1922
SCIENTIA POTESTAS EST

GEORGIAN TECHNICAL UNIVERSITY

SINCE 1922

PROCEEDINGS BOOK

Editors
Prof. Dr. Tamar Lominadze
Assoc. Prof. Dr. Manuchar Shishinashvili
Assoc. Prof. Dr. Giorgi Chubinidze



05-06 / OCTOBER / 2026
TBILISI, GEORGIA

ISBN: 979-8-89695-586-3

PROCEEDINGS BOOK

INTERNATIONAL CONFERENCE ON GLOBAL PRACTICE OF MULTIDICIPLINARY SCIENTIFIC STUDIES - III

October 05-06, 2026

Tbilisi, Georgia

Editors

Prof. Dr. Tamar Lominadze
Assoc. Prof. Dr. Manuchar Shishinashvili
Assoc. Prof. Dr. Giorgi Chubinidze

22.10.2026
by Liberty Academic Publishers, New York, USA
ALL RIGHTS RESERVED NO PART OF THIS BOOK MAY BE REPRODUCED IN ANY FORM, BY PHOTOCOPYING OR BY ANY ELECTRONIC OR MECHANICAL MEANS, INCLUDING INFORMATION STORAGE OR RETRIEVAL SYSTEMS, WITHOUT PERMISSION IN WRITING FROM BOTH THE COPYRIGHT OWNER AND THE PUBLISHER OF THIS BOOK.
© Liberty Academic Publishers 2026
The digital PDF version of this title is available Open Access and distributed under the terms of the Creative Commons Attribution-Non Commercial 4.0 license (http://creativecommons.org/licenses/by-nc/4.0/) which permits adaptation, alteration, reproduction and distribution for noncommercial use, without further permission provided the original work is attributed. The derivative works do not need to be licensed on the same terms.
adopted by Mariam Rasulan

ISBN: 979-8-89695-586-3

CONTENT

CONGRESS ID	1
SCIENTIFIC COMMITTEE	2
PHOTO GALLERY	3
PROGRAM	4
CONTENT	5

PROCEEDINGS BOOK

Robraw ANN *STANDARDIZED TESTING IN CAMBODIAN UPPER SECONDARY SCHOOLS: IMPLEMENTATION STATUS AND CHALLENGES IN KAMPONG CHHNANG PROVINCE*	1
Anana Majumdar *PERFORMING AUTHORITY: ELITE POWER, REPRESENTATION, AND EXCHANGE IN EARLY MODERN EUROPE*	2
Meryem TEMİZ *THE OTHERNESS OF THE MUSLIM TURKISH MINORITY IN WESTERN THRACE*	9
Yusuf Ersöz GÜRÇAY, Ayşegül ALAYBEYOĞLU *ENHANCING MARITIME TRAFFIC SURVEILLANCE VIA EXPLAINABLE MACHINE LEARNING: DYNAMIC AIS-BASED VESSEL VERIFICATION AND DECISION BOUNDARY ANALYSIS*	22
Ayşe ÇAY ATALAY, Mesud FAKİRULLAHOĞLU *KARBONUN HALK SAĞLIĞI VE ÖZNEL İYİ OLUŞ ÜZERİNDEKİ ETKİSİ*	31
Feyza GÜR, Osman Nuri ÖCALAN *COMPARATIVE EVALUATION OF THE EFFECTS OF CULTIVATION CONDITIONS ON STRAWBERRY STORAGE PERFORMANCE*	32
Maryam Halliru Idris, Aliyu Ibrahim Yaradua, Hadiza Kabir Matazu, Hafsat Nasir Nayaya *EFFECT OF ASPERGILLUS NIGER FERMENTATION ON ANTI-NUTRITIONAL FACTORS OF MILLET (PENNISETUM GLAUCUM) STALK*	34
Chokri BAYOUDH, Yassmine GHRAIRI, Afifa MAJDOUB, Taoufik BETTAIEB *EFFICACY OF ROSEMARY AND THYME ESSENTIAL OILS ON PEAR (Pyrus communis L.) EXPLANT EVOLUTION ON IN VITRO ESTABLISHMENT PHASE*	35
Ahmed Baki ŞAFAK, Dilan Şerife ŞİŞKİN *INFORMATION SECURITY IN UNIVERSITY LIBRARIES: AN EVALUATION WITHIN THE SCOPE OF LITERATURE STUDIES*	36

ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ: LİTERATÜR ÇALIŞMALARI KAPSAMINDA BİR DEĞERLENDİRME

INFORMATION SECURITY IN UNIVERSITY LIBRARIES: AN EVALUATION WITHIN THE SCOPE OF LITERATURE STUDIES

Ahmed Baki ŞAFAK [1]

[1] *Öğretim Görevlisi, Ankara Üniversitesi, Bala Meslek Yüksekokulu, Yönetim ve Organizasyon Bölümü, Ankara, Türkiye*

[1] *ORCID ID: https://orcid.org/0009-0004-9160-1094*

Dilan Şerife ŞİŞKİN [2]

[2] *Yüksek Lisans Mezunu, Hacettepe Üniversitesi, Edebiyat Fakültesi, Bilgi ve Belge Yönetimi, Ankara, Türkiye*

[2] *ORCID ID: https://orcid.org/0000-0003-2923-8859*

ÖZET

Son dönemlerde kişisel verilerin korunması ve bilgi güvenliği önemi artan konulardan biri haline gelmiştir. Üniversite kütüphaneleri, basılı ve elektronik bilgi kaynaklarının yanı sıra kullanıcı verileri, kurumsal kayıtlar, bilgi sistemleri ve teknolojik altyapı gibi korunması gereken çok sayıda bilgi varlığını bünyesinde barındırmaktadır. Üniversite kütüphanelerinde bilgi güvenliğinin sağlanması, belli bir vizyonu olan üniversite kütüphanelerinde kişisel verilerin işlenmesi, aktarılması ve transfer edilmesine yönelik koşulların belirlenmesi kurumda bilgi güvenliği kültürünün oluşturulmasına zemin hazırlayacaktır. Bu bilgiler ışığında, üniversite kütüphanelerinde bilgi güvenliğine ilişkin ulusal ve uluslararası literatür, alanda öne çıkan çalışma konuları ve kütüphane bilgi sistemlerinin güvenliğinin değerlendirilmesine yönelik geliştirilen bir model araştırma kapsamında değerlendirilecektir. Araştırmada betimleme yöntemi kullanılmış, veriler literatür taraması yoluyla elde edilmiştir. Bu kapsamda Taylor & Francis, Springer, ProQuest ve çeşitli uluslararası veri tabanları ile Türk Kütüphaneciliği, Bilgi Dünyası ve Bilgi Yönetimi dergileri taranmış; ayrıca Google Akademik üzerinden ilgili yayınlara erişilmiştir. İncelenen çalışmalar, üniversite kütüphanelerinde bilgi güvenliğinin; kullanıcı ve personel güvenliği, kişisel verilerin korunması, bilgi sistemleri ve koleksiyon güvenliği, fiziksel güvenlik, ağ ve yazılım güvenliği ile bilgi güvenliği farkındalığı gibi farklı başlıklar altında ele alındığını göstermektedir. Literatür çalışmalarından hareketle, araştırmada Ismail ve Zainab (2013) tarafından geliştirilen Kütüphane Bilgi Sistemleri Güvenlik Değerlendirme Modeli analiz edilmiştir. Modelde kütüphane bilgi sistemlerinde bilgi güvenliği, teknolojik ve organizasyonel önlemler temelinde ele alınmakta; teknolojik güvenlik, bilgi güvenliği politikası, prosedürler ve kontroller, yönetim araç ve yöntemleri ile farkındalık oluşturma olmak üzere beş aşamada değerlendirilmektedir. Araştırma sonucunda, üniversite kütüphanelerinde etkili bilgi güvenliğinin yalnızca teknolojik altyapının korunmasıyla sağlanamayacağı; bilgi güvenliği ve kişisel verilerin korunmasına yönelik politika, standart, prosedür, yönetim uygulamaları ve personel ve yönetici farkındalığının da sürecin temel unsurları olduğu görülmüştür. Ayrıca araştırmada, Türkiye'de bilgi ve belge yönetimi alanında üniversite kütüphanelerinde bilgi güvenliğini doğrudan ele alan çalışmaların sınırlı olduğu belirlenmiştir. Bu nedenle alana özgü bilgi güvenliği uygulamalarını, politikalarını ve farkındalık düzeylerini inceleyen çalışmaların artırılması önem taşımaktadır.

Anahtar sözcükler: Üniversite kütüphaneleri, bilgi güvenliği, kişisel verilerin korunması, bilgi sistemleri, bilgi güvenliği farkındalığı.

ABSTRACT

In recent years, the protection of personal data and information security have become increasingly important issues. University libraries contain a wide range of information assets that need to be protected, including printed and electronic information resources, user data, institutional records, information systems, and technological infrastructure. Ensuring information security in university libraries and establishing clear conditions for the processing, disclosure, and transfer of personal data in libraries with an institutional vision can contribute to the development of an information security culture within the institution. In light of these considerations, this study examines the national and international literature on information security in university libraries, prominent research topics in the field, and a model developed for evaluating the security of library information systems. The descriptive method was employed in the study, and the data were obtained through a literature review. Within this scope, Taylor & Francis, Springer, ProQuest, and various international databases were searched, together with the journals Türk Kütüphaneciliği, Bilgi Dünyası, and Bilgi Yönetimi. Relevant publications were also accessed through Google Scholar. The reviewed studies demonstrate that information security in university libraries has been addressed under various headings, including user and staff security, protection of personal data, information system and collection security, physical security, network and software security, and information security awareness. Based on the literature, the Library Information Systems Security Evaluation Model developed by Ismail and Zainab (2013) was analyzed in this study. The model approaches information security in library information systems on the basis of technological and organizational measures and evaluates it across five dimensions: technological security, information security policy, procedures and controls, management tools and methods, and awareness-raising activities.

The findings indicate that effective information security in university libraries cannot be achieved solely through the protection of technological infrastructure. Policies, standards, procedures, management practices, and the awareness of both staff and administrators regarding information security and personal data protection are also essential components of the process. The study further reveals that research directly addressing information security in university libraries within the field of information and records management in Türkiye remains limited. Therefore, increasing the number of studies examining field-specific information security practices, policies, and awareness levels is considered important for the further development of the literature.

Keywords: University libraries, information security, personal data protection, information systems, information security awareness.

1.Giriş

Bilginin elektronik ortamda üretilmesi aynı zamanda bilgi taşıyıcılarının da bu ortama uyumluluk sağlamasını gerektirmektedir. Bu durum ayrıca bilgi taşıyıcılarının fiziksel ortamın yanı sıra elektronik ortamda da kalıcılığının sağlanmasına yönelik çabaları beraberinde getirmiştir. Böylelikle kurumlar ihtiyaç duyulan bilgilere zamandan ve mekândan bağımsız olarak erişim olanağı sağlamanın yanı sıra bu bilgilerin kolay bir şekilde paylaşılmasına ve kopyalanmasına imkân tanımaktadır. Diğer taraftan bu avantajlara rağmen bu ortamın bilginin kötü niyetli kullanımına ya da güvenilirliğinin ve kalıcılığının sürdürülmesine yönelik bir takım tehdit ve saldırılara açık olduğunu söylemek mümkündür. Yeni teknolojilerin şekil verdiği günümüz dijital dönüşüm çağı, siber saldırılar, kişisel verilerin izinsiz kullanımını, bilişim suçları, veri ihlalleri ve siber zorbalık gibi birtakım bireysel ve toplumsal riskleri de beraberinde getirmektedir. Bu riskler, ekonomik kayıplara, hizmet sunumunda aksaklıklara ve kurum ve kuruluşlarda itibar kaybına neden olabilmektedir (Seferoğlu, Yıldız Durak, Karaoğlan Yılmaz ve Yılmaz, 2018, s.31). Bununla birlikte, bireyler sanal ortamda virüs, kimlik avı, oltalama, siber zorbalık gibi farklı saldırı türlerine maruz kalabilmekte, kullanıcı hesapları ya da kredi kartı bilgileri kötü niyetli kişilerin eline geçebilmektedir (Gültekin & Özel, 2023, s.312). Bu çerçevede bilginin, bilgi sistemlerinin ve depolandığı ortamın güvenliğinin sağlanması, tüm dünyada yaşamın bir parçası haline gelen internet kullanımının yaygınlaşması, siber suç oranlarındaki artış, iş dünyası ve kişisel bilgi gizliliğini tehdit eden bilgi teknolojilerine bağlı unsurların etkisinin artması, yasal sorumlulukların artması, tehditlerin

çoğalması ve daha karmaşık bir yapıya dönüşmesi nedeniyle zorunlu hale gelmiştir (Henkoğlu ve Yılmaz, 2013, s. 452). Bu sebeple, kurum ve kuruluşların sahip oldukları bilgilerin güvenliğine yönelik olarak geliştirilen standartlara ve yasal düzenlemelere uyum sağlamaları önemli görülmektedir.

Türkiye'de kamu kurum ve kuruluşları açısından bilgi güvenliğine yönelik atılan adımların en güzel örneklerinden biri kamuda dijital dönüşüm hedefiyle Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından atılmıştır. Hazırlanan projeler (açık veri, Kamunet vb.) ve rehberler (Bilgi ve İletişim Güvenliği) ile kamu kurum ve kuruluşlarında yüksek katma değerli, etkili ve verimli bir performans alt yazılımının oluşturulması hedeflenmektedir (Türkiye Cumhuriyeti Cumhurbaşkanlığı, Dijital Dönüşüm Ofisi, 2020). Bu durumun temel sebepleri arasında ise, kamu kurumlarındaki elektronik belge yönetim sistemlerinde karşılaşılan güvenlik sorunları, kişisel verilerin korunmasına yönelik sorunlar, arşivleme ve depolama sorunları örnek olarak gösterilebilmektedir. Bu bağlamda, kamu kurum ve kuruluşlarında bilgi güvenliğine yönelik çalışmaların yapılması kaçınılmaz bir hal almıştır. Konunun diğer bir boyutunu da, büyük veri, blok zincir, otonom, siber güvenlik, kuantum, nesnelerin interneti, açık devlet verisi, robotik vb. alanlar ile beraber gelen bilgisayar ve yapay zekâ sistemlerine dayanan dijital dönüşüm oluşturmaktadır. Kamu kurum ve kuruluşlarını etkileyen bu değişim ve dönüşüm ise, Türkiye'de son birkaç yılda bilimsel ve teknolojik gelişmeler ışığında bilgiye ve veriye dayalı erişim, gizlilik, bütünlük konusunda daha çok adım atılmasını sağlamıştır. Bunun en güzel örneklerini ise, Türkiye'nin küresel rekabet gücünü arttıracak ve kalkınmasına olanak sağlayacak "Milli Teknoloji Hamlesi" doğrultusunda hazırlanan politika ve uygulamalar, kalkınma planları, düzenlemeler, genelgeler, projeler ve açılan kurum ve kuruluşlarla beraber gelen (Kişisel Verilerin Korunması Kurumu, Dijital Dönüşüm Ofisi) yenilikçi yaklaşımlar oluşturmaktadır. Diğer taraftan, günümüzdeki tüm bu yeniliklerin yanında gelen belirsizlikler ve riskler de bulunmaktadır. Günümüz teknolojik gelişmelerinin sonucunda ortaya çıkan bilgi, belge artışıyla beraber bilginin üretilmesi ve bilgiye erişilmesi kolaylaşmış, ancak bu durum verilerin daha faydalı bilgiye dönüştürülmesi, sınıflanması, saklanması, güvenirliklerinin ve güvenliğinin sağlanması sürecinde güçlüklerin yaşanmasına neden olmuştur. Bu doğrultuda, Türkiye'nin ilerleme ve gelişme hedefleri gizlilik, veri ihlalleri, veri sızıntısı, kişisel verilerin ihlali konularında tedbirlerin ve önlemlerin alınmasını gerektirmiştir.

Uluslararası alanda kütüphanelerde güvenlik, bilgi güvenliği, gizlilik ve kişisel verilerin korunması, siber güvenlik ve kullanıcı gizliliği konusunda kütüphane derneklerinin rehber, ilkeler, kontrol listeleri vb. çalışmalarının fazla olduğu anlaşılmaktadır (American Library Association-ALA, 2021; Association of College and Research Libraries-ACRL 2026; International Federation of Library Associations and Institutions - IFLA). Örneğin, ALA'nın hazırlamış olduğu 'Gizlilik Rehberleri' (Privacy Field Guides), kütüphaneciler için daha güvenli ve emniyetli bir ortamın oluşturulması için yapılması gerekenleri içermektedir (ALA, n.d.). Kütüphanelerde bilgi güvenliğinin sağlanması, teknolojik önlemlerin yanı sıra kütüphane çalışanlarının bilgi güvenliği konusundaki farkındalıklarını da gerekli kılmaktadır. Uluslararası Kütüphane Dernekleri ve Kurumları Federasyonu (IFLA), 2026 yılında düzenlenen Dünya Kütüphane ve Bilgi Kongresi kapsamında yayımladığı "Kütüphanelerde Siber Güvenlik" başlıklı oturum çağrısında, kütüphanelerde siber güvenlik uygulamalarının önemine dikkat çekmiştir. Söz konusu çağrıda, kütüphane çalışanlarına ve kullanıcılarına yönelik siber güvenlik eğitimleri, mevcut ve yeni ortaya çıkan tehditler, güvenlik uygulamaları ve yapay zekânın siber güvenliğe etkileri ele alınması önerilen konular arasında sıralanmıştır (IFLA, 2026).

Türkiye'de faaliyet gösteren kütüphanecilik derneklerinin çalışmalarını incelediğimizde ise, daha az sayıda olduğu ortaya çıkmaktadır (Şişkin ve Çakmak, 2020, s.476). Kamu kurumlarından birisi olan üniversite kütüphanelerinin de üniversitenin itibarını arttırmak, sahip olduğu bilgi varlıklarını koruyarak bilgi ekonomisine katkı sağlaması gerekmektedir. Dijital rekabet ortamının yaşandığı günümüzde üniversite kütüphanelerinin güvenli, güvenilir teknolojik alt yapılarını oluşturmaları, politika ve stratejilerini hazırlamaları gerekmektedir. Çünkü, belli bir vizyonu ve misyonu olan üniversite kütüphanelerinde kişisel verilerin işlenmesi, aktarılması ve transfer edilmesine yönelik koşulların belirlenmesi kurumda bilgi güvenliği ve bilgi güvenliği kültürünün oluşturulmasına zemin hazırlayacaktır.

2. Çalışmanın Amacı, Kapsamı ve Yöntemi

Bu araştırmada, Türkiye'deki üniversite kütüphanelerinde kişisel verilerin korunması ve bilgi güvenliği yaklaşımını değerlendirmek amaçlanmaktadır. Nitel araştırma türlerinden olan betimleme yöntemi kapsamında, 2013-2026 yılları arasında yayınlanan bilimsel araştırma, araştırma makalesi, yüksek lisans doktora tezleri ulusal ve uluslararası alanda indexslenen dergiler incelenmiştir. Araştırma kapsamında incelenen veritabanları ise şu şekildedir:

Türkiye'de bilgi güvenliği ve kişisel verilerin korunması yönündeki atılımlar, kişisel verilerin korunması yönündeki yeni sayılabilecek nitelikteki girişimler (6698 Sayılı Kişisel Verilerin Korunması Kanunu, Kişisel Verileri Koruma Kurumunun ortaya çıkışı) Türkiye'deki üniversite kütüphanelerinin konuyu daha ayrıntılı boyutlarda ele alınmasını zorunlu kılmıştır. Bu doğrultuda, araştırma soruları şu şekilde belirlenmiştir:

S1. Türkiye'de üniversite kütüphanelerinde bilgi güvenliği uygulamalarına yönelik eğilim nasıldır?

S2. Türkiye'de üniversite kütüphanelerinde kişisel verilerin korunmasına yönelik eğilim nasıldır?

Araştırmada elde edilen bilimsel makaleler içerik analiz yöntemi ile analiz edilmiştir. İçerik analizi, *"yazılı metinden hareketle yazılı olmayan mesajlara ve anlamlara ulaşabilmeyi mümkün kılan bir teknik"* şeklinde tanımlanmaktadır (Alanka, 2024, s. 72). Bu çerçevede araştırmada üniversite kütüphanelerinde bilgi güvenliğine yönelik araştırma makaleleri içerikleri açısından değerlendirilmiştir. Söz konusu değerlendirme sürecinde, 'kişisel veri', 'kişisel verilerin korunması', 'mahremiyet' ve 'bilgi güvenliği', 'üniversite kütüphaneleri' gibi anahtar kavramlardan bilimsel makaleler taranarak analiz edilmiştir.

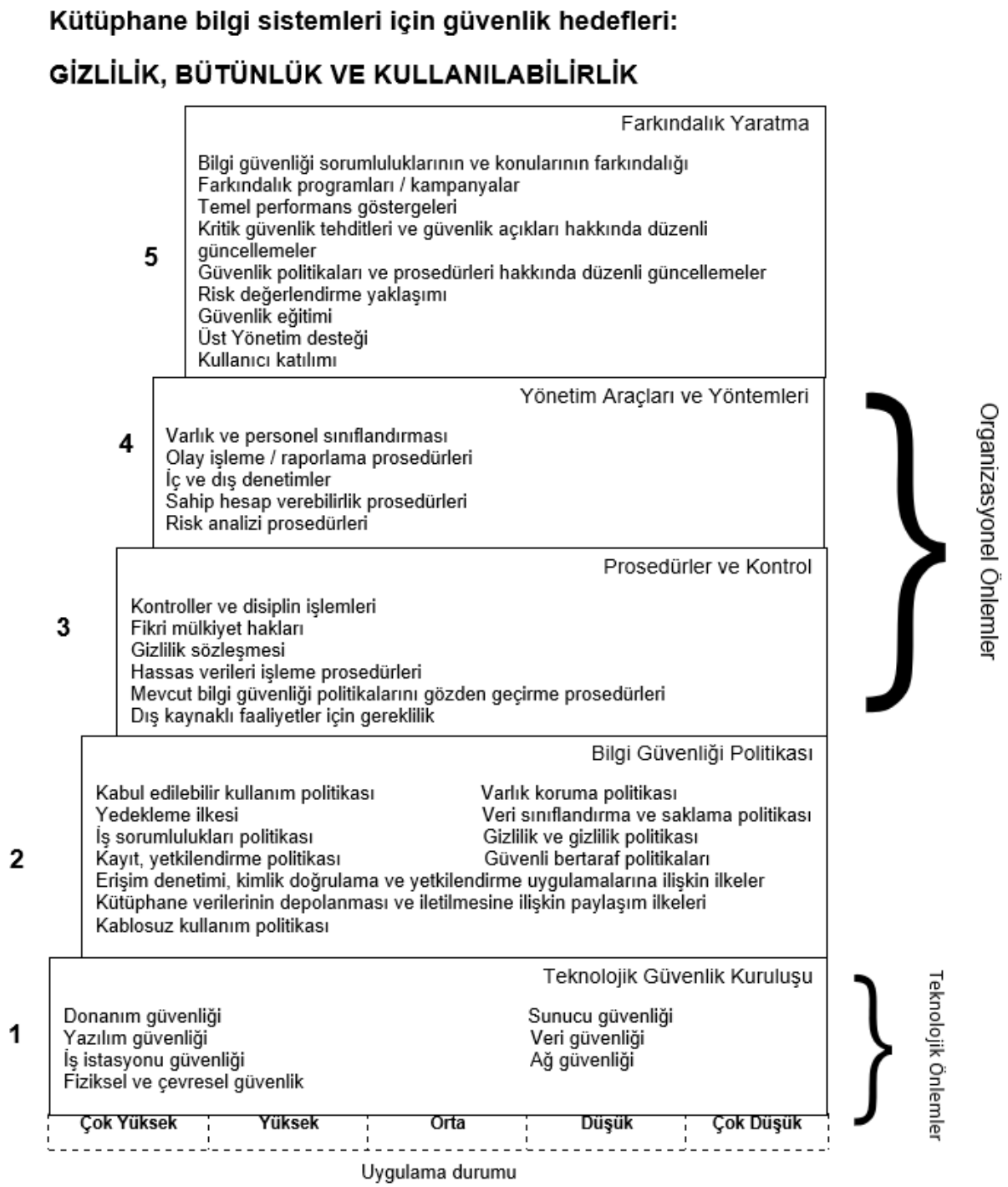
4. Bilgi güvenliği kavramı

Literatür çalışmalarında bilgi güvenliği kavramı hakkında pek çok tanım bulunmaktadır (Şafak, 2025, s.22). Bilgi güvenliği güvenli bir bilgi sisteminin oluşturulması ve bilginin istenmeyen kişi ya da kişiler tarafından elde edilmesini önleme girişimleri ve çabalarını ifade etmektedir (Seferoğlu, Durak ve diğerleri, 2018, s.31). Bilgi güvenliği, bilginin kullanım hakkına sahip kişi veya kurum haricinde başka herhangi bir kişi ya da kurum tarafından erişilememesi, kullanılamaması, değiştirilmemesi, gizliliğinin ve bütünlüğünün bozulmaması olarak tanımlanmaktadır. Bilgi güvenliği, bilginin hata, ifşa ve manipülasyona karşı korunması olarak da nitelendirilmektedir. Oldukça kapsamlı ve farklı boyutları ile değerlendirilmesi gereken bilgi güvenliğinin, bilginin korunacak nitelikleri (gizliliği, bütünlülüğü, kullanılabilirliği), bilginin durumu (transferi, depolanması, işlenmesi), güvenlik önlemleri (teknoloji, politikalar, farkındalık) ve risk yönetimi etkenlerinin de göz önünde bulundurulması gerekmektedir (Henkoğlu ve Külcü, 2013, s.70). Kurum bilgilerinin tehlikeye atılması, kurum bilgilerinin temel üç özelliğinin başarısızlığına bağlı olarak kendini gösterebilmektedir. Bu üç özellik, gizlilik, bütünlük ve kullanılabilirlik olarak tanımlanabilmektedir. Genellikle, "CIA (Confidentiality – Integrity - Availability) üçlüsü" olarak nitelendirilen her özellik önemli bir değer taşımaktadır ve her türlü tehdide karşı korunmalıdır (Waddell, 2013, s.21). Bir bilgiye erişmesi uygun görülen kişiler tarafından erişimin sağlanabilmesi gizlilik, bilgi merkezlerinde ya da herhangi bir elektronik ortamda yer alan bilgi kaynaklarının yayıncı tarafından ulaştırılan orijinal halinin, yetkisiz kişiler tarafından değiştirilmemiş olması bütünlük, kullanıcının ihtiyacı olan bilgiye yetki alanı sınırları içinde ve istediği anda ulaşabilmesi ise erişilebilirlik olarak tanımlanmaktadır (Henkoğlu ve Yılmaz, 2013, s. 455; Baykara, Daş ve Karadoğan, 2013, s. 238). Bu üç temel bileşene alt bileşenler olarak kayıt tutma, kimlik tespiti, güvenilirlik ve inkâr edememe bileşenleri de eklenebilmektedir (Tekerek, 2008, s.133). Bunlar arasında, bilgiye, sisteme veya ağa erişmek isteyen kişinin gerçekten iddia ettiği kişi olduğundan emin olması kimlik denetimi, veri iletişiminde mesajı gönderenin veya mesajı alanın, gönderdiği veya aldığı mesajı yadsımaması inkâr edememe, ağ üzerinde veya herhangi bir sistem üzerinde gerçekleşen her türlü olayın, sonrasında incelenmek üzere kayıt altına alınması izlenebilirlik olarak tanımlanmaktadır (Can ve Akbaş, 2014, s. 18). Verilen tanımlardan hareketle bu çalışma kapsamında Türkiye'de üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin korunması yönünde güncel durumun ele alındığı bu çalışma kütüphane özelinde bilgi güvenliği bağlamında gerçekleştirilecek yeniliklere ışık tutacağı değerlendirilmektedir.

5.Üniversite kütüphanelerinde bilgi güvenliği

Dünyada yapay zekâ, blokchan teknolojisi, metaverse, vb. gelişmelerle dijital dönüşümün ve değişimin giderek artması, siber suç oranlarındaki artış, yasal sorumlulukların artması, iş dünyası ve kişisel veri gizliliğini tehdit eden bilgi teknolojilerine bağlı unsurların etkisinin artması, tehditlerin çoğalması ve daha komplike bir yapıya dönüşmesi nedeniyle bilgi güvenliğinin sağlanması zorunlu hale gelmiştir (Henkoğlu ve Yılmaz, 2013, s.452). Yükseköğretim kurumlarında (YÖK) bilgi güvenliği uygulamalarına ilişkin araştırmalar, bireysel sorumluluğun giderek artması ve bunun sonucunda karmaşık siber saldırılara maruz kalınması nedeniyle kritik bir araştırma alanı olarak ortaya çıkmıştır (Bwino ve diğerleri, 2026, s.1). Kütüphanelerde bilgi güvenliği, değişen teknoloji ortamına, dijital kaynaklara artan bağımlılığa ve hassas bilgilere yönelik artan tehditlere yanıt olarak yıllar içinde gelişmiştir. Dijital dönüşüm çağı başlamadan önce kütüphanelerde bilgi güvenliği öncelikle fiziksel güvenlik ile ilgili olmaktadır (Igbinovia ve Oladokun, 2024, s.4). Kütüphane bağlamında bilgi güvenliği tehditleri, bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak için bu varlıkların tehditlerden korunması gerekliliğini ifade etmektedir. Kütüphane Bilgi Sistemi, kütüphane web sitesi üzerinden uzaktan erişilebilen kütüphane bilgileri için çok sayıda kaynak, hizmet ve kullanıcı kaydı içermektedir (Yusuf, Yusuf ve Zaynana, 2021, s. 39). Üniversite kütüphaneleri de yükseköğretimin entelektüel mimarisinde temel bir konuma sahiptir. Birikmiş bir bilginin koruyucusu, birincil araştırma çıktılarının depoları, küresel bilgi ağlarına açılan ağ geçitleri ve öğretim üyeleri, öğrenciler ve araştırmacılar için hizmet platformları olarak hizmet etmektedirler (Edet ve Emmenuel, s.2026, s.102). Kurumların nitelikli faaliyetler göstermesi, kurumsal belleğini etkin ve verimli bir biçimde kullanabilmesi ve geleceğe yönelik planlar yapabilmesi için bilgi güvenliği önem arz etmektedir. Bünyesinde bilgi merkezlerini barındırması sebebi ile üniversitelerde de bilgi güvenliği son derece önem taşımaktadır. Üniversite kurumları bilginin üretiminde, korunmasında, sunumunda ve dağıtımında sorumluluk taşıyan ve bu konuda görevleri olan kurumlardandır (Şafak ve Alaca, 2024, s.182).” Günümüzde İnternet kullanımının artmasıyla kötücül yazılım, oltalama, siber saldırı, fidye yazılım ve sosyal mühendislik, siber zorbalık gibi sanal tehditler ortaya çıkmıştır. Sanal ortamı tehdit eden bu güvenlik sorunları ise, kişisel ve hassas verilerin kötü niyetli kişiler tarafından ele geçirilmesi kişiselre veya kurumlara ciddi hasarlar/zararlar verebilmektedir. Bilgi İletişim ve Teknolojilerinin gelişmesi ve özellikle son yıllarda mobil telefon, bilgisayar ve akıllı saat gibi dijital cihazların hayatımızın bir parçası haline gelmesi, dijiral ortamlarda birtakım tehlikelerin ve ihlallerin oetaya çıkması bilgi güvenliği konusunu ön plana çıkarmıştır (Gültekin & Özel, 2023, s.21). Gültekin ve Özel’e göre (2023, s.314), “bireyler sanal ortamda virüs, kimlik avı, oltalama, siber zorbalık gibi farklı saldırı türlerine maruz kalabilmekte, kullanıcı hesapları ya da kredi kartı bilgileri kötü niyetli kişilerin eline” geçebilmektedir.

Kavak’a göre (2023, s.160) bilgi güvenliği, “kütüphane bilgi sistemlerinde işlenen ve depolanan kurumsal ve kişisel bilgilerin korunması ve veri bütünlüğü sağlamayı amaçlayan bir disiplindir. Üniversite kütüphanelerinde iyi bir bilgi güvenliği yönetim anlayışı, akademik araştırmaların doğruluğunu ve güvenilirliğini sağlamak için kritik bir faktördür.” Bu bağlamda karşımıza dijital veri güvenliği çıkmaktadır. Dijital veri güvenliği, kütüphane sistemlerinde depolanan kişisel ve hassas verilerin artan miktarından dolayı kütüphaler için kritik bir öenem sahiptir. Kişisel ve hassas veriler kapsamına ise, kullanıcı ödünç alma kayıtları, kişisel olarak tanımlanabilir bilgiler ve erişim geçmişleri dâhildir. Söz konusu verilerin tehlikeye atılırsa, gizlilik ihlallerine ve kütüphaneler için misyon ve vizyon kaybına yol açabilir (Mater, 2026, s.21). Kişisel veriler genel olarak “kişinin kontrolü ve hatta bilgisi dışında toplanmaktadır. Bireyleirn arama geçmişleri, konum verileri, gezinme alışkanlıkları, alışveriş tercihleri, okuma davranışları gibi pek çok veri hayal bile edilecemeyek amaç ve şekillerde kullanılabilmektedir. Hatta, insanların kişisel bilgilerinden yola çıkılarak birçok pazarlama stratejisi bile geliştirilmektedir (Şeşen & Şeşen, 2025, s. 262). Bilgi Dünyası dergisinde yayınlanan bir makalede, “üniversite kütüphanelerinde bilgi güvenliği kavramı daha çok bilgisayar ve iletişim teknolojilerine dayalı uygulamaların ortaya çıkardığı tehditlere karşı alınan önlemleri ifade etmektedir. Yetkisiz erişim girişimleri, kullanıcıların yasal olmayan ya da sahte içerikli web sitelerini ziyaret etmeleri ve bunun sonucunda maruz kalınan virüs saldırıları kütüphanelerde bilgi güvenliğini tehdit eden başlıca unsurlar arasındadır (Öztemiz ve Yılmaz, 2013, s.94).



Görsel 1. Kütüphane bilgi sistemleri değerlendirme modeli

Ismail ve Zainab tarafından 2013 yılında hazırlanan kütüphane bilgi sistemleri için güvenlik değerlendirmesi modeli[2] incelendiğinde, kütüphanelerde bilgi güvenliği organizasyonel ve teknolojik olmak üzere iki bağlamda ele alınmıştır. Kurum ve kuruluşlar için organizasyonel önlemler, farkındalık yaratma, yönetim araçları ve yöntemleri, prosedürler ve kontrol ve bilgi güvenliği olmak üzere dört süreçte ele alınmaktadır. Kurumlar için teknolojik önlemler ise, bilgi ve iletişim teknolojileri bağlamında ele alınmaktadır.

[2] Kütüphane Bilgi Güvenliği Sistemi Modeli, Hagen ve dig. (2008, s.391) hazırlamış olduğu modelden uyarlanarak hazırlanmıştır.

Modele bakıldığında, etkili bir Bilgi Güvenliği Sistemi'nin birbirine bağlı iki temel bileşenden oluşan bir merdiven yapısından inşa edilmesi gerektiğini göstermektedir. İki temel bileşen ise, teknolojik ve organizasyonel ölçümlerdir. Teknolojik önlemler, (1. Aşama), herşeyden önce mevcut olması gereken kritik ve temel aşamayı oluşturmaktadır. Modelde yer alan teknolojik güvenlik önlemleri, kütüphanelerdeki donanım güvenliği, yazılım güvenliği, iş istasyonu güvenliği, sunucuları, donanımı, yazılımı, verileri, ağı ve ağın fiziksel tesislerini ve ortamını ifade etmektedir (Ismail & Zainab, 2013, s.233).

Organizasyonel bileşenler dört aşamadan oluşmaktadır. Bilgi güvenliği politikasının varlığı (aşama 2), prosedür ve kontrollerin oluşturulması (aşama 3), yeterli yönetim araçları ve yöntemlerin formüle edilmesi (aşama 4) ve farkındalık yaratılması (aşama 5) aşamalarını kapsamaktadır. Bilgi güvenliği politikası, kütüphanenin genel güvenlik stratejisini açıklayan ve bilgi sistemlerine veya bilgi sistemi tarafından desteklenen ürün ve hizmetlerine erişim ve kullanım için kurallar ve yönergeler içeren yazılı bir belgeyi ifade etmektedir (Ismail & Zainab, 2013, s.234).

5. Literatür Çalışmalarında Bilgi Güvenliği

Türkiye'de üniversite kütüphanelerinde bilgi güvenliği alanında yapılan çalışmaların sayısı oldukça sınırlıdır. Literatür çalışmalarında da çalışmaların kütüphane ve kütüphaneci boyutuyla ele alan çalışmaların sınırlı oluşuna vurgu yapılmaktadır (Şafak ve Alaca, 2024, s. 181). Akdoğan'da (2022, s.13-41) çalışmasında Türkiye'de bilgi ve belge yönetimi alanında bilgi güvenliğinin durumunun henüz gelişme aşamasında olduğunu belirtmiştir. Söz konusu çalışmalara yönelik ilk adımın ise, 2013 yılında atıldığı literatür çalışmalarından anlaşılmaktadır (Öztemiz ve Yılmaz, 2013). İlerleyen yıllarda, teknolojik gelişmelere dayalı olarak devlet ve özel üniversite kütüphaneleri ekseninde kullanıcı, personel ve yönetici üçgeni çerçevesinde bilgi güvenliği konusunun araştırma alanı genişleyerek kişisel verilerin korunması, bilgi güvenliği politikası, üniversite kütüphanelerinde bilgi güvenliği ve hassas veri, hassas verilerin korunması, kişisel verilerin korunması, teknolojik ve kurumsal bilgi güvenliği dijital veri güvenliği, bilgi sistemlerinin güvenliği, fiziksel güvenlik konuları bağlamında ele alındığı saptanmıştır. Bu bölümde, bilgi güvenliği konusunu ele alan ulusal ve uluslararası çalışmalara ilişkin kısa değerlendirmeler yapılmakta, kütüphaneler ve kütüphaneciler kapsamında ele alınan çalışmalara değinilmektedir.

Bilgi güvenliği araştırmalarına temel oluşturan bir araştırmada, Ankara'da bulunan 14 üniversite kütüphanesinin bilgi güvenliği uygulamaları ve yöneticilerin bilgi güvenliği farkındalıkları ele alınmıştır. Araştırma sonuçlarına göre, kütüphanelerde bilgi güvenliğini sağlamaya yönelik uygulamaların Bilgi İşlem Daire Başkanları tarafından yapıldığı, kütüphanelerin çoğunda bilgi güvenliğini sağlamaya yönelik politikaların bulunmadığı, küyüphane personellerinin bilgi güvenliği farkındalığının düşük düzeyde olduğu tespit edilmiştir (Öztemiz ve Yılmaz, 2013, s.97). Henkoğlu tarafından ele alınan ele alınan başka bir çalışmada ise, (2015, s.162-166), Ankara'da yer alan 15 üniversitenin BİDB, PDB ve bilgi merkezlerinin bilgi güvenliği önlemleri mevcut hukuksal düzenlemeler çerçevesinde değerlendirilmiştir. Araştırma sonuçlarına göre "üniversitelerde hukuksal düzenlemelerle uyumlu ve standartlaşmış bilgi güvenliği politikalarının bulunmadığı ve üniversitelerde kişisel verilerin korunmasına ilişkin kapsamlı bilgi güvenliği politikasının bulunmadığı saptanmıştır. Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi'nde yayınlanan bir araştırmada ise, Bilgi ve Belge Yönetimi Bölümü öğrencilerinin kişisel veri algıları analiz edilmiştir. Eroğlu'nun 2018 (s.150), yılında gerçekleştirmiş olduğu çalışma sonucuna göre ise, öğrencilerin kişisel veri algılarının yetersiz seviyede olduğu tespit edilmiştir.

Türkiye'de üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin korunması konusunda ilginin ve önemin artması sebebiyle, literaüt çalışmalarının 2020 yılı ve sonrasında artış gösterdiği dikkatleri çekmektedir. Literatür çalışmalarında dikkatleri çeken bir nokta ise, araştırmaların çoğunluğunun Ankara kapsamında olmasıdır. Üniversite kütüphanelerinin bilgi güvenliği uygulamalarına ve kişisel verilerin korunmasına ilişkin mevcut durumu tespit etmeye çalışan bir araştırmada da, Ankara'da bulunan üniversite kütüphaneleri yöneticilerinin ve kütüphanecilerinin bilgi güvenliğive kişisel verilerin yönetimi konusunda bilgi ve farkındaıkları incelenmiştir. Araştırma bulgularına göre, kişisel verilerin yönetimine yönelik politika eksikliği, yönetici ve kütüphanecilerde farkındalık eksikliği belirlenmiştir. Bununla beraber, üniversite kütüphanelerinde bina, koleksiyon, yazılım ve donanım olmak üzere bilgi

güvenliği uygulamalarına yönelik yetersizlikler olduğu tespit edilmiştir (Şişkin, 2020, s.115-122;). Kamu kurumlarında BGYS'ler için politika metodolojisi geliştirmeyi amaçlayan bir araştırmada (Akdoğan, 2022, s.15), bilgi ve belge yöneticilerinin bilgi güvenliği alanındaki rolleri tanımlanmıştır.

"Üniversite kütüphanelerinde bilgi güvenliği yönetimi ve bir rehber önerisi" başlıklı doktora tezinde (Kavak, 2023, s.9), "Türkiye'de üniversite kütüphanelerinin mevcut bilgi güvenliği tehditlerini belirlemek ve bilgi güvenliği yönetimi ile ilgili uygulanan teknolojik ve kurumsal uygulamaların düzeyini tespit etmek amaçlanmıştır. Araştırma sonucunda, *"üniversite kütüphanelerinde en yaygın bilgi güvenliği tehditlerinin insan / personel ile ilgili tehditler kategorisinde gerçekleştiği ve bu tehdit kategorisini sırasıyla ağ, yazılım, fiziksel ve çevresel, veri ve donanım tehditi kategorilerinin izlediği"* saptanmıştır. Bununla beraber, *"Türkiye'deki üniversite kütüphanelerinde teknolojik ve kurumsal bilgi güvenliği önlemlerinin genel olarak ortadüzeyin üzerinde uygulandığı, ancak bilgi güvenliği yönetimi açısından yeterli düzeylerde olmadığı"* tespit edilmiştir. Bununla beraber araştırma sonucunda, *"Türkiye'de üniversite kütüphanelerinde iyi bir bilgi güvenliği yönetim sisteminin gelişmediği"* belirlenmiştir (Kavak ve Odabaş, 2023, s.293-323).

Şafak'ın 2025 (s.7), yılında gerçekleştirmiş olduğu araştırmada ise, Ankara'da üniversite kütüphanelerinini, kütüphanecilerinin bilgi güvenliği farkındalık düzeyleri orta seviyede bulunmuş ve bilgi güvenliği uygulamalarında eksiklikler bulunmaktadır. Türkiye'deki devlet ve vakıf üniversitelerinde kütüphanecilerin dijital veri güvenliği farkındalığını saptayan bir araştırmada (Mater, 2026, s. 23) ise, üniversite kütüphanecilerinin temel parola güveliği konularında farkındalıklarının yüksek olduğu belirlenirken, çevrim içi ortamlarda güvenliği doğrudan etkileyen bazı unsurlara ilişkin bilgi düzeylerinin düşük olduğu tespit edilmiştir. İbekçi'nin 2025 (s.92) yılında gerçekleştirmiş olduğu bir araştırmada ise, Bilgi ve Belge Yönetimi Bölümü lisans öğrencilerinin dijital okuryazarlık düzeylerinin orta seviyede olduğu, dijital veri güvenliği farkındalık düzeylerinin ise iyi düzeyde olduğu saptanmıştır. Bilgi profesyonelleri için dijital koruma stratejilerini ele alan başka bir araştırmada ise, son yıllarda Türkiye'de ulusal mevzuat ve kurumsal dijital dönüşüm politikaları bağlamında dijital koruma çalışmalarının gün geçtikçe arttığına değinilmiştir. Ayrıca çalışmada özellikle Türkiye'de 6698 sayılı Kişisel Verilerin Korunması Kanunu'na bağlı olarak (KVKK) kamu kurumlarında dijital bilgi varlıklarının güvenli bir biçimde yönetilmesine yönelik çalışmaların artması, ve buna bağlı olarak *"Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlanan politika belgeleri, kamu kurumlarında dijital arşivleme, veri yönetimi ve bilgi güvenliği uygulamalarını bütüncül bir çerçevede"* ele alındığından mevzu bahis olunmuştur. Söz konusu gelişmelerin ise, "kütüphaneler ve bilgi merkezlerinde dijital koruma faaliyetlerinin yalnızca teknik değil, aynı zamanda yönetsel ve hukuki bir sorumluluk alanı olarak ele alınmasını gerekli kıldığına" urgu yapılmıştır (Yener Sarıçoban ve Şahin, 2026, s. 28).

The Journal of Academic Librarianship'nde (Akademik Kütüphanecilik Dergisi) yayınlanan bir makalede (Eroğlu, 2026, s.y), Türkiye'deki üniversite kütüphanelerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu'na (KVKK) ve kurumsal web sitelerinde kişisel verilerin korunması kriterlerine ne ölçüde uyduklarını incelenmiştir. Araştırma bulgularına göre, uyumluluğun genel olarak düşük seviyede olduğu tespit edilmiştir. Bununla birlikte, üniversite kütüphanelerinde web sitelerinin gizlilik bildirimleri, erişilebilirlik bilgileri ve erişilebilir formatlar nispeten sık görünürken, güncelleme tarihleri, açık rıza beyanları ve formlardaki veri koruma uyarıları gibi unsurlar büyük ölçüde eksip olarak saptanmıştır.

Türkiye'de 6. düzenlenen Elektronik Belge Yönetim ve Arşiv Sistemi sepmozyumu "Elektronik Belgelerin Geleceği ve Geleceğin Belgeleri" başlıklı sempozyumda bilgi ve belge yönetimi alanında kişisel verilerin korunması ve mahremiyet konularına da yer verilmiştir (e-BEYAS, 2026). Kişisel verilerin korunması ve dijital mahremiyet alanında yapılan çalışmaların e-BEYAS'a yansıması ve çalışmaların arttırılması ise oldukça dikkat çekici olmuştur.

Allameh Tabatabai Üniversitesi kütüphanesinin Bilgi Güvenliği Yönetimi'nin durumunu değerlendirmeyi ISO/IEC 27002 standarlarına göre değerlendirmeyi amaçlayan bir araştırmada, kütüphanein bilgi güvenliği yönetim performansı istenilen düzeyde belirlenmiştir (Malekolkalami, vd., 2024, s. 579). Kanyika ve diğerleri (2025), akademik kütüphanelerde blok zincir uygulamaları konulu çalışmalarında blok zinciri teknolojisinin kendine özgü olanakları sebebiyle akademik kütüphanelerde

oldukça ilgi gördüğünü belirtmekteler. Blok zincir teknolojilerinin veri güvenliğini artırma, şeffaflığı yükseltme, kütüphaneler içinde ve arasında iş birliğini teşvik gibi faydaları vurgulanmaktadır. Çalışma, verimlilik ve etkinliği artırmak için akademik kütüphanelerde blok zincir teknolojilerinin benimsenmesini tavsiye etmektedir. Başarılı bir uygulama için, özellikle kütüphaneler için eğitim sektöründe nispeten yeni bir kavram olan Blok zincir teknolojilerinin kütüphane bağlamında nasıl uygulanacağına dair kütüphane personeline kapsamlı eğitim verilmesi gerektiği önerilmektedir.

Oduluru (2025), kütüphanelerde bilgi teknolojileri konulu çalışmasında sistematik literatür taraması yöntemiyle 81 akademik yayını incelemiştir. Çalışmada, kütüphanelerin geleneksel bilgi hizmetlerinin ötesine geçerek kullanıcıların dijital ihtiyaçlarını karşılayan teknoloji merkezlerine dönüştüğü belirtilmektedir. Bu bağlamda yapay zekâ, bulut bilişim ve makine öğrenimi gibi teknolojilerin kütüphane hizmetlerine katkıları vurgulanmaktadır. Çalışmada, bilgi teknolojileri hizmetlerinin sürdürülebilirliği için teknolojik altyapının geliştirilmesi, personelin eğitilmesi ve bu eğitimlerin sürekli hale gelmesi gerektiği öneriler arasındadır.

Kütüphane çalışanları arasında kişisel veri gizliliği okuryazarlığı, kişisel veri farkındalığı ve kütüphane gizliliği farkındalığı arasındaki ilişkiyi inceleyen bir araştırmada, söz konusu kavramların ampirik olarak olarak ilişkili ancak kavramsal olarak farklı yapılar olduğunu belirtmiştir. Araştırma bulgularına bakıldığında ise, kütüphane çalışanlarının en çok kullanıcı etkileşimlerinin dışarıdan izlenmesi ve kullanıcıların sınırlı veri gizliliği okuryazarlığı konusunda endişeli olduklarını göstermektedir (Anderson vd., 2026, s. 8).

7. Bulgular

"Bilgi güvenliği konusu literatürde çok disiplinli bir yaklaşımla ele alınmaktadır ve literatürde de bilgi güvenliği konusunda gerçekleştirilmiş birçok çalışma mevcuttur (Şafak ve Soylu, 2025, s. 195)." Bilgi merkezlerinde ve kütüphanelerde ise, kurumsal bilgi güvenliği yönetimine ilişkin araştırmaların ise daha az sayıda olduğu anlaşılmaktadır (Kavak ve Odabaş, 2023, s.299). Bu bağlamda literatür çalışmalarında hareketle, Türkiye'de bilgi merkezleri ve kütüphaneler, üniversite kütüphaneleri bağlamında bilgi güvenliği ve kişisel verilerin korunması konusunda gerçekleştirilen araştırmaların sınırlı olduğu literatür çalışmalarından anlaşılmaktadır. Özellikle Türkiye'de 6698 sayılı KVKK kanunu kapsamında gizlilik, mahremiyet ve kişisel veriler ekseninde gelişmelerin ve korunma çalışmalarının artması da üniversite kütüphanelerinin de yönetici-kütüphaneci-kullanıcı bağlamında gizlilik, mahremiyet, kişisel verilerin korunması bağlamında bilgi güvenliğinin sağlanmasını ve veri bütünlüğünün sağlanmasını zorunlu kılmıştır. Bilgi ve belge merkezlerine yansıyan bu zorunluluk hali, etkili bir Bilgi Güvenliği Yönetim Sistemi'nin ve ISO/IEC 27001 strandartlarının oluşturulması, bilgi güvenliği ve kişisel verilerin korunması konusunda politika belgelerinin hazırlanmasının gerekli kılmıştır.

Araştırma kapsamında da ele alınan model çerçevesinde, Kütüphane Bilgi Sistemi Değerlendirme Modeli'nin teknolojik ve organizasyonel ölçümler bağlamında iki farklı şekilde uygulandığı tespit edilmiştir. Söz konusu ölçümlerin farkındalık, yönetim, prosedür, politika ve teknoloji bağlamında ele alınmıştır. Bilgi güvenliği yalnızca teknik sistemlerin korunmasına yönelik bir konu olmaktan çıkarak insan süreç ve teknoloji unsurlarının birlikte ele alınmasını gerektiren bütüncül bir yönetim alanına dönüştüğü Ismail ve Zainab'ın hazırlamış olduğu modelden anlaşılmaktadır. Aynı zamanda literatür çalışmalaında da kütüphane güvenliğinin yalnızca tekbik bir işlev olarak değil, çok boyutlu kurumsal bir kaygı olarak ele alınması gerektiğinden bahsedilmiştir (Bhatt vd., 2026, s. 3).

Literatür çalışmalarındaki veriler ışığında, araştırmamızın birinci sorusu (S1) bağlamında Türkiye'de üniversite kütüphanelerinde bilgi güvenliği uygulamalarının giderek arttığı ve yönetici/personel/kullanıcı farkındalık düzeylerinin giderek arttığı görülmektedir. Araştırmanın ikinci sorusuna yönelik sonuçlar incelendiğinde ise, kişisel verilerin korunmasına yönelik üniversite kütüphanelerinde uygulamaların istenilen düzeyde olmadığı, kütüphane ve yöneticilerin bu konuda özellikle bilinç ve farkındalıklarının arttırılması gerektiği tespitedilmiştir. Bununla beraber, üniversite kütüphaneleri bağlanmında kullanıcılar ile ilişkilendirilebilen hassas verilerin korunmasına yönelik bilimsel çalışmaların arttırılması dikkatleri çekmektedir.

7. Sonuç ve öneriler

Araştırma kapsamında bilgi güvenliği, üniversite kütüphanelerinde bilgi güvenliği, kişisel verilerin korunması ve bu kavramlara dayalı olarak 'üniversite kütüphaneleri' bağlamında literatür çalışmaları gözden geçirilmiştir. Literatür çalışmalarından elde edilen sonuçlara göre, genel olarak Türkiye'de üniversite kütüphanelerinde bilgi güvenliği ve kişisel veri uygulamalarının yeterli derecede uygulanmadığı, bilgi güvenliği ve kişisel verillerin korunması farkındalık düzeylerinin yeterli düzeyde olmadığı saptanmıştır. Aynı zamanda, araştırma çerçevesinde Ismail & Zainab'ın (2013) yılında hazırlamış olduğu Kütüphane Bilgi Sistemi Modeli değerlendirilmiştir. Model çervevesinde bilgi güvenliğinin sadece teknik önlemlerle sınırlı kalmayacağı bunun yanı sıra organizasyonel önlemler çerçevesinde de değerlendirilmesi gerektiği belirlenmiştir. Araştırma çerçevesinde literatür çalışmalarına ve Kütüphane Bilgi Güvenliği Sistemi'ne dayanılarak üniversite kütüphanelerinde bilgi güvenliğinin sağlanması ve etkili bir veri korumanın sağlanması için geliştirilen öneriler şu şekildedir :

- Bilgi güvenliği ve kişisel verilerin korunması konusunda uygulamaların ve çalışmaların arttırılması,
- Üniversite kütüphanelerinde yönetici-personel-kullanıcı ekseninde bilgi güvenliği ve kişisel verilerin korunması konusunda eğitim ve programların düzenlenmesi,
- Bilgi güvenliği ve kişisel verilerin korunması hususunda bilinç ve farkındalık oluşturulmalı,
- Türkiye'de Üniversite ve Araştırma Kütüphaneciler Derneği'nin (ÜNAK) bilgi güvenliği ve kişisel verilerin korunması konusunda uygulamaların ve çalışmaların gerçekleştirilmesi,
- Türkiye'de Kütüphanecilik derneklerinin bilgi güvenliği ve kişisel verilerin korunması konusunda rehber ve politikaların hazırlanması,
- Türkiye'de üniversite kütüphanelerinde iyi bir bilgi güvenliği yönetim sisteminin geliştirilmesi gerekmektedir.

Kaynakça

Akkoyunlu, A. İşman ve H. F. Odabaşı (Ed). Eğitim teknolojileri okumaları 2018, (3. Bölüm, ss. 29-43). TOJET ve Sakarya Üniversitesi, Adapazarı. [Çevrim-içi: http://

yunus.hacettepe.edu.tr/~sadi/yayin/Kitap_ETO2018_Bolum3_29-43_BilgiGuvenligi.pdf, Erişim tarihi: 02.10.2018.]

Alanka, D. (2024). Nitel bir araştırma yöntemi olarak içerik analizi: teorik bir çerçeve. *Kronotop İletişim Dergisi, 1*(1), 64-84. https://izlik.org/JA92LL24LY

Anderson, B., Lund, B. D., Mohammed, Y., & Khan, Z. I. (2026). Personal data privacy literacy and library privacy awareness and concern among academic library employees. The Journal of Academic Librarianship, 52(5), 103310. https://doi.org/10.1016/j.acalib.2026.103310

Baykara, M., Daş, R. ve Karadoğan, İ. (2013). Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. 1st International Symposium on Digital Forensics and Security, 20-21 May 2013.

Elazığ, Turkey. Erişim adresi : http://web.firat.edu.tr/mbaykara/bg.pdf

Bhatt, K., Chander, R., Gandotra, P., Dhar, M., & Vashishtha, A. (2026). Knowledge protection in academic libraries: an empirical study of evolving security challenges and strategic measures. Studies in Higher Education, 1–20. https://doi.org/10.1080/03075079.2026.2706706

Bwiino, Keefa, Mayoka, Geoffrey Kituyi, Nkamwesiga, Lawrence, Nyamadi, Makafui, A systematic literature review of ınformation security practices in higher education contexts, IET Information Security, 2026, 6324508, 19 pages, 2026. https://doi.org/10.1049/ise2/6324508

Can, Ö., & Akbaş, M. (2014). Kurumsal ağ ve sistem güvenliği politikalarının önemi ve bir durum çalışması. TÜBAV Bilim Dergisi, 7(2), 16-31. https://izlik.org/JA28RL55JH

Data protection in the Eu: what does it mean for libraries? (briefing) – IFLA. (t.y.). Geliş tarihi 30 Eylül 2026, gönderen https://www.ifla.org/publications/data-protection-in-the-eu-what-does-it-mean-for-libraries-briefing/

Dijital Dönüşüm Ofisi. (t.y.). Hakkımızda. Erişim adresi: https://cbddo.gov.tr/hakkimizda/

Elihaki Kanyika, M., Sadykova, R., Tuenbaeva, K., & Chuwa, L. (2025). Yeni teknolojilere uyum: Akademik kütüphanelerde blok zinciri uygulamasının sistematik bir literatür incelemesi. *Bilgi Geliştirme* , *0* (0). https://doi.org/10.1177/02666669241312153

Eroğlu, Ş. (2026). Measuring transparency: evaluating privacy and data protection practices on academic library websites in Türkiye. The Journal of Academic Librarianship, 52(2), 103200. https://doi.org/10.1016/j.acalib.2026.103200

Gültekin, V., & Özel, N. (2023). üniversite öğrencilerinin bilgi güvenliği farkındalığı: Ankara üniversitesi örneği. Bilgi Yönetimi, 6(2), 310-331. https://doi.org/10.33721/by.1366855

Igbinovia, M. O., & Oladokun, B. D. (2025). Information security in libraries, librarianship, and ınformation science. In Encyclopedia of Libraries, Librarianship, and Information Science (pp. 401–411). Elsevier. https://doi.org/10.1016/B978-0-323-95689-5.00162-0

Henkoğlu, T., ve Uçak, N. Ö. (2015). Üniversite kütüphanelerinde kişisel verilerin korunması. Bilgi Dünyası, 16(1), 45-74. Erişim adresi : https://bd.org.tr/index.php/bd/article/view/87/80

Henkoğlu, T. (2015). Hassas bilgi varlıklarının ve kişisel verilerin hukuksal düzenlemeler ile korunması ve bu kapsamda üniversiteler için bilgi güvenliği politikasının geliştirilmesi (Tez No. 380076) [Doktora tezi, Hacettepe Üniversitesi]. Ulusal Tez Merkezi.

Henkoğlu, T. ve Yılmaz, B. (2013). Avrupa Birliği (AB) bilgi güvenliği politikaları. Türk

Kütüphaneciliği, 27(3), s.451-471. Erişim adresi : https://dergipark.org.tr/en/download/article-file/811421

Henkoğlu, T. ve Külcü, Ö. (2013). Bilgi erişim platformu olarak bulut bilişim: riskler ve hukuksal koşulllar üzerine bir inceleme. Bilgi Dünyası, 14(1), s. 62-86. Erişim adresi: https://bd.org.tr/index.php/bd/article/view/135/129

Henkoğlu, T. Ve Özenç Uçak, N. (2012). Elektronik bilgi güvenliğinin sağlanması ile ilgili hukuki ve etik sorumluluklar. Bilgi Dünyası, 13(2), s. 377-396. Erişim adresi: https://bd.org.tr/index.php/bd/article/view/147/141

Henkoğlu, T., & Külcü, Ö. (2013). Bilgi erişim platformu olarak bulut bilişim: riskler ve hukuksal koşullar üzerine bir inceleme. *Bilgi* Dünyası, 14(1), 62-86. https://doi.org/10.15612/BD.2013.135

Edet, N., & Emmanuel, E. (2026). Cybersecurity and Information Management in Digital Libraries: Emerging Challenges for Nigerian Academic Institutions. Global Journal of Modern Research and Emergıng Trends, 2(4), 101-123. https://doi.org/10.67487/gjmret.v2i4.245

Gültekin, V., & Özel, N. (2023). Üniversite öğrencilerinin bilgi güvenliği farkındalığı: ankara üniversitesi örneği. Bilgi Yönetimi, 6(2), 310-331. https://doi.org/10.33721/by.1366855

International Federation of Library Associations and Institutions. (2026, 12 Mayıs). Open session call for submission: Cybersecurity in libraries (updated). https://www.ifla.org/news/open-session-call-for-submission-cybersecurity-in-libraries-updated/

Igbinovia, M. O., & Oladokun, B. D. (2025). Information security in libraries, librarianship, and ınformation science. Içinde Encyclopedia of Libraries, Librarianship, and Information Science (ss. 401-411). Elsevier. https://doi.org/10.1016/B978-0-323-95689-5.00162-0

Ismail, R., & Zainab, A. N. (2013). Assessing the status of library information systems security. Journal of Librarianship and Information Science, 45(3), 232-247. https://doi.org/10.1177/0961000613477676

Kavak, A., & Odabaş, H. (2023). Üniversite kütüphanelerinde teknolojik ve kurumsal bilgi güvenliği önlemlerinin uygulanma yeterliliği. Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 14(2), 293-332. https://doi.org/10.54558/jiss.1321640

Kavak, A. (2023). Üniversite kütüphanelerinde bilgi güvenliği yönetimi ve bir rehber önerisi (Tez No. 813823) [Doktora tezi, Çankırı Karatekin Üniversitesi]. Ulusal Tez Merkezi.

Kotoroi, G. (2023). Constraints facing African academic libraries in applying electronic security systems to protect library materials. International Journal of Librarianship, 8(1), 31-48. https://doi.org/10.23974/ijol.2023.vol8.1.272

Library Privacy Guidelines for Library Management Systems | ALA. (t.y.). Geliş tarihi 30 Eylül 2026, gönderen https://www.ala.org/advocacy/privacy/guidelines/library-management-systems

Malekolkalami, M., Jabbari, L., & Mantegh, H. (2024). Evaluating the status of information security management in faculty libraries: A case study of Allameh Tabatabai University. Information Security Journal: A Global Perspective, 33(5), 579-592. https://doi.org/10.1080/19393555.2024.2347255

Odularu OI (2025), "Bilgi teknolojisinin sürdürülmesinde kütüphanelerin önemine dair bir inceleme: Geleceğe yönelik yöntemlerne yönelik yeniden düşünmeye yönelik". Kütüphane Yönetimi , Cilt 46, Sayı 1-2, ss. 109–131, doi: https://doi.org/10.1108/LM-11-2023-0118

Privacy Field Guides for Libraries. (t.y.). Geliş tarihi 30 Eylül 2026, gönderen https://libraryprivacyguides.org/ https://doi.org/10.1108/LM-11-2023-0118

Öztemiz, S., & Yılmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği. Bilgi Dünyası, 14(1), 87-100. https://doi.org/10.15612/BD.2013.136

Program. E-Beyas. (2026, 13 Ekim). Gönderen https://2026.ebeyas.org/program

Sarıçoban, B. Y. Y., & Şahin, L. Ö. (2026). Bilgi profesyonelleri için dijital koruma stratejileri: Kütüphaneciler Özelinde Kavramsal Bir Değerlendirme. Education and Technology in Information Science, 3(2), 27-37.

Şafak, A. B. (2025). Üniversite kütüphanelerinde bilgi güvenliği politikalarının analizi ve kütüphanecilerin bilgi güvenliği farkındalık düzeylerinin belirlenmesi: Ankara'daki üniversite kütüphaneleri örneği (Tez No. 984189) [Yüksek lisans tezi, Ankara Yıldırım Beyazıt Üniversitesi]. Ulusal Tez Merkezi.

Seferoğlu, S.,Yıldız Durak, H., Karaoğlan Yılmaz, F.G., Yılmaz, R. (2018) Bilgi güvenliği farkındalığı ve bilgi güvenliği politikalarıyla ilgili bir inceleme, Eğitim Teknolojileri Okumaları, s.29-43, Adapazarı.

Şeşen, Y., & Şeşen, E. (2025). Üniversite öğrencilerinin kişisel verilerin korunması ve unutulma hakkı farkındalıkları: bilgi ve belge yönetimi, gazetecilik ve hukuk bölümleri üzerine bir araştırma. Bilgi Dünyası, 26(1), 255-286. https://doi.org/10.15612/BD.2025.775

Şişkin, D. Ş., & Çakmak, T. (2020). Üniversite kütüphanelerinde kişisel veriler: Ankara'daki 15 üniversite kütüphanesindeki uygulamaların analizi. Türk Kütüphaneciliği, 34(3), 458-484. https://doi.org/10.24146/tk.754346

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2020). Bilgi ve iletişim güvenliği rehberi. Erişim adresi : https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf

Tekerek, M. (2008). Bilgi güvenliği yönetimi. Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik Dergisi, 11(1), 132-137. Erişim adresi: https://dergipark.org.tr/en/download/article-file/423183

Yusuf, A., Yusuf, S. & Zayyana, H.M. (2021). Assessment of information security threats to information systems in Federal University Libraries, Nigeria. Samaru Journal of Information Studies, 21(1), s.38-47.

Zickau, A. (t.y.). LibGuides: learning analytics toolkit: privacy and Ethics. Geliş tarihi 30 Eylül 2026, gönderen https://acrl.libguides.com/val/latoolkit/privacy