cevabınız "*EVET*" ise kim tarafından (sistemi tasarlayan ya da dışarıdan) yapılıyor?
☐ Evet (…….……..)
☐ Hayır

18. Sistem güvenlik testleri yapılırken veri tabanında bulunan kişisel ve hassas veriler de kullanılıyor mu? ☐ Evet ☐ Hayır

19. Bilgi varlıklarının hangi yasal düzenlemeler kapsamında korunduğu açık olarak belirtiliyor mu? Cevabınız "*EVET*" ise bu bilgilere nereden erişilebilir?
☐ Evet (…….……..)
☐ Hayır

20. Kişisel verilerin korunmasına ilişkin olarak hangi hukuksal düzenlemeler çerçevesinde sorumluluklarınız olduğunu düşünüyorsunuz? (*Birden fazla seçeneği işaretleyebilirsiniz*)
☐ T.C. Anayasası
☐ Türk Ceza Kanunu
☐ 5651 Sayılı Kanun
☐ Kişisel Verilerin Korunması Kanunu Tasarısı
☐ Avrupa Birliği Veri Koruma Kanunu
☐ Hukuksal çerçevede sorumluluğumun olduğunu düşünmüyorum

21. Bilgi güvenliği ve kişisel verilerin korunması konusunda hukuksal düzenlemeleri yeterli buluyor musunuz? ☐ Evet ☐ Hayır ☐ Fikrim Yok

22. Üniversite üst yönetim kademelerinde bilgi güvenliğinin sağlanması konusuna önem verildiğini düşünüyor musunuz? ☐ Evet ☐ Hayır ☐ Fikrim Yok

23. Bilgi güvenliği sorumluluğu üniversitenin tüm birimleri tarafından paylaşılıyor mu? ☐ Evet ☐ Hayır ☐ Fikrim Yok

24. Üniversite personelinin görev tanımında kişisel bilgilerin korunmasına ilişkin sorumluluklar açık olarak belirtiliyor mu? ☐ Evet ☐ Hayır ☐ Fikrim Yok

25. Üniversitede birimlerinin "bilişim sorumluları" yazılı olarak belirlenmiş mi? ☐ Evet ☐ Hayır ☐ Fikrim Yok

26. Üniversitedeki bilişim faaliyetlerinin düzenlenmesi amacıyla kurulan bir "bilişim komisyonu" bulunuyor mu? Cevabınız "*EVET*" ise komisyonda kişisel verilerin korunmasına ilişkin konular gündeme getiriliyor mu?
☐ Evet (……)
☐ Hayır
☐ Fikrim Yok

27. PDB ve Bilgi Merkezi tarafından kaydedilen kişisel bilgilerin sorumluluğu nasıl paylaşılıyor?
(……)

28. Kişisel verilerin ihlal edilmesi durumunda aşağıdakilerden hangileri haberdar edilmektedir? (Birden fazla seçeneği işaretleyebilirsiniz)
☐ Savcılık
☐ Bağlı bulunulan idari amir
☐ Kişisel verileri ihlal edilen kişi
☐ Haber verilmeksizin en kısa sürede sistem yeniden aktif hale getirilir
☐ Diğer (……..…….)

29. Kişisel bilgileri içeren kayıtlar hangi sıklıkta yedeklenmektedir?
(……)

30. Kişisel veriler sınıflandırılarak diğer verilerden ayrı fiziksel ortamlarda saklanıyor mu? ☐ Evet ☐ Hayır

31.	Kişisel verilerin bulunduğu bilgisayarların farklı sanal ağlar üzerinde bulunması sağlanıyor mu?		☐ Evet	☐ Hayır
32.	Bilgi güvenliğinin sağlanmasına yönelik donanımsal gereksinimler yönetim tarafından ivedilikle karşılanıyor mu?	☐ Evet	☐ Hayır	☐ Kısmen
33.	Bilgi Sistemlerinin bakım/onarımı için dışarıdan destek alınıyor mu?	☐ Evet	☐ Hayır	☐ Kısmen
34.	Dışarıdan destek veren şirket çalışanları için güvenlik araştırması yapılıyor mu?	☐ Evet	☐ Hayır	☐ Kısmen
35.	Üniversitede yapılmış bir bilgi varlığı değerlendirmesi ve risk analizi raporu bulunuyor mu?		☐ Evet	☐ Hayır
36.	Herhangi bir veri ihlali olması durumunda uygulanabilecek bir yazılı eylem planınız var mı?		☐ Evet	☐ Hayır
37.	Kişisel verilerin bulunduğu veri tabanlarına yönelik saldırı girişimleri oluyor mu? Cevabınız "*EVET*" ise ne sıklıkla oluyor?	☐ Evet (……) ☐ Hayır ☐ Fikrim Yok		
38.	Herhangi bir veri ihlali olması durumunda tüm bilgi sistemlerinin yeniden aktif hale getirilmesi ne kadar zaman almaktadır? (……)			
39.	Üniversite birimde kullanım süresi dolan sabit disklerin imhasından kim sorumludur? ☐ Bilgisayarın bulunduğu ilgili birim ☐ Üniversite BİDB ☐ Bu konuda belirlenmiş bir sorumluluk bulunmamaktadır ☐ Diğer (…….)			

Konuya ilişkin olarak ilâve etmek istediğiniz görüş ve öneriler

Katkılarınız için teşekkür ederiz.

EK 2. Üniversite Personel Daire Başkanlığı Değerlendirme Anketi

Aşağıda, akademik bir çalışmada kullanılmak üzere hazırlanmış anket soruları yer almaktadır. Araştırmada kullanılan sorular, kapsamlı bir bilgi güvenliği politikasının oluşturulabilmesi ve üniversitelerde kişisel verilerin daha üst düzeyde korunmasının sağlanabilmesi için gerekli bilgi ve önerileri elde etmeye yönelik olarak hazırlanmıştır. Bu çalışma kapsamında elde edilen araştırma verileri büyük bir gizlilik içinde saklanarak kişi, kurum ve kuruluşlarla paylaşılmayacak ve çalışma içinde üniversite isimleri belirtilmeyecektir.

(Anket İçinde Kullanılan Kısaltmalar: PDB: Personel Daire Başkanlığı, BİDB: Bilgi İşlem Daire Başkanlığı)

1. Kişisel verilerin korunması konusunda yazılı bilgi güvenliği politikanız var mı? Cevabınız "*EVET*" ise bu politikalara nereden erişilebilir?
   ☐ Evet (……)
   ☐ Hayır
   ☐ Fikrim Yok
2. Kişisel verilerin korunmasına ilişkin bilgi güvenliği politikalarının olması iş süreci ve sorumluluğunuzu belirlemeye katkısı olur mu?
   ☐ Evet ☐ Hayır ☐ Fikrim Yok
3. Personel kayıtlarının korunmasına ilişkin olarak hangi hukuksal düzenlemeler çerçevesinde sorumluluklarınız olduğunu düşünüyorsunuz? (*Birden fazla seçeneği işaretleyebilirsiniz*)
   ☐ T.C. Anayasası
   ☐ Türk Ceza Kanunu
   ☐ 5651 Sayılı Kanun
   ☐ Kişisel Verilerin Korunması Kanunu Tasarısı
   ☐ Avrupa Birliği Veri Koruma Kanunu
   ☐ Hukuksal çerçevede sorumluluğumun olduğunu düşünmüyorum
4. Bilgi güvenliği kapsamında dikkate alınan uluslararası standartlar ya da mesleki etik ilkeler var mıdır? Cevabınız "*EVET*" ise lütfen isimlerini yazınız.
   ☐ Evet (……..……..)
   ☐ Hayır
5. Personel bilgilerinin ihlali halinde uygulanacak yaptırımlar belirlenmiş midir? Cevabınız "*EVET*" ise bu yaptırımlar nelerdir?
   ☐ Evet (……..……..)
   ☐ Hayır
6. Personele ait hangi bilgilerin toplanacağına nasıl karar verilmektedir?
   (……...…)
7. Kişilerin kendisine ait toplanan tüm veriler hakkında bilgisi var mıdır?
   ☐ Evet ☐ Hayır
8. Personele ait kayıtların hangi gerekçe ile paylaşımına izin verilmektedir? (*Birden fazla seçeneği işaretleyebilirsiniz*)
   ☐ Yasal çerçevede savcılık tarafından istenmesi durumunda
   ☐ Bilgi Edinme Hakkı Kanunu çerçevesinde
   ☐ İstatistiksel 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
   ☐ Personel bilgileri hangi sebeple olursa olsun verilmez.

9. Sekizinci soru kapsamında personele ait kayıtların paylaşılması durumunda ilgili personele bilgi veriliyor mu? ☐ Evet ☐ Hayır ☐ Bazen

10. Kişisel bilgilerin amaç dışı kullanımı, korunması ve izinsiz olarak paylaşımına ilişkin personele yazılı taahhütte bulunulmakta mıdır? ☐ Evet ☐ Hayır

11. Personel kayıtları içeren belgeler gizlilik seviyesine göre sınıflandırılıyor mu? ☐ Evet ☐ Hayır ☐ Kısmen

12. Personel kayıtları içeren belgeler hangi ortamda saklanıyor? (Birden fazla seçeneği işaretleyebilirsiniz)
    - ☐ Şifreli/korumalı dolaplarda
    - ☐ Şifresiz/korumasız klasör ya da dolaplarda
    - ☐ Merkezi olarak Per. Daire Bşk. (PDB) içinde bulunan sunucu bilgisayarda
    - ☐ Merkezi olarak BİDB.lığı içinde bulunan sunucu bilgisayarda
    - ☐ Diğer (…….…….)

13. Personel kayıtları <u>hangi sıklıkta</u> gözden geçiriliyor ya da güncelleniyor? (*Birden fazla seçeneği işaretleyebilirsiniz*)
    - ☐ Personel bilgilerinde değişme olduğunda
    - ☐ Görevde yükselme, sicil, ilişik kesme vb. işlemler sırasında
    - ☐ Diğer (……..…….)

14. Aşağıdaki seçeneklerden hangilerinin personel ile ilişkilendirilmesi halinde "hassas" ya da "kişisel veri" kapsamında korunması gerektiğini düşünüyorsunuz? (*Birden fazla seçeneği işaretleyebilirsiniz*)
    - ☐ Personelin sicil bilgileri
    - ☐ Personelin PDB kaynaklarına bağlandığı IP adresi
    - ☐ Personelin kimlik bilgileri (Ad-Soyad, TC kimlik numarası vd.)
    - ☐ Personelin iletişim bilgileri (adres, telefon, e-posta adresi vd.)
    - ☐ Personelin akademik özgeçmişine ilişkin bilgiler
    - ☐ Personelin etnik, din, dil, ırk bilgileri
    - ☐ Hiçbiri

15. Personel kayıtlarının ne kadar süre ile saklanacağı yazılı olarak belirlenmiş midir? Cevabınız "*EVET*" ise bu süre nedir? ☐ Evet (……..……...) ☐ Hayır

16. Belge güvenliği için elektronik imza kullanılıyor mu? Cevabınız "*EVET*" ise e-imza sertifika süresi dolan belgelere nasıl işlem yapılıyor?
    - ☐ Evet (…….……..)
    - ☐ Hayır

17. Personel bilgilerinin kaydedildiği bilgisayarların ya da sabit disklerinin kullanım ömrü dolması halinde hangi işlem yapılmaktadır?
    - ☐ BİDB'lığı tarafından değişimi yapılmaktadır
    - ☐ Yeni bilgisayarların kurulumu yapılarak eskileri çöpe atılmaktadır
    - ☐ Eski sabit diskler özel imha işlemine tabi tutulmaktadır.
    - ☐ Bilgi sahibi değilim.
    - ☐ Diğer (…….……....)

18. Personel kayıtlarını içeren belgeler nasıl imha ediliyor?
    (……...…)

19. Kişisel verilerin korunmasına ilişkin olarak bilgilendirildiniz mi? Cevabınız "*EVET*" ise ne tür toplantılara katıldınız? Toplantılar hangi sıklıkta ve hangi birim tarafından yapılıyor?
    - ☐ Evet (…….……..)
    - ☐ Hayır

20. Kişisel verilerin korunmasına ilişkin birtakım teknik önlemlerin alınması konusunda sorumluluklarınız bulunuyor mu? Cevabınız "*EVET*" ise ne tür sorumluluklarınız bulunuyor?
    ☐ Evet (…….……..)
    ☐ Hayır
    ☐ Fikrim Yok
21. Personel bilgilerinin kaydedildiği bilgisayarların internet bağlantısı bulunuyor mu? ☐ Evet ☐ Hayır
22. Kişisel verilerin ihlal edilmesi durumunda aşağıdakilerden hangileri haberdar edilmektedir? (Birden fazla seçeneği işaretleyebilirsiniz)
    ☐ Savcılık
    ☐ Bilgi İşlem Daire Başkanlığı
    ☐ Bağlı bulunulan idari amir
    ☐ Kişisel verileri ihlal edilen kişi
    ☐ Haber verilmeksizin en kısa sürede sistem yeniden aktif hale getirilir
    ☐ Diğer (……..…….)
23. Personel bilgilerinin kaydedildiği bilgisayarlarda oturum açma işlemi nasıl uygulanmaktadır?
    ☐ Her kullanıcı sadece kendi kullanıcı adı ile oturum açabilmektedir
    ☐ Ortak kullanıcı hesabı ile oturum açılmaktadır
    ☐ Ortak ya da kişiye özel kullanıcı adı ve şifresi ile oturum açılabilmektedir
    ☐ Oturum açmak için kullanıcı adı ve parola ihtiyaç duyulmamaktadır
24. Personele ait kişisel verilerin korunmasına ilişkin önlemleri öncelik sırasına göre "1" (en öncelikli) ile "5" arasında sıralayınız. Sorumluluğunuz olmadığını düşünüyorsanız ilgili seçeneği işaretleyiniz.
    ☐ Hukuksal düzenlemeler kapsamında korunmalıdır
    ☐ Teknik önlemler alınmalıdır
    ☐ İdari önlemler alınmalıdır
    ☐ Etik ilkeler çerçevesinde korunmalıdır
    ☐ Kişisel verilerin korunması PDB'nin sorumluluklarından biri değildir

Konuya ilişkin olarak ilâve etmek istediğiniz görüş ve öneriler

Katkılarınız için teşekkür ederiz.

EK 3. Üniversite Bilgi Merkezi Değerlendirme Anketi

Aşağıda, akademik bir çalışmada kullanılmak üzere hazırlanmış anket soruları yer almaktadır. Kapsamlı bir bilgi güvenliği politikasının oluşturulabilmesi ve üniversitelerde kişisel verilerin daha üst düzeyde korunmasının sağlanabilmesi amacıyla yapılan bu çalışmada, düşünce ve önerileriniz bizim için son derece önemlidir. Bu çalışma kapsamında elde edilen araştırma verileri büyük bir gizlilik içinde saklanarak kişi, kurum ve kuruluşlarla paylaşılmayacak ve çalışma içinde üniversite isimleri belirtilmeyecektir.

(Anket İçinde Kullanılan Kısaltmalar: PDB: Personel Daire Başkanlığı, BİDB: Bilgi İşlem Daire Başkanlığı)

1. Kişisel verilerin korunması konusunda yazılı bilgi güvenliği politikanız var mı? Cevabınız "*EVET*" ise bu politikalara nereden erişilebilir?
   ☐ Evet (……)
   ☐ Hayır
   ☐ Fikrim Yok
2. Kişisel verilerin korunmasına ilişkin bilgi güvenliği politikalarının olması iş süreci ve sorumluluğunuzu belirlemeye katkısı olur mu?
   ☐ Evet ☐ Hayır ☐ Fikrim Yok
3. Kullanıcı kayıtlarının korunmasına ilişkin olarak hangi hukuksal düzenlemeler çerçevesinde sorumluluklarınız olduğunu düşünüyorsunuz? (*Birden fazla seçeneği işaretleyebilirsiniz*)
   ☐ T.C. Anayasası
   ☐ Türk Ceza Kanunu
   ☐ 5651 Sayılı Kanun
   ☐ Kişisel Verilerin Korunması Kanunu Tasarısı
   ☐ Avrupa Birliği Veri Koruma Kanunu
   ☐ Hukuksal çerçevede sorumluluğumun olduğunu düşünmüyorum
4. Bilgi güvenliği kapsamında dikkate alınan uluslararası standartlar ya da mesleki etik ilkeler var mıdır? Cevabınız "*EVET*" ise lütfen isimlerini yazınız.
   ☐ Evet (……..……..)
   ☐ Hayır
5. Kullanıcı bilgilerinin ihlali halinde personele uygulanacak yaptırımlar belirlenmiş midir? Cevabınız "*EVET*" ise bu yaptırımlar nelerdir?
   ☐ Evet (……..……..)
   ☐ Hayır
6. Kullanıcılara ait hangi bilgilerin toplanacağına nasıl karar verilmektedir?
   (……...…)
7. Kullanıcılara ait kayıtların hangi gerekçe ile paylaşımına izin verilmektedir? (*Birden fazla seçeneği işaretleyebilirsiniz*)
   ☐ Yasal çerçevede savcılık tarafından istenmesi durumunda
   ☐ Bilgi Edinme Hakkı Kanunu çerçevesinde
   ☐ İstatistiksel 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 bilgileri hangi sebeple olursa olsun verilmez.
8. Yedinci soru kapsamında kullanıcılara ait kayıtların paylaşılması durumunda ilgili kullanıcıya bilgi veriliyor mu?
   ☐ Evet ☐ Hayır

9. Kişisel bilgilerin amaç dışı kullanımı, korunması ve izinsiz olarak paylaşımına ilişkin kullanıcıya yazılı taahhütte bulunulmakta mıdır? ☐ Evet ☐ Hayır

10. Personel kayıtları içeren belgeler gizlilik seviyesine göre sınıflandırılıyor mu? ☐ Evet ☐ Hayır ☐ Kısmen

11. Kullanıcı kayıtları içeren belgeler hangi ortamda saklanıyor? (Birden fazla seçeneği işaretleyebilirsiniz)
    ☐ Şifreli/korumalı dolaplarda
    ☐ Şifresiz/korumasız klasör ya da dolaplarda
    ☐ Merkezi olarak bilgi merkezi içinde bulunan sunucu bilgisayarda
    ☐ Merkezi olarak BİDB.lığı içinde bulunan sunucu bilgisayarda
    ☐ Diğer (…….……)

12. Aşağıda tanımlanan amaçları bilgi hizmetlerinin sunulmasıyla ilişkili olarak <u>öncelik sırasına göre</u> "1" (en öncelikli) ile "4" arasında sıralayınız.
    ☐ Bilgi erişiminin sağlanması ve araştırmacının en kısa sürede bilgi ile buluşturulması
    ☐ Düşünce özgürlüğü çerçevesinde sınırsız bilgi hizmeti sunulması
    ☐ Bilgi varlıklarının gizliliği, bütünlüğü ve kullanılabilirliğinin teknik olanaklarla sağlanması
    ☐ Bilgi varlıklarının ihlallere karşı etik ve hukuksal koşullar çerçevesinde korunması

13. Aşağıdaki seçeneklerden hangilerinin kullanıcı ile ilişkilendirilmesi halinde "hassas" ya da "kişisel veri" kapsamında korunması gerektiğini düşünüyorsunuz? (*Birden fazla seçeneği işaretleyebilirsiniz*)
    ☐ Kullanıcının araştırma konusu
    ☐ Kullanıcının danışma hizmetleri kapsamında edindiği bilgiler
    ☐ Ödünç alınan yayınların listesi
    ☐ Web sayfasına yapılan ziyaretlere ilişkin kayıtlar (Zaman bilgileri, IP adresi, görüntülenen sayfalar, tarama amacıyla kullanılan kelimeler vb.)
    ☐ Kullanıcının bilgi merkezi kaynaklarına ve veri tabanlarına bağlandığı IP adresi
    ☐ Kullanıcının kimlik bilgileri (Ad-Soyad, TC kimlik numarası vd.)
    ☐ Kullanıcının iletişim bilgileri (adres, telefon, e-posta adresi vd.)
    ☐ Hiçbiri

14. Kullanıcı kayıtlarının ne kadar süre ile saklanacağı yazılı olarak belirlenmiş midir? Cevabınız "*EVET*" ise bu süre nedir? ☐ Evet (……..……) ☐ Hayır

15. Danışma hizmetleri kapsamında yapılan araştırma konusu ve notları hizmet sunulan kişi ile ilişkilendirilerek kayıt altına alınıyor mu? ☐ Evet ☐ Hayır

16. Kullanıcı bilgilerinin kaydedildiği bilgisayarların ya da sabit disklerinin kullanım ömrü dolması halinde hangi işlem yapılmaktadır?
    ☐ BİDB'lığı tarafından değişimi yapılmaktadır
    ☐ Yeni bilgisayarların kurulumu yapılarak eskileri çöpe atılmaktadır
    ☐ Eski sabit diskler özel imha işlemine tabi tutulmaktadır.
    ☐ Bilgi sahibi değilim.
    ☐ Diğer (…….)

17. Kullanıcılarının kullanmış olduğu bilgisayarlarda kullanım kayıtları düzenli olarak temizleniyor mu? ☐ Evet ☐ Hayır ☐ Fikrim Yok

18. Kişisel verilerin korunmasına ilişkin olarak bilgilendirildiniz mi? Cevabınız "*EVET*" ise ne tür toplantılara katıldınız? Toplantılar hangi sıklıkta ve hangi birim tarafından yapılıyor?
    ☐ Evet (…….……..)
    ☐ Hayır

19. Kişisel verilerin korunmasına ilişkin birtakım teknik önlemlerin alınması konusunda sorumluluklarınız bulunuyor mu? Cevabınız "*EVET*" ise ne tür sorumluluklarınız bulunuyor?
    ☐ Evet (…….……..)
    ☐ Hayır
    ☐ Fikrim Yok

20. Kullanıcı bilgilerinin kaydedildiği bilgisayarların internet bağlantısı bulunuyor mu? ☐ Evet ☐ Hayır

21. Kişisel verilerin ihlal edilmesi durumunda aşağıdakilerden hangileri haberdar edilmektedir? (Birden fazla seçeneği işaretleyebilirsiniz)
    - ☐ Savcılık
    - ☐ Bilgi İşlem Daire Başkanlığı
    - ☐ Bağlı bulunulan idari amir
    - ☐ Kişisel verileri ihlal edilen kişi
    - ☐ Haber verilmeksizin en kısa sürede sistem yeniden aktif hale getirilir
    - ☐ Diğer (……..…….)

22. Kullanıcı bilgilerinin kaydedildiği bilgisayarlarda oturum açma işlemi nasıl uygulanmaktadır?
    - ☐ Her personel sadece kendi kullanıcı adı ile oturum açabilmektedir
    - ☐ Ortak kullanıcı hesabı ile oturum açılmaktadır
    - ☐ Ortak ya da kişiye özel kullanıcı adı ve şifresi ile oturum açılabilmektedir
    - ☐ Oturum açmak için kullanıcı adı ve parola ihtiyaç duyulmamaktadır

23. Kullanıcılara ait kişisel verilerin korunmasına ilişkin önlemleri öncelik sırasına göre "1" (en öncelikli) ile "4" arasında sıralayınız. Sorumluluğunuz olmadığını düşünüyorsanız ilgili seçeneği işaretleyiniz.
    - ☐ Hukuksal düzenlemeler kapsamında korunmalıdır
    - ☐ Teknik önlemler alınmalıdır
    - ☐ İdari önlemler alınmalıdır
    - ☐ Etik ilkeler çerçevesinde korunmalıdır
    - ☐ Kişisel verilerin korunması bilgi merkezinin sorumluluklarından biri değildir

Konuya ilişkin olarak ilâve etmek istediğiniz görüş ve öneriler

Katkılarınız için teşekkür ederiz.