



T.C.

BARTIN ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI

YÜKSEK LİSANS TEZİ

KAMU SEKTÖRÜNDE VERİ GÜVENLİĞİ VE VERİ MAHREMİYETİ
İLE İLGİLİ SORUNLAR VE ÇÖZÜM ÖNERİLERİ

FEYZA SÜMER

DANIŞMAN

PROF. DR. ALPER AYTEKİN

BARTIN-2025



T.C.

BARTIN ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI

**KAMU SEKTÖRÜNDE VERİ GÜVENLİĞİ VE VERİ MAHREMİYETİ İLE
İLGİLİ SORUNLAR VE ÇÖZÜM ÖNERİLERİ**

YÜKSEK LİSANS TEZİ

Feyza SÜMER

JÜRİ ÜYELERİ

Danışman : Prof. Dr. Alper AYTEKİN
Üye : Doç. Dr. Hakan ÖZKÖSE
Üye : Dr. Öğr. Üyesi Zafer BOZYER

BARTIN-2025

KABUL VE ONAY

Feyza SÜMER tarafından hazırlanan “KAMU SEKTÖRÜNDE VERİ GÜVENLİĞİ VE MAHREMİYETİ İLE İLGİLİ SORUNLAR VE ÇÖZÜM ÖNERİLERİ” başlıklı bu çalışma, 04.11.2025 tarihinde yapılan savunma sınavı sonucunda oy birliği ile başarılı bulunarak jürimiz tarafından Yüksek Lisans Tezi olarak kabul edilmiştir.

Başkan : Doç. Dr. Hakan ÖZKÖSE

Üye : Prof. Dr. Alper AYTEKİN

Üye : Dr. Öğr. Üyesi Zafer BOZYER

Bu tezin kabulü Lisansüstü Eğitim Enstitüsü Yönetim Kurulu’nun/...../20... tarih ve 20...../.....-..... sayılı kararıyla onaylanmıştır.

Prof. Dr. Zafer CEYLAN
Enstitü Müdürü

BEYANNAME

Bartın Üniversitesi Lisansüstü Eğitim Enstitüsü tez yazım kılavuzuna göre Prof. Dr. Alper AYTEKİN danışmanlığında hazırlamış olduğum “KAMU SEKTÖRÜNDE VERİ GÜVENLİĞİ VE MAHREMİYETİ İLE İLGİLİ SORUNLAR VE ÇÖZÜM ÖNERİLERİ” başlıklı yüksek lisans tezimin bilimsel etik değerlere ve kurallara uygun, özgün bir çalışma olduğunu, aksinin tespit edilmesi halinde her türlü yasal yaptırımını kabul edeceğimi beyan ederim.

04.11.2025

Feyza SÜMER

ÖN SÖZ

Bu tez çalışmasının hazırlanmasında bilgi ve deneyimiyle bana rehberlik eden, her aşamada yapıcı katkıları ve kıymetli yönlendirmeleriyle sürece ışık tutan danışmanım Sayın Prof. Dr. Alper Aytekin'e en içten teşekkürlerimi sunarım.

Tez izleme ve değerlendirme sürecinde katkılarını esirgemeyen değerli jüri üyeleri Sayın Dr. Öğretim Üyesi Zafer Bozyer ve Sayın Doç. Dr. Hakan Özköse'ye, bilimsel katkıları ve değerli değerlendirmeleri için teşekkür ederim.

Bu süreçte desteğini her daim hissettiğim ve akademik ilerleyişime katkı sağlayan çalıştığım kuruma teşekkür ederim. Tez süreci boyunca desteğini esirgemeyen dostum Dr. Fatma AKGÜN'e, sabrıyla ve sevgisiyle yanımda olan, bana hep güç veren sevgili eşim Yavuz Selim SÜMER'e, hayatıma neşe ve huzur katan kedim Duman'a ve bu süreç biterken bana armağan olarak gelen, henüz gözlerini açmamış minik bebeğime teşekkür ederim.

Bununla birlikte, isimlerini tek tek anamasam da bu süreçte bilgi, destek ve moral sağlayan tüm dostlarıma ve katkı sunan herkese teşekkür ederim. Varlığınız, bu akademik yolculuğu daha anlamlı ve değerli kıldı.

Feyza SÜMER

ÖZET

Yüksek Lisans Tezi

KAMU SEKTÖRÜNDE VERİ GÜVENLİĞİ VE VERİ MAHREMİYETİ İLE İLGİLİ SORUNLAR VE ÇÖZÜM ÖNERİLERİ

Feyza SÜMER

Bartın Üniversitesi

Lisansüstü Eğitim Enstitüsü

Yönetim Bilişim Sistemleri Anabilim Dalı

Tez Danışmanı: Prof. Dr. Alper AYTEKİN

Bartın-2025, sayfa: 113

Bu tez ile, kamu sektöründe veri güvenliği ve veri mahremiyetiyle ilişkin mevcut sorunlar belirlenmiş ve bu sorunlara yönelik çözüm önerileri geliştirilmiştir. Dijital dönüşüm süreciyle birlikte kamu kurumları, büyük hacimli ve hassas nitelikli kişisel verileri işlemekle sorumlu hale gelmiştir. Ancak artan siber saldırılar ve sistemsel güvenlik açıkları, veri güvenliği politikalarının etkinliğini sorgulatmakta; kamu hizmetlerinin sürdürülebilirliği ve vatandaş mahremiyeti açısından risk oluşturmaktadır.

Araştırmada nicel yöntemler kullanılarak İçişleri Bakanlığı bünyesinde görev yapan teknik personelin veri güvenliği ve veri mahremiyetine ilişkin farkındalık düzeyleri ile çözüm önerilerine yönelik tutumları ölçülmüştür. Elde edilen bulgular, farkındalık düzeyinin orta-iyi seviyede olduğunu, ancak uygulamalarda çeşitli eksikliklerin bulunduğunu göstermektedir. İlişkisel analiz bulguları, farkındalığın çözüm önerilerine yönelik tutumlar üzerinde anlamlı ve pozitif etkisi olduğunu ortaya koymuştur.

Bu çerçevede kamu çalışanlarının sürekli eğitimi, ileri teknolojilerin kullanımı, güvenlik politikalarının güncellenmesi ve kurumlar arası iş birliğinin güçlendirilmesi önerilmiştir.

Çalışma ayrıca, gelecekte yapılacak nitel araştırmalar için teorik ve pratik bir zemin oluşturmaktadır.

Anahtar Kelimeler: Veri güvenliği, veri mahremiyeti, kamu sektörü



ABSTRACT

M.A. Thesis

PROBLEMS AND SOLUTION SUGGESTIONS REGARDING DATA SECURITY AND DATA PRIVACY IN THE PUBLIC SECTOR

Feyza SÜMER

Bartın University

Graduate School

Department of Management Information Systems

Thesis Advisor: Prof. Dr. Alper AYTEKİN

Bartın-2025, pp:113

This thesis identifies existing issues related to data security and data privacy in the public sector, and develops solutions to address these issues. In the context of the digital transformation process, public institutions have been assigned the responsibility of processing substantial quantities of sensitive personal data. However, the increasing frequency of cyberattacks and systemic security vulnerabilities call into question the effectiveness of data security policies, posing risks to the sustainability of public services and citizen privacy.

Quantitative methodologies were employed in the research to assess the awareness levels of technical personnel working within the Ministry of Interior regarding data security and data privacy, as well as their attitudes towards proposed solutions. The findings indicate that awareness levels are moderate to good, but there are various shortcomings in implementation. The findings of the relational analysis demonstrated that awareness exerts a significant and positive effect on attitudes towards proposed solutions.

In this context, it is recommended that public employees receive continuous training, advanced technologies be used, security policies be updated, and inter-institutional

cooperation be strengthened. The study also provides a theoretical and practical basis for future qualitative research.

Keywords: Data security, data privacy, public sector



İÇİNDEKİLER

KABUL VE ONAY.....	ii
BEYANNAME	iii
ÖN SÖZ	iv
ÖZET	v
ABSTRACT	vii
İÇİNDEKİLER.....	ix
ŞEKİLLER DİZİNİ.....	xii
TABLolar DİZİNİ.....	xiv
EKLER DİZİNİ.....	xv
KISALTMALAR.....	xvi
1.GİRİŞ.....	1
1.1. Tezin Amacı ve Kapsamı	1
1.2. Problem Tanımı	2
1.3. Araştırma Soruları	3
1.4. Araştırmanın Önemi.....	5
1.5. Tezin Yapısı.....	6
2.KAVRAMSAL ÇERÇEVE	8
2.1.Veri: Tanımı ve Önemi.....	8
2.2. Kişisel Veri Kavramı.....	9
2.1.1. Kişisel Verilerin İşlenmesi	10
2.2.2.Özel Nitelikli Kişisel Veriler	12
2.3. Veri Güvenliği: Tanımlar ve Kavramlar	13
2.3.1. Veri Güvenliği Saldırıları ve Etkileri	15
2.4. Veri Mahremiyeti: Tanımlar ve Kavramlar	17
2.5. Veri Güvenliği ve Veri Mahremiyeti Arasındaki İlişki.....	18
2.6. Kamu Sektöründe Veri Yönetimi	20

2.7. Kişisel Verilerin Korunması: Yasal Düzenlemeler ve Uygulamalar	21
2.7.1. Türkiye'de Kişisel Verilerin Korunması Kanunu (KVKK)	21
2.7.2. Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)	23
2.7.3. Uluslararası Diğer Yasal Düzenlemeler	25
2.8. Dijitalleşmenin Kamu Sektöründeki Rolü	29
2.9. Kamu Sektöründe Veri Güvenliği Ve Mahremiyeti.....	31
2.10. Kamu Sektöründe Veri Güvenliği Sorunları	32
2.10.1. İç Tehditler	32
2.10.2. Dış Tehditler.....	32
2.10.3. Veri Mahremiyeti İhlalleri ve Sonuçları.....	33
2.10.3.1. Kişisel Veri İhlallerinin Bireyler Üzerindeki Etkileri.....	34
2.10.3.2. Veri İhlallerinin Kurum İmajı ve Güvenilirliği Üzerindeki Etkiler.....	34
2.11. Siber Saldırıları ve Kamu Sektörü.....	35
2.11.1. Kamu Kuruluşlarına Yönelik Yaygın Siber Tehditler	35
2.11.2. Kamu Sektörüne Yönelik Saldırılarda Siber Savunma Stratejileri	35
2.12. Kamu Sektöründe Veri Güvenliği Politikaları ve Uygulamaları.....	36
2.12.1. Mevcut Politikalar ve Stratejiler.....	36
2.13. Veri Güvenliği Ve Mahremiyetine Yol Açan Sorunlar	37
2.13.1. Teknolojik Altyapının Yetersizliği	37
2.13.1.1. Eski Sistemler ve Güvenlik Açıkları.....	38
2.13.1.2. Veri Yedekleme ve Kurtarma Eksiklikleri	38
2.13.2. Kamu Çalışanlarının Farkındalık ve Eğitim Eksikliği	39
2.13.2.1. Eğitim Programlarının Yetersizliği	41
2.13.2.2. Çalışanların Güvenlik Protokollerine Uyumu.....	41
2.13.3. Yasal Boşluklar ve Düzenleme Eksiklikleri.....	42
2.13.3.1. Yasal Düzenlemelerde Eksik Kalan Alanlar	43
2.13.3.2. Veri İhlali Sonrasında Yasal Yaptırımlar.....	43

2.13.4. Finansal Kısıtlamalar	44
2.13.4.1. Veri Güvenliği için Ayrılan Kaynakların Azlığı	45
2.13.4.2. Güvenlik Teknolojilerine Yatırım Eksikliği	46
2.13.5. Kurum İçi Güvenlik Kültürünün Eksikliği.....	46
2.13.5.1. Yönetimsel Destek Eksikliği	48
2.13.5.2. Çalışanların Güvenlik Sorunlarına Yaklaşımı	48
2.14. Türkiye'de Kamu Kurumlarına Yönelik Siber Saldırı Örnekleri.....	49
2.14.1. 2016 Türkiye Cumhuriyeti Bilgi Teknolojileri ve İletişim Kurumu (BTK) Saldırısı.....	50
2.14.2. 2020 Sağlık Bakanlığı Saldırısı	50
2.14.3. 2018 Türkiye Cumhuriyeti Merkez Bankası Saldırısı.....	50
2.14.4. 2022 Belediyelere Yapılan Fidyeye Yazılım Saldırıları.....	51
2.15. Veri Güvenliği ve Mahremiyetine Yönelik Çözüm Önerileri.....	51
2.15.1. Teknolojik Altyapının Güçlendirilmesi	51
2.15.1.1. Bulut Teknolojilerinin Kullanımı	51
2.15.1.2. Güncel Güvenlik Sistemleri ve Yazılımlar	52
2.15.2. Kamu Çalışanlarının Eğitim ve Farkındalık Programları	53
2.15.2.1. Farkındalık Yaratma Stratejileri.....	53
2.15.2.2. Düzenli Güvenlik Eğitimi ve Sertifikasyon Programları.....	54
2.15.3. Güçlendirilmiş Yasal Düzenlemeler	54
2.15.3.1. KVKK ve GDPR Kapsamındaki Düzenlemelerin İyileştirilmesi	54
2.15.3.2. Veri İhlallerine Karşı Yasal Yaptırımların Artırılması	55
2.15.4. Finansal Kaynakların Artırılması	55
2.15.4.1. Kamu Bütçelerinde Veri Güvenliğine Ayrılan Payın Yükseltilmesi.....	55
2.15.4.2. Güvenlik Teknolojilerine Yatırım	56
2.15.5. Kurumlar Arası İşbirlikleri ve İşbirliği Modelleri	57
2.15.5.1. Kamu-Özel Sektör İşbirlikleri	57

2.15.5.2. Ulusal ve Uluslararası Güvenlik İnisiyatifleri	58
3. LİTERATÜR TARAMASI.....	60
4. ARAŞTIRMA METODOLİJİSİ.....	64
4.1. Araştırma Yöntemi.....	64
4.2. Örneklem Seçimi	64
4.3. Araştırmanın Modeli ve Hipotezi.....	65
4.4. Veri Toplama Araçları.....	66
4.4.1. Veri Toplama Süreci	67
4.4.2. Veri Analizi	67
4.4.3. Araştırma Ölçekleri.....	68
4.5. Araştırmanın Sınırlılıkları.....	69
5. BULGULAR VE TARTIŞMA	71
5.1. Tanımlayıcı Bulgular.....	71
5.2. Geçerlilik Analizi.....	76
5.2.1. Veri Güvenliği ve Mahremiyeti Farkındalık Ölçeği Geçerlilik Analizi Bulguları.....	76
5.2.2. Veri Güvenliği ve Mahremiyeti Çözüm Önerileri Ölçeği Geçerlilik Analizi.....	78
5.3. Güvenilirlik Analizi	79
5.3.1. Veri Güvenliği ve Mahremiyeti Farkındalık Ölçeğine dair Güvenilirlik Analizi.....	79
5.3.2. Veri Güvenliği ve Mahremiyeti Çözüm Önerileri Ölçeğine dair Güvenilirlik Analizi.....	80
5.4. Normallik Bulguları	81
5.5. İlişkisel Bulgular	82
5.5.1. Cinsiyet Değişkenine Göre Farklılık Analizi Bulguları	83
5.5.2. Yaş Aralığı Değişkenine Göre Farklılık Analizi Bulguları.....	84
5.5.3. Eğitim Değişkenine Göre Farklılık Analizi Bulguları.....	86

5.6. Alt Boyutlar Arasındaki Korelasyon Bulguları.....	87
5.7.Genel Bulguların Deęerlendirilmesi	88
5.8.Tartışma	89
6. SONUÇ VE ÖNERİLER	93
6.1. Sonuç.....	93
6.2. Öneriler	96
6.2.1. Kamu Kurumlarına Yönelik Öneriler	96
6.2.2. Gelecek Araştırmalara Yönelik Öneriler	98
KAYNAKLAR.....	99
EKLER	109
ÖZGEÇMİŞ	112

ŞEKİLLER DİZİNİ

Şekil	Sayfa
No	No
2.1:	Saldırı türlerine göre en çok saldırıya uğrayan 10 sektörün dağılımı 16



TABLÖLAR DİZİNİ

No	Sayfa
2.1: Kamu sektöründe karşılaşılan başlıca saldırı türleri ve bu saldırıların potansiyel etkileri	15
5.1: Demografik bilgilerin tanımlayıcı bulguları	71
5.2: Ölçeklere ait maddelerin tanımlayıcı bulguları	74
5.3: VGMFÖ geçerlilik analizi bulguları	77
5.4: VGMÇÖÖ geçerlilik analizi bulguları	79
5.5: VGMFÖ güvenirlik analizi bulguları	80
5.6: VGMÇÖÖ güvenirlik analizi bulguları	81
5.7: Alt boyutların normallik testi bulguları	82
5.8: Cinsiyet ile KUF, KRF ve KÇS alt boyutları arasındaki Bağımsız Örneklem T testi bulguları	83
5.9: Cinsiyet ile SÖ alt boyutu arasındaki Mann Whitney U testi bulguları	84
5.10: Yaş aralığı ile KUF, KRF ve KÇS alt boyutları arasındaki Tek Yönlü Anova testi bulguları	84
5.11: Yaş aralığı ile SÖ alt boyutu arasındaki Kruskal Wallis testi bulguları	85
5.12: Eğitim ile KUF, KRF ve KÇS alt boyutları arasındaki Tek Yönlü Anova testi bulguları	86
5.13: Eğitim ile SÖ alt boyutu arasındaki Kruskal Wallis testi bulguları	87
5.14: Spearman Korelasyon analizi bulguları	88

EKLER DİZİNİ

Ek	Sayfa
No	No
EK 1. Anket formu.....	110
EK 2. Etik Kurulu Onay belgesi.	112



SİMGELER VE KISALTMALAR DİZİNİ

e	: Hata payı
max	: Maximum
min	: Minimum
min	: Minimum
N	: Evren büyüklüğü
n	: Örneklem sayısı
p	: Anlamlılık değeri
r	: Korelasyon katsayısı
Sıra $\bar{x}$	: Sıra ortalaması
ss	: Standart sapma
$\bar{x}$	: Ortalama
α	: Cronbach's Alpha değeri

KISALTMALAR

ABD	: Amerika Birleşik Devletleri
AFA	: Açımlayıcı Faktör Analizi
ANOVA	: Analysis of Variance
AES-256	: Gelişmiş Şifreleme Standardı
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
BX SX	: Bölüm x Soru x
CISA	: Sertifikalı Bilgi Sistemleri Denetçiliği
DDoS	: Dağınık Hizmet Reddi
DoS	: Hizmet Reddi
DLP	: Veri Kaybı Önleme
ENISA	: Avrupa Siber Güvenlik Ajansı
FISMA	: Federal Bilgi Güvenliği Yönetimi Yasası
GDPR	: Avrupa Birliği Genel Veri Koruma Tüzüğü
HIPAA	: Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası
IDS/IPS	: Saldırı Tespit ve Önleme Sistemleri
KÇS	: Kurumsal Çözüm Süreçleri
KUF	: Kurumsal Uygulama/Farkındalık

KRF	: Kurumsal Risk Farkındalığı
KVKK	: Kişisel Verileri Koruma Kurumu
PDPA	: Singapur Kişisel Verilerin Korunması Yasası
PIPA	: Güney Kore Bilgi Koruma Yasası
PIPEDA	: Kanada Kişisel Bilgilerin Korunması ve Elektronik Belgeler Yasası
SÖ	: Stratejik Öncelik
SPSS	: Sosyal Bilimler için İstatistik Programı
VGMFÖ	: Veri Güvenliği ve Mahremiyeti Farkındalık Ölçeği
VGMÇÖÖ	: Veri Güvenliği ve Mahremiyeti Çözüm Önerileri Ölçeği



1.GİRİŞ

Bu bölümde; tezin kapsamı ve amacı, karşılaşılan problem durumu ile araştırma soruları, çalışmanın önemi ve tezin genel yapısına dair bilgiler sunulmaktadır.

1.1. Tezin Amacı ve Kapsamı

Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler, günümüz toplumlarını derinden etkilemekte ve "dijital dönüşüm" adı verilen yeni bir çağı başlatmaktadır. Bu dönüşüm, kamu sektörü de dahil olmak üzere tüm sektörlerde veriye dayalı hizmet modellerine geçişi zorunlu kılmaktadır (Çeliksoy ve Akça, 2024). Kamu kurumları, vatandaşlarına daha etkin, verimli, şeffaf ve erişilebilir hizmetler sunabilmek için giderek artan bir şekilde büyük miktarda veri toplamakta, işlemekte ve saklamaktadır (Ökmen ve Çağatay, 2016). Bu veriler, nüfus kayıtlarından sağlık bilgilerine, vergi ödemelerinden adli kayıtlara kadar geniş bir yelpazede hassas kişisel bilgileri içerebilmektedir.

Ancak, bu verilerin hassasiyeti ve önemi göz önüne alındığında, kamu sektöründeki veri güvenliği ve veri mahremiyeti, kritik bir önem arz etmektedir. Veri güvenliği, verilerin yetkisiz erişime, kullanıma, ifşaya, değiştirilmeye, silinmeye veya tahrip edilmeye karşı korunması anlamına gelirken; veri mahremiyeti, bireylerin kendi verileri üzerinde kontrol sahibi olma hakkını ifade eder. Kamu kurumları, hem kendi operasyonel süreçlerinin güvenliğini sağlamak hem de vatandaşlarının temel hak ve özgürlüklerini korumak için verileri etkili bir şekilde yönetmek ve korumakla yükümlüdür (Dülger, 2016).

Bu tez, kamu sektöründe veri güvenliği ve veri mahremiyeti ile ilgili mevcut sorunları incelemeyi ve bu sorunlara yönelik çözüm önerileri sunmayı amaçlamaktadır. Günümüz dünyasında hızla artan dijitalleşme ve teknolojik gelişmeler, kamu kuruluşlarını büyük miktarda kişisel ve hassas veriyi yönetmekle yükümlü kılmaktadır. Bu durum, kamu sektörünü veri güvenliği ve mahremiyeti açısından önemli risklerle karşı karşıya bırakmaktadır. Bu çalışmanın amacı, Kamu sektöründeki bu riskleri ve sorunları ele almak ve bu alanlarda uygulanabilecek etkili stratejiler geliştirmektir. Bu tez çalışmasının amacı, kamu sektöründe veri güvenliği ve veri mahremiyeti konularında mevcut sorunları tespit etmek ve bu sorunlara yönelik çözüm önerileri geliştirmektir. Kamu sektörü, devletin temel işleyişini sağlamak için büyük miktarda veri işlemektedir ve bu verilerin güvenliği, hem

kamu kurumlarının hem de bireylerin mahremiyeti açısından kritik bir öneme sahiptir. Bu tezde, veri güvenliği ve mahremiyetine dair kavramsal çerçeve oluşturularak, veri güvenliği ve mahremiyetine yol açan sorunlar ve çözüm önerileri incelenecektir. Ayrıca, anket çalışması aracılığıyla İçişleri Bakanlığında çalışan bilgi işlem uzmanlarının görüşleri alınarak, veri güvenliği konusundaki farkındalık düzeyleri ve bu alandaki sorunları belirlemeye yönelik veri toplanacaktır. Sonuç olarak bu çalışma, Kamu sektöründeki veri güvenliği ve mahremiyetine dair pratik ve uygulanabilir çözüm önerileri sunmayı hedeflemektedir.

1.2. Problem Tanımı

Kamu sektörü, dijital dönüşümün beraberinde getirdiği fırsatları değerlendirirken aynı zamanda önemli zorluklarla da karşı karşıyadır. Özellikle, kamu kurumlarının giderek artan bir şekilde veriye dayalı hizmetlere yönelmesi, veri güvenliği ve veri mahremiyeti konularını kritik bir noktaya taşımıştır. Artık sadece verilerin toplanması ve saklanması değil, aynı zamanda bu verilerin yetkisiz erişim, kullanım, ifşa, değiştirme, silme veya tahrip edilmeye karşı etkin bir şekilde korunması da büyük önem taşımaktadır.

Bu noktada Kamu sektörü, çok boyutlu ve karmaşık bir problemle karşı karşıyadır. Giderek artan siber tehditler, Kamu kurumlarının veri sistemlerini hedef almakta ve hassas bilgilere erişmeye çalışmaktadır. Devlet destekli sofistike hacker gruplarından, kişisel çıkar sağlamayı hedefleyen siber suçlulara kadar geniş bir yelpazede yer alan tehdit aktörü, kamu kurumlarını hedef almaktadır. Bu sebeple veri ihlalleri, kamu kurumlarının itibarına ciddi zararlar verebilir, mali kayıplara yol açabilir ve hatta ulusal güvenliği tehdit edebilir (Badur ve Konca, 2022).

Bununla birlikte, problem sadece dış tehditlerle sınırlı da değildir. Kamu kurumları içerisinde yaşanan insan hataları, sistemsal açıklar ve yetersiz güvenlik politikaları da veri güvenliği ve veri mahremiyeti açısından önemli riskler oluşturmaktadır. Çalışanların farkındalık eksikliği, zayıf parola kullanımı veya sosyal mühendislik saldırılarına maruz kalmaları, veri ihlallerine davetiye çıkarabilmektedir (Demir ve Filiz, 2018).

Diğer bir problem ise, hızla gelişen teknolojilere ve değişen tehditlere ayak uydurmakta zorlanan yasal düzenlemelerdir. Mevcut düzenlemeler, her zaman yeni ortaya çıkan

tehditlere karşı yeterli koruma sağlayamayabilir ve bu durum belirsizlik ve uygulamada tutarsızlıklara yol açabilir.

Özellikle gelişmekte olan ülkelerde Kamu kurumlarının veri güvenliği ve veri mahremiyeti alanına yeterli kaynak ayıramaması da önemli bir problem olarak karşımıza çıkmaktadır. Yetersiz finansal kaynaklar, teknolojik altyapı eksikliği ve uzman personel yetersizliği, kamu kurumlarının veri güvenliği ve veri mahremiyetini sağlama kapasitesini olumsuz etkilemektedir (Hilbert, 2013).

Tüm bu faktörler bir araya geldiğinde, kamu sektöründe veri güvenliği ve veri mahremiyetinin sağlanmasının ne kadar karmaşık ve zorlu bir görev olduğu ortaya çıkmaktadır. Bu nedenle, problemin çok boyutlu yapısını anlamak ve etkili çözüm stratejileri geliştirmek büyük önem taşımaktadır.

Veri güvenliği ve mahremiyeti, Kamu sektörü gibi geniş bir kullanıcı tabanına sahip alanlarda, kritik bir sorun haline gelmiştir. Kamu kuruluşları, vatandaşlardan topladıkları verilerle hizmet vermekte ve bu verilerin gizliliğini sağlamak zorundadır. Ancak, kamu sektörüne yönelik artan siber saldırılar ve veri ihlalleri, bu kuruluşların veri güvenliği stratejilerinin yetersiz olduğunu göstermektedir. Bu bağlamda, kamu sektöründe veri güvenliği politikalarının nasıl güçlendirilebileceği ve bu alandaki farkındalık eksikliklerinin nasıl giderilebileceği önemli bir araştırma sorunu olarak ortaya çıkmaktadır (Ndou, 2004).

Kamu sektöründe veri güvenliği ve mahremiyeti, giderek dijitalleşen dünyada daha da ön plana çıkmaktadır. Ancak, bu alanda karşılaşılan sorunlar çeşitlilik göstermekte ve genellikle yetersiz altyapı, eğitim eksiklikleri ve yasal boşluklardan kaynaklanmaktadır. Özellikle teknolojik altyapının yetersizliği, eski sistemlerin kullanılması ve veri yedekleme süreçlerinin eksikliği gibi faktörler, kamu kurumlarının siber saldırılara karşı savunmasız kalmasına neden olmaktadır (Çakır ve Taşer, 2023). Ayrıca, çalışanların veri güvenliği konusundaki farkındalık düzeylerinin yeterli olmaması, kurum içi güvenlik kültürünün zayıflamasına yol açmakta ve veri ihlalleri ile karşılaşma riski artmaktadır.

1.3. Araştırma Soruları

Kamu sektöründe veri güvenliği ve veri mahremiyeti konularını çok yönlü bir perspektifle ele almayı ve detaylı bir şekilde açıklanan problemin, çözümüne katkı sağlayacak bulgular ortaya koymayı hedeflemektedir. Bu amaç doğrultusunda aşağıdaki araştırma sorularına cevap aranacaktır:

1.Kamu sektöründe veri güvenliği ve veri mahremiyeti alanında karşılaşılan başlıca sorunlar nelerdir? Bu soru, Kamu kurumlarının veri güvenliği ve veri mahremiyeti alanında karşılaştığı zorlukları ve tehditleri derinlemesine anlamak amacıyla sorulmaktadır. Siber saldırılar, iç tehditler, insan hataları, sistemsel açıklar, yasal düzenlemelerdeki yetersizlikler ve kaynak kısıtları gibi faktörler, bu kapsamda detaylı bir şekilde incelenecektir.

2.Mevcut yasal düzenlemeler, kamu sektöründe veri güvenliği ve veri mahremiyetinin sağlanması için yeterli midir? Bu soru, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) gibi temel yasal düzenlemelerin, kamu sektöründeki veri güvenliği ve veri mahremiyeti uygulamalarını ne ölçüde kapsadığını ve ne gibi eksiklikler içerdiğini analiz etmeyi amaçlamaktadır.

3.İçişleri Bakanlığında görev yapan bilgi işlem uzmanlarının veri güvenliği konusundaki farkındalık düzeyleri ve bu alandaki beklentileri nelerdir? Bu soru, veri güvenliği uygulamalarının başarısında insan faktörünün önemine dikkat çekmek ve İçişleri Bakanlığında görev yapan bilgi işlem uzmanlarının bakış açısını anlamak amacıyla sorulmaktadır. Uzmanların veri güvenliği konusundaki bilgi düzeyleri, karşılaştıkları zorluklar, mevcut uygulamalara yönelik değerlendirmeleri ve beklentileri bu kapsamda ele alınacaktır.

4.Kamu sektöründe veri güvenliği ve veri mahremiyetinin sağlanması için hangi çözüm önerileri geliştirilebilir? Bu soru, tez çalışmasının temel amacı doğrultusunda, kamu kurumlarının veri güvenliği ve veri mahremiyetini güçlendirmek için kullanabilecekleri somut, uygulanabilir ve etkili politika önerileri, teknik çözümler ve düzenlemeler geliştirmeyi hedeflemektedir.

Bu araştırma sorularına verilecek cevaplar, kamu sektöründe veri güvenliği ve veri mahremiyetinin sağlanması konusunda atılabilecek adımlar hakkında değerli bilgiler sunacak ve daha güvenli bir dijital ortam oluşturulmasına katkı sağlayacaktır.

1.4. Araştırmanın Önemi

Kamu sektörü, vatandaşların güvenliği ve gizliliği açısından kritik bir role sahiptir. Bu nedenle, bu sektörde yaşanan veri ihlalleri ve güvenlik zafiyetleri, hem kurumlar için hem de toplumun genel güvenliği için ciddi sonuçlar doğurabilir. Bu araştırma, kamu sektöründe veri güvenliği ve mahremiyetini artırmaya yönelik öneriler sunarak, hem akademik literatüre katkıda bulunmayı hem de pratikte uygulanabilir çözümler sunmayı hedeflemektedir. Ayrıca bu çalışma, kamu çalışanlarının veri güvenliği ve mahremiyeti konusundaki farkındalıklarını artırmaya yönelik stratejilerin geliştirilmesine de ışık tutacaktır.

Bu araştırmada, kamu çalışanlarının veri güvenliği ve mahremiyeti konusundaki farkındalıklarını ölçmek amacıyla iki ana yöntem kullanılmıştır. İlk olarak olarak, literatür taraması yöntemi kullanılarak mevcut çalışmalar incelenmiştir. Literatür taraması, kamu sektöründe veri güvenliği ve mahremiyeti ile ilgili mevcut sorunları, çözüm önerilerini ve uygulanan stratejileri anlamak amacıyla gerçekleştirilmiştir. Mevcut akademik çalışmaların, raporların ve yasal düzenlemelerin incelenmesi, bu alandaki temel kavramları ve teorik çerçeveleri anlamak açısından önemli bir kaynak sağlamaktadır. Ayrıca literatür taraması, araştırmanın temelini oluşturacak kavramların ve metodolojilerin belirlenmesine de yardımcı olmuştur.

İkinci olarak, kamu sektöründe çalışan çeşitli kademelerdeki personele yönelik bir anket uygulanmıştır. Anket, veri güvenliği ve mahremiyeti ile ilgili sorular içermekte olup, katılımcıların bu konulardaki bilgi düzeylerini, farkındalıklarını ve mevcut politikalar hakkındaki görüşlerini ölçmeyi hedeflemiştir. Elde edilen veriler, betimleyici istatistiksel analizler kullanılarak değerlendirilmiştir. SPSS programı aracılığıyla verilerin frekans analizleri, yüzde dağılımları ve çapraz tablolar oluşturularak analiz edilmiştir. Ayrıca, bazı soruların sonuçları arasında anlamlı farklılık olup olmadığını test etmek amacıyla korelasyon ve regresyon analizleri gibi ileri istatistiksel analizler uygulanmıştır.

Literatür taraması sonucunda elde edilen bilgiler, anket sonuçlarıyla karşılaştırılarak daha geniş bir perspektif sunmuş, kamu sektöründe veri güvenliği ve mahremiyetinin güçlendirilmesine yönelik önerilerin geliştirilmesine katkı sağlamıştır. Bu yaklaşım hem teorik hem de pratik açıdan zengin bir veri seti oluşturmayı hedeflemektedir.

1.5. Tezin Yapısı

Bu tez, veri güvenliği ve mahremiyeti konularını kapsamlı bir şekilde ele alarak, kamu sektöründeki uygulamaları ve sorunları derinlemesine incelemektedir. Birinci bölümde, tezin amacı ve kapsamı net bir şekilde belirlenmiş, araştırmanın temel problemleri ve soruları ortaya konmuştur. Araştırmanın önemine ve kullanılan yöntemlere dair bilgiler verilmiştir.

İkinci bölümde, kavramsal çerçeve oluşturulmuş, veri, kişisel veri ve veri güvenliği ile mahremiyeti konuları detaylandırılmıştır. Veri güvenliği saldırıları ve veri mahremiyeti ile ilgili temel kavramlar, yasal düzenlemeler ve uluslararası standartlar ışığında ele alınmıştır. Kamu sektöründe veri yönetimi konusuna odaklanılmış ve kişisel verilerin korunması ile ilgili yasal düzenlemeler detaylı bir şekilde incelenmiştir. Türkiye'deki Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) gibi önemli mevzuatlar, kamu sektörü uygulamaları ile ilişkilendirilmiştir. Kamu kurumlarında veri güvenliğinin önemi, karşılaşılan sorunlar ve siber saldırılar ile bunların sonuçları kapsamlı bir şekilde ele alınmıştır. Bununla birlikte veri güvenliği ve mahremiyetine yol açan sorunlar detaylandırılmış, teknolojik altyapının yetersizliği, kamu çalışanlarının farkındalık eksiklikleri, yasal boşluklar ve finansal kısıtlamalar gibi konular, güncel örneklerle desteklenerek tartışılmıştır. Türkiye'de kamu kurumlarına yönelik siber saldırı örnekleri ele alınarak, 2016'dan itibaren meydana gelen saldırılar incelenerek kamu sektöründeki güvenlik açıkları ve bu saldırıların sonuçları üzerinde durulmuş, veri güvenliği ve mahremiyetine yönelik çözüm önerileri sunulmuştur. Teknolojik altyapının güçlendirilmesi, kamu çalışanlarının eğitim programları ve yasal düzenlemelerin iyileştirilmesi gibi konular somut önerilerle desteklenmiştir.

Üçüncü bölümde, kamu sektöründe veri güvenliği ve veri mahremiyeti konusundaki mevcut literatür incelenerek bu alandaki sorunlar, çözüm önerileri ve önceki araştırmaların bulguları ele alınmıştır.

Dördüncü bölümde, araştırma metodolojisini detaylandırılmış, kullanılan yöntemler, örneklem seçimi ve veri toplama araçları hakkında bilgi verilmiştir.

Beşinci bölümde ise, toplanan verilerin analizi ve bulgularını içermektedir. Demografik özelliklerin değerlendirilmesi, farkındalık ve çözüm önerileri ölçeklerine ait alt boyutların bulguları ile değişkenler arası ilişkiler kapsamlı bir şekilde ele alınmıştır. Bu bölüm, araştırmanın temel bulgularını ve istatistiksel analizlerini sunmaktadır.

Son olarak, altıncı bölümde sonuçlar ve öneriler yer almaktadır. Elde edilen bulguların ışığında, veri güvenliği ve mahremiyeti konusundaki mevcut durum değerlendirilmiş ve gelecekteki araştırmalar için önerilerde bulunulmuştur.

Bu tez, veri güvenliği ve mahremiyeti konularında derinlemesine bir anlayış geliştirmeyi ve kamu sektöründeki uygulamaların iyileştirilmesine yönelik somut öneriler sunmayı amaçlamaktadır.



2.KAVRAMSAL ÇERÇEVE

Bu bölümde; veri, kişisel veri, veri güvenliği ve mahremiyeti kavramlarının tanımları ile önemleri, aralarındaki ilişkiler, kamu sektöründeki yönetim, yasal düzenlemeler, dijitalleşme süreçleri, karşılaşılan sorunlar, siber tehditler, mevcut politikalar ve çözüm önerilerine dair kapsamlı bir kavramsal çerçeve sunulmaktadır.

2.1.Verİ: Tanımı ve Önemi

Veri, bilgi teknolojileri çağının temel yapı taşlarından biridir (Doluküp ve Hakbilen, 2021). En geniş anlamıyla, veri belirli bir konu hakkında bilgi içeren ve çeşitli şekillerde temsil edilen semboller, sayılar veya metinlerdir. Ham bilgi olarak tanımlanan veri, işlenerek bilgiye dönüştürülür; bu bilgi, karar verme süreçlerinde, analizlerde ve stratejik planlamalarda kullanılır. Verinin doğru ve etkin bir şekilde yönetilmesi, özellikle kamu sektörü gibi büyük veri tabanlarına sahip organizasyonlar için kritik öneme sahiptir.

Veri, başlı başına bir anlam ifade etmese de, işlendiğinde ve yorumlandığında karar alma süreçlerini yönlendiren, eylemleri tetikleyen ve değer yaratan bir potansiyele sahiptir. Ayrıca, statik bir kavram olmayıp sürekli olarak evrimleşen ve çeşitlenen bir yapıya sahiptir. Bu bağlamda, veriyi daha iyi anlamak için farklı boyutlarıyla ele almak gerekir:

- **Yapılandırılmış ve Yapılandırılmamış Veri:** Geleneksel veritabanlarında düzenli bir şekilde depolanan ve kolayca analiz edilebilen yapılandırılmış verinin yerini, giderek artan bir biçimde yapılandırılmamış veri almaktadır. Metinler, e-postalar, sosyal medya paylaşımları, resimler ve videolar gibi formlarda var olan yapılandırılmamış veri, analiz edilmesi ve anlamlandırılması daha zorlu olsa da büyük bir potansiyel taşımaktadır (Zehir ve Bilgetürk, 2023).
- **Büyük Veri:** İnternetin yaygınlaşması ve nesnelerin interneti (IoT) gibi teknolojilerin gelişmesiyle birlikte üretilen veri miktarında muazzam bir artış yaşanmıştır. Büyük veri; hacmi, hızı ve çeşitliliği ile geleneksel veri işleme yöntemlerini zorlayan ve yeni teknolojiler gerektiren bir olgudur (Özköse, 2020).

- **Gerçek Zamanlı Veri:** Sensörler ve sosyal medya platformları gibi kaynaklardan anlık olarak üretilen gerçek zamanlı veri, anlık karar alma süreçleri, risk yönetimi ve müşteri deneyimini kişiselleştirme gibi alanlarda büyük bir dönüşüm potansiyeline sahiptir (Akram ve Dağdeviren, 2020).

21.yüzyılda veri odaklı bir topluma doğru hızla ilerlerken, verinin önemi ve etkileri her geçen gün artmaktadır. Günümüzde veri, işletmeler ve uluslar için önemli bir ekonomik değer haline gelmiştir. Veri analitiği ve yapay zeka gibi teknolojiler sayesinde, verilerden elde edilen içgörüler, yeni ürün ve hizmetlerin geliştirilmesi, operasyonel verimliliğin artırılması, müşteri deneyiminin iyileştirilmesi ve rekabet avantajı sağlanması gibi alanlarda kullanılmaktadır (Davenport, 2018).

Verinin etkin kullanımı, sağlık, eğitim, güvenlik ve çevre gibi alanlarda toplumsal sorunların çözümüne katkı sağlama ve yaşam kalitesini artırma potansiyeline sahiptir. Sağlık verilerinin analizi, hastalıkların erken teşhis ve tedavisinde, salgın hastalıkların önlenmesinde ve kişiselleştirilmiş sağlık hizmetlerinin sunulmasında önemli bir rol oynamaktadır (Alyass, Turcotte ve Meyre, 2015).

Veri analizi ve modelleme teknikleri, bilimsel araştırmalarda yeni keşiflerin yapılmasına ve karmaşık problemlerin çözülmesine olanak tanımaktadır. Genetik araştırmalar, iklim değişikliği modellemesi ve uzay araştırmaları gibi alanlarda veri, bilim insanlarının daha derinlemesine analizler yapmalarına ve yeni bilgiler üretmelerine yardımcı olmaktadır.

Veri, bilgi çağının vazgeçilmez bir unsuru haline gelmiş ve bireyler, kurumlar ve toplumlar üzerinde derin etkiler yaratmıştır. Verinin önemini kavramak, verinin doğru ve etik bir şekilde toplanması, işlenmesi, saklanması ve kullanılması için gerekli yasal ve etik çerçevelerin oluşturulması açısından büyük önem taşımaktadır (Sawiz, 2024). Özellikle kamu sektöründe verinin etkin ve verimli kullanımı, şeffaflığın ve hesap verebilirliğin artırılması, vatandaşlara daha iyi hizmetler sunulması ve toplumsal faydanın maksimize edilmesi için büyük bir potansiyel sunmaktadır. Ancak bu potansiyelin tam olarak hayata geçirilebilmesi için veri güvenliği ve mahremiyetinin sağlanması, veriye erişimin demokratikleştirilmesi ve veri okuryazarlığının yaygınlaştırılması gibi konulara öncelik verilmesi gerekmektedir.

2.2. Kişisel Veri Kavramı

Kişisel veri, belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmaktadır. Bu tür veriler, bireylerin kimliklerinin tespit edilmesine olanak tanır. Kişisel veriler, ad, soyad, T.C. kimlik numarası, doğum tarihi, adres, telefon numarası ve e-posta adresi gibi temel bilgilerden; sağlık bilgileri, finansal bilgiler, konum bilgileri ve genetik veriler gibi daha hassas bilgilere kadar geniş bir yelpazede ele alınabilir. Kişisel verilerin hassasiyeti, verinin niteliğine ve işleme amacına göre değişkenlik göstermektedir (Egemen, 2023).

Kişisel verilerin korunması, bireylerin özel hayatlarının gizliliğini sağlamak ve kötüye kullanılmasını önlemek amacıyla önemli bir konudur. Kamu sektörü, geniş bir veri tabanına sahip olması nedeniyle, kişisel veri koruma konusunda büyük bir sorumluluk taşımaktadır (Kocabıyık, 2023). Bu koruma, bireylerin mahremiyetini ve güvenliğini sağlamak amacıyla çeşitli yasal düzenlemelerle desteklenmektedir. Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), kişisel verilerin korunması konusunda katı kurallar getirmiştir. Türkiye'de ise Kişisel Verilerin Korunması Kanunu (KVKK) bu alanda önemli düzenlemeler içermektedir. Bu yasal düzenlemeler, kişisel verilerin toplanması, işlenmesi ve saklanması süreçlerinde belirli standartların uygulanmasını zorunlu kılmaktadır.

Kişisel verilerin korunması sadece yasal bir zorunluluk değil, aynı zamanda etik bir sorumluluktur. Bireylerin kişisel verilerinin izinsiz kullanılmaması, bu verilerin güvenli bir şekilde saklanması ve üçüncü şahıslarla paylaşılmaması, kamu kurumlarının güvenilirliğini artırmaktadır. Ayrıca, kişisel verilerin korunması, bireylerin dijital dünyada kendilerini güvende hissetmelerini sağlamaktadır.

Kişisel veri kavramı, modern bilgi toplumlarında büyük bir öneme sahiptir. Kişisel verilerin korunması, bireylerin mahremiyetinin sağlanması ve kamu kurumlarının güvenilirliğinin artırılması açısından kritik bir rol oynamaktadır. Bu nedenle, kişisel verilerin korunması konusunda yasal düzenlemelere uyulması ve gerekli önlemlerin alınması, kamu sektörü için vazgeçilmez bir gereklilik olarak öne çıkmaktadır.

2.2.1. Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi, kişisel verilerin otomatik sistemlerle veya otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması veya kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi kapsar (Yosif, 2021). Bu süreçler, hem kamu hem de özel sektörde, bireylerin mahremiyetini korumak ve veri güvenliğini sağlamak amacıyla belirli kurallara tabi tutulur. Kişisel verilerin işlenmesi, bireylerin rızasıyla veya yasal bir zorunluluk gereği gerçekleştirilmelidir.

Kişisel verilerin işlenmesinde iki temel ilke; hukuka uygunluk ve meşru amaçtır (Yücedağ, 2019). Kişisel veriler, ancak ilgili kişinin açık rızasına dayalı olarak veya kanunda öngörülen belirli şartların varlığı halinde işlenebilir. Bu şartlar arasında, bir sözleşmenin kurulması veya ifası için veri işlemenin zorunlu olması, yasal bir yükümlülüğün yerine getirilmesi, hayati çıkarların korunması gibi durumlar sayılabilir (Polater, 2019).

Kişisel verilerin işlenmesi sürecinde dikkat edilmesi gereken diğer ilkeler şunlardır:

- **Doğru ve gerektiğinde güncel olma:** Kişisel verilerin doğruluğunu ve gerektiğinde güncellenmesini sağlamak için gerekli önlemler alınmalıdır.
- **İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma:** Kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması gerekmektedir.
- **İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme:** Kişisel veriler, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

Bu ilkeler, hem bireylerin haklarını korumak hem de veri işleme süreçlerinde şeffaflık ve güvenilirlik sağlamak amacıyla belirlenmiştir. Kamu sektörü, geniş veri tabanlarına sahip olması ve vatandaşların kişisel bilgilerini toplaması nedeniyle, bu ilkelere uygun hareket etmek zorundadır. Bu, hem yasal bir zorunluluk hem de etik bir sorumluluktur.

Kişisel verilerin işlenmesi sürecinde, veri sorumlularının dikkat etmesi gereken önemli bir diğer konu, veri güvenliğidir. Veri güvenliği, kişisel verilerin yetkisiz erişim, değişiklik, ifşa

veya imha gibi risklere karşı korunması anlamına gelir. Bu amaçla, teknik ve idari tedbirlerin alınması gerekmektedir. Örneğin, şifreleme, erişim kontrolü ve veri maskeleyme gibi teknik önlemler, veri güvenliğini sağlamak için kullanılabilir (Şişkin, 2020).

Kişisel verilerin işlenmesi süreci, bireylerin mahremiyetini korumak ve veri güvenliğini sağlamak amacıyla belirli kurallara ve ilkelere uygun olarak yürütülmelidir. Kamu sektörü, bu süreçte yasal düzenlemelere ve etik sorumluluklara uygun hareket ederek, vatandaşların güvenliğini kazanmalı ve veri güvenliğini en üst düzeyde sağlamalıdır.

2.2.2. Özel Nitelikli Kişisel Veriler

Özel nitelikli kişisel veriler, bireylerin ırkı, etnik kökeni, siyasi düşünceleri, dini veya felsefi inançları, sendika üyeliği, sağlık bilgileri, cinsel hayatı, biyometrik ve genetik verileri gibi hassas bilgilerden oluşur. Bu tür veriler, bireylerin mahremiyetinin korunması açısından daha yüksek bir risk taşır ve bu nedenle daha sıkı koruma önlemleri gerektirir. Özel nitelikli kişisel veriler, kişilerin temel hak ve özgürlüklerini ihlal etme riski daha yüksek olan verilerdir ve bu nedenle daha sıkı kurallara tabidir (Özer Deniz, 2021).

Özel nitelikli kişisel verilerin işlenmesi, genellikle bireyin açık rızası ile veya yasal bir zorunluluk gereği gerçekleştirilir. Bu tür verilerin işlenmesi sürecinde dikkat edilmesi gereken bazı temel ilkeler ve kurallar şunlardır:

- **Açık Rıza:** Özel nitelikli kişisel verilerin işlenmesi, kural olarak, verisi işlenen bireyin açık rızasına bağlıdır. Açık rıza, belirli bir konuya yönelik, bilgilendirmeye dayalı ve özgür irade ile verilen onay anlamına gelir. Bireylerin özel nitelikli kişisel verilerinin işlenmesi, onların mahremiyetine ve kişisel haklarına yüksek derecede önem verilmesini gerektirir.
- **Yasal Zorunluluk:** Bazı durumlarda, özel nitelikli kişisel veriler, yasal bir zorunluluk veya kamu yararı gereği işlenebilir. Ülkemizde e-nabız sisteminde sağlık verilerinin işlenmesi, halk sağlığının korunması veya tıbbi teşhis ve tedavi süreçlerinin yürütülmesi amacıyla yasal olarak zorunludur.
- **Ayrımcılık Yapmama:** Özel nitelikli kişisel verilerin işlenmesi, ayrımcılığa yol açmamalıdır. Bu tür veriler, bireylerin ırkı, etnik kökeni, dini inançları veya cinsel

yönelimi gibi hassas bilgileri içerdiği için, bu verilerin kötüye kullanılması ayrımcılığa ve hak ihlallerine neden olabilir.

Özel nitelikli kişisel verilerin korunması, veri güvenliği açısından daha yüksek bir standart gerektirir. Bu verilerin korunması için alınması gereken teknik ve idari tedbirler, diğer kişisel verilere kıyasla daha kapsamlı ve etkili olmalıdır. Biyometrik verilerin korunması için gelişmiş şifreleme teknikleri kullanılabilir ve bu verilere erişim yetkisi sadece belirli yetkililere verilebilir (Natgunanathan vd., 2016).

Özel nitelikli kişisel verilerin işlenmesi ve korunması konusundaki yasal düzenlemeler de oldukça katıdır. Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ve Türkiye'de Kişisel Verilerin Korunması Kanunu (KVKK), bu tür verilerin işlenmesi ve korunması konusunda ayrıntılı hükümler içermektedir. Bu yasal düzenlemeler, özel nitelikli kişisel verilerin işlenmesi sürecinde bireylerin haklarını korumayı hedeflemektedir.

Özel nitelikli kişisel verilerin işlenmesi sürecinde dikkat edilmesi gereken diğer önemli bir konu, veri minimizasyonudur. Veri minimizasyonu, sadece gerekli olan verilerin toplanması ve işlenmesi anlamına gelir. Bu ilke, gereksiz veri toplama ve işleme riskini azaltarak bireylerin mahremiyetini korur. Ayrıca, özel nitelikli kişisel verilerin işlenmesi sürecinde, verilerin anonimleştirilmesi veya takma ad kullanılması gibi yöntemler de kullanılabilir. Bu yöntemler, verilerin bireylerle doğrudan ilişkilendirilmesini engelleyerek mahremiyetin korunmasına katkı sağlar (Laurinaitis, Stitilis ve Verenius, 2021).

Özel nitelikli kişisel veriler, bireylerin mahremiyetini ve haklarını korumak amacıyla daha sıkı koruma önlemleri gerektirir. Bu tür verilerin işlenmesi sürecinde, yasal düzenlemelere ve etik ilkelere uygun hareket edilmesi büyük önem taşır. Kamu sektörü, özel nitelikli kişisel verilerin korunması konusunda yüksek standartları benimseyerek, vatandaşların güvenliğini kazanmalı ve veri güvenliğini en üst düzeyde sağlamalıdır.

2.3. Veri Güvenliği: Tanımlar ve Kavramlar

Veri güvenliği, bilgi sistemlerinin, verilerin ve bilgi kaynaklarının yetkisiz erişim, kullanım, ifşa ve yok edilme gibi tehditlere karşı korunmasını amaçlayan bir dizi strateji, politika ve teknolojik önlemleri içeren bir disiplindir (Kavak ve Odabaş, 2023). Bu kavram, hem kamu

hem de özel sektörde bilgi güvenliğinin sağlanması açısından kritik bir öneme sahiptir. Veri güvenliği, yalnızca teknik önlemlerle sınırlı kalmayıp aynı zamanda insan kaynağı yönetimi, organizasyonel süreçler ve yasal düzenlemeleri de kapsayan geniş bir çerçeveye sunar.

Veri güvenliği, bilgi teknolojilerinin gelişmesiyle birlikte bireylerin ve kurumların karşı karşıya kaldığı en büyük tehditlerden biri haline gelmiştir. Veri güvenliğinin temel bileşenleri arasında gizlilik, bütünlük ve erişilebilirlik yer almaktadır. Gizlilik, yalnızca yetkili kişiler tarafından verilere erişim sağlanmasını ifade ederken; bütünlük, verilerin doğruluğu ve tutarlılığına odaklanır. Erişilebilirlik ise, yetkili kullanıcıların verilere zamanında ulaşabilmesini sağlamayı hedefler (Nissenbaum, 2004). Bu üç bileşen, veri güvenliğinin etkin bir şekilde sağlanabilmesi için bir arada ele alınmalıdır.

Günümüzde özellikle dijital dönüşüm süreciyle birlikte, bilgi sistemleri üzerindeki tehditler de çeşitlenmiştir. Siber saldırılar, malware yazılımları, veri ihlalleri ve iç tehditler gibi unsurlar veri güvenliğini tehdit eden başlıca faktörler arasında yer almaktadır. Bu doğrultuda, veri güvenliği stratejileri; risk yönetimi, şifreleme, kimlik doğrulama ve güvenlik duvarları gibi çeşitli teknik ve organizasyonel önlemleri içermektedir (Al Naim ve Ghouri, 2023).

Gelişen teknolojiler, veri güvenliği alanında yeni yöntemlerin ve araçların ortaya çıkmasına olanak tanımaktadır. Ancak, aynı zamanda siber saldırıların sayısını ve karmaşıklığını da artırmıştır. Kamu sektöründe veri güvenliği, sadece teknik önlemlerle değil aynı zamanda politika ve eğitimle de desteklenmelidir. Kurumların veri güvenliği politikalarının oluşturulması, çalışanların bu politikalar hakkında bilinçlendirilmesi ve düzenli eğitimlerle desteklenmesi, veri güvenliğini artırmada önemli adımlar olarak değerlendirilmektedir. Şifreleme yöntemleri, çok faktörlü kimlik doğrulama sistemleri ve blockchain teknolojisi gibi yenilikçi çözümler, veri güvenliğini sağlamada etkin araçlar olarak öne çıkmaktadır (Yılmaz ve Ballı, 2016).

Veri güvenliği yalnızca teknik bir gereklilik değil, aynı zamanda bireylerin ve toplumun güvenliğini sağlamak için stratejik bir önceliktir. Özellikle kamu sektöründe veri güvenliği, güvenilir bir dijital altyapı oluşturma ve vatandaşların haklarını korumanın temel taşıdır. Bu nedenle, kamu kurumlarının veri güvenliği stratejilerini güçlendirmeleri ve sürekli olarak güncellemeleri elzemdir (Supangkat, Firmansyah, Rizkia ve Kinanda, 2025).

Veri güvenliği, modern bilgi sistemlerinin temel bir bileşeni olarak karşımıza çıkmakta ve sürekli olarak gelişen tehditler karşısında dinamik bir yaklaşım gerektirmektedir. Kamu sektörü için özellikle veri güvenliğinin büyük önem arz etmektedir ki vatandaşların kişisel bilgilerinin korunması ve kamu hizmetlerinin sağlıklı bir şekilde yürütülmesi açısından kritik bir rol oynamaktadır. Bu nedenle Kamu kurumları, veri güvenliği politikalarını oluşturmalı, bu politikaları düzenli olarak gözden geçirmeli ve güncellemeli, çalışanlarını bu konuda eğitmeli ve bilinçlendirmelidir. Ayrıca veri güvenliği teknolojilerinin etkin bir şekilde kullanılması ve sürekli olarak yeniliklerin takip edilmesi gerekmektedir.

Gelişen tehditler ve değişen teknoloji karşısında, veri güvenliği sürekli olarak güncel kalması sağlanmalıdır. Kamu sektörü, bu konuda proaktif bir yaklaşım benimsemeli ve veri güvenliği stratejilerini sürekli olarak gözden geçirerek, yeni tehditlere karşı önlemler almalıdır. Bu sayede, vatandaşların güveni kazanılabilecek ve kamu hizmetlerinin kesintisiz ve güvenli bir şekilde sunulması sağlanabilecektir (Enocson ve Söderholm, 2018).

Veri güvenliği Kamu sektöründe sadece bir gereklilik değil, aynı zamanda bir sorumluluk olarak kabul edilmelidir. Kamu kurumları, vatandaşların kişisel bilgilerinin korunması ve veri güvenliğinin sağlanması konusunda yüksek standartları benimsemeli ve bu standartları sürekli olarak geliştirmelidir ki böylelikle kamu hizmetlerinin güvenilirliği artırılabilir ve vatandaşların hakları korunabilir.

Veri güvenliği, vatandaşların kişisel bilgilerinin korunması ve kamu hizmetlerinin güvenli bir şekilde sunulması açısından büyük bir sorumluluk taşımaktadır. Bu nedenle, Kamu kurumlarının veri güvenliği stratejilerini güçlendirmeleri, sürekli olarak güncellemeleri ve bu alanda en iyi uygulamaları benimsemeleri gerekmektedir.

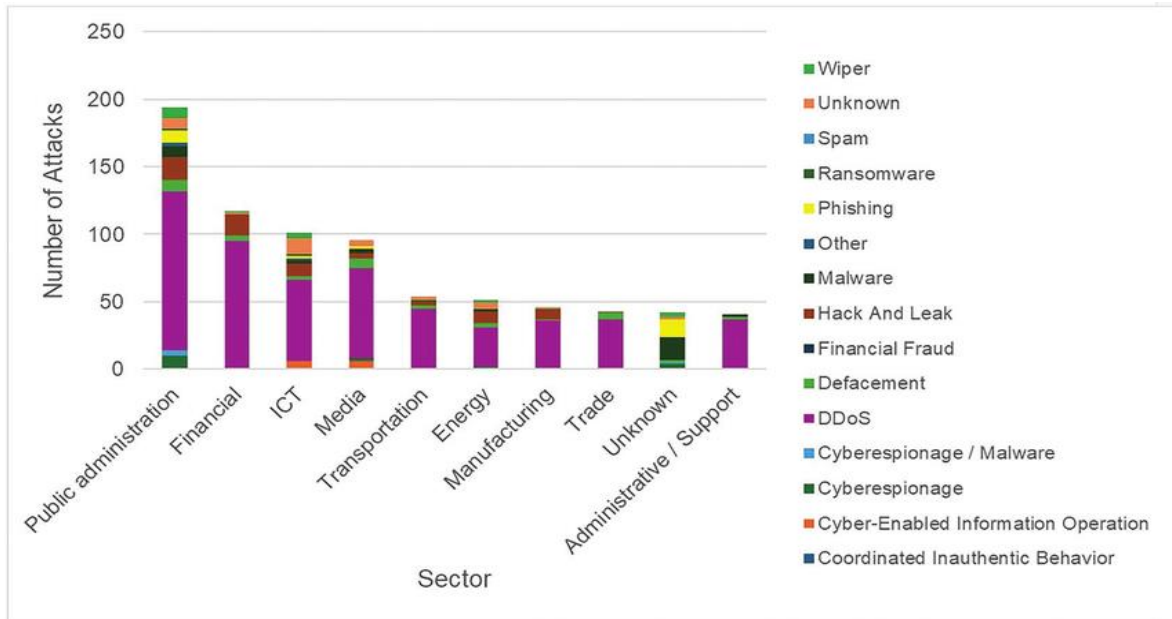
2.3.1. Veri Güvenliği Saldırıları ve Etkileri

Veri güvenliği, kamu sektöründeki kritik sistemlerin ve verilerin korunması açısından hayati bir öneme sahiptir. Bu bağlamda, çeşitli saldırı türleri, kamu kurumlarının veri güvenliği stratejilerini tehdit etmekte ve veri mahremiyetini riske atmaktadır. Kamu sektöründe karşılaşılan başlıca saldırı türleri ve bu saldırıların potansiyel etkileri aşağıdaki tabloda gösterilmiştir (Wicaksono, Purbaratri, Alam ve Safitri, 2024).

Tablo 2.1: Kamu sektöründe karşılaşılan başlıca saldırı türleri ve bu saldırıların potansiyel etkileri

Saldırı Türü	Tanım	Potansiyel Etkileri	Örnekler
Kötü Amaçlı Yazılım	Bilgisayara zararlı yazılım yükleyerek veri çalma	Veri kaybı, sistem arızası, mali kayıplar	Fidye yazılımları (Ransomware)
Phishing	Kullanıcıları sahte e-postalarla kandırarak kişisel bilgilerini çalma	Kimlik hırsızlığı, yetkisiz erişim	Oltalama e-postaları
DoS Saldırıları	Hizmetin kesintiye uğramasına neden olan saldırılar	Hizmet kesintileri, kamu güveninin zedelenmesi	DDoS (Dağıtık Hizmet Engelleme)
Veri İhlalleri	Yetkisiz erişimle hassas verilerin açığa çıkması	Kişisel verilerin kötüye kullanımı, itibar kaybı	Veri tabanı ihlalleri

Kamu sektöründeki saldırı türleri arasında en yaygın olarak hizmet engelleme (DoS), kötü amaçlı yazılımlar ve oltalama (phishing) saldırıları bulunmaktadır. Bu tür saldırılar, hem verilerin güvenliğini tehdit etmekte hem de kamu hizmetlerinin sürekliliğini riske atmaktadır. Özellikle fidye yazılımları, kamu sektöründeki kuruluşların operasyonlarını durdurma kapasitesine sahip olup, bu durum kamu güvenliğini ve vatandaşların hizmet alımını olumsuz etkilemektedir (Case, 2021).



Şekil 2.1 : Saldırı türlerine göre en çok saldırıya uğrayan 10 sektörün dağılımı (URL-1)

2.4. Veri Mahremiyeti: Tanımlar ve Kavramlar

Veri mahremiyetinin temel bileşeni "kişisel veri" kavramıdır. Kişisel veriler, bireyleri tanımlayan veya tanımlayabilen her türlü bilgiyi içermektedir. Bu bilgiler, isim, adres, telefon numarası ve e-posta gibi tanımlayıcı verilerin yanı sıra sağlık durumu, mali bilgiler ve çevrimiçi davranışlar gibi hassas verileri de kapsamaktadır (Bulut, 2020). Bu tür verilerin güvenliği, bireylerin mahremiyet haklarının korunması açısından son derece önemlidir.

Veri mahremiyeti, bireylerin kişisel verilerinin toplanması, işlenmesi ve paylaşılması ile ilgili haklarını ifade eder. Bu kavram, bireylerin rızası olmadan kişisel verilerinin kullanılmasını engellemeye yönelik bir çerçeve sunmaktadır. Dijitalleşmenin hız kazanmasıyla birlikte veri mahremiyeti daha da önem kazanmaktadır. Kamu sektörü, vatandaşların kişisel verilerini işleyen bir yapı olduğundan, veri mahremiyetine ilişkin yasal düzenlemeleri dikkate almak zorundadır (Ertekin, 2022).

Veri mahremiyetinin sağlanması, bireylerin kendi verileri üzerindeki kontrollerini arttırmakta ve veri işleme süreçlerinin şeffaflığını sağlamaktadır. Böylelikle veri mahremiyeti yalnızca bireylerin haklarını korumakla kalmaz, aynı zamanda toplumun güvenini de artırmaktadır. Kamu sektöründeki veri mahremiyeti uygulamaları, hem yasal düzenlemelere hem de etik ilkelere dayanmalıdır.

Veri mahremiyeti, teknoloji ve iletişim araçlarının gelişimiyle daha önce görülmemiş bir önem kazanmıştır. İlk olarak 19. yüzyılın sonlarında Amerika Birleşik Devletleri'nde "privacy" hakkı olarak tanımlanan bu kavram, dijital çağda kişisel verilerin korunması ile eş anlamlı hale gelmiştir (Solove, 2004). Günümüzde veri mahremiyeti, bireylerin haklarının korunmasının yanı sıra bilgi güvenliğinin sağlanması ve siber suçların önlenmesi için temel bir unsur olarak değerlendirilmektedir.

Veri mahremiyetine yönelik ihlaller yalnızca yasal sorunlar değil, aynı zamanda etik krizler de yaratabilmektedir. Özellikle, bireylerin bilgisi dışında toplanan ve ticari amaçlarla kullanılan veriler, etik kuralların ihlali olarak değerlendirilmektedir. Kamu sektörü, bu noktada vatandaşlarının haklarını korumak için etik ilkelere dayalı politikalar geliştirmelidir. "Privacy by Design" gibi yaklaşımlar, veri mahremiyetini sistemlerin tasarım

aşamasına entegre ederek proaktif bir koruma sağlamaktadır (Van Rest, Boonstra, Everts, Van Rijn ve Van Paassen, 2012).

Veri mahremiyetinin korunmasında teknolojik araçlar ve yöntemler önemli bir rol oynamaktadır. Şifreleme teknolojileri, anonimleştirme teknikleri ve blockchain uygulamaları, kişisel verilerin kötüye kullanılmasını engelleyebilir. Ancak, bu teknolojilerin etkili bir şekilde uygulanması, kamu kurumlarının teknolojik altyapılarının yeterliliğine bağlıdır (Rai, Shukla, Tightiz ve Padmanaban, 2024).

Veri mahremiyetine yönelik ihlallerin sonuçlarını anlamak için geçmişte yaşanan vakalar yol gösterici olabilir. 2020 yılında Hindistan’da kamu hizmetleri platformu Aadhaar’ın veri ihlali, milyonlarca vatandaşın kişisel bilgilerinin ifşa edilmesine yol açmıştır (Yoganandham, 2024). Bu tür olaylar, kamu sektöründe veri mahremiyetinin sağlanmasının ne kadar kritik olduğunu gözler önüne sermektedir.

Veri mahremiyeti, bireylerin güvenliğini ve mahremiyet haklarını korumanın yanı sıra kamu kurumlarının toplum nezdinde güvenilirliğini artırmaktadır. Dijitalleşmenin hız kazanmasıyla birlikte kamu sektöründeki veri mahremiyeti politikalarının sürekli olarak güncellenmesi ve iyileştirilmesi büyük önem taşımaktadır.

2.5. Veri Güvenliği ve Veri Mahremiyeti Arasındaki İlişki

Veri güvenliği ve veri mahremiyeti, günümüz dijital dünyasında birbirini tamamlayan ve etkileşim içinde olan iki kritik kavramdır. Bu kavramlar, veri koruma alanında sağlıklı bir denge kurulması açısından birlikte değerlendirilmelidir.

Veri güvenliği, bilgilerin yetkisiz erişim, hasar, kayıp veya kötüye kullanım gibi tehditlere karşı korunmasını ifade eder. Bu koruma, fiziksel ve dijital güvenlik önlemleri, şifreleme, kimlik doğrulama ve erişim kontrolü gibi çeşitli yöntemlerle sağlanmaktadır (Özkaya ve Toprak, 2022). Kamu sektöründe veri güvenliği, vatandaşların kişisel bilgilerinin korunması ve devletin bilgi sistemlerinin istikrarlı bir şekilde çalışmasının sağlanması açısından hayati bir öneme sahiptir.

Veri güvenliğinin sağlanması, yalnızca bireylerin haklarını korumakla kalmaz, aynı zamanda kamu kurumlarının itibarını da etkiler. Güvenlik ihlalleri, kamu güvenliğini zedelerken, bu durum devletin işleyişine olumsuz yansımaktadır.

Veri mahremiyeti ise bireylerin kişisel verilerinin toplanması, işlenmesi ve paylaşılması süreçlerinde, bireylerin rızasının alınmasını ve bu verilerin gizli tutulmasını ifade eder. Mahremiyet, bireylerin kendilerini güvende hissetmeleri ve özel hayatlarının korunması açısından kritik bir unsurdur. GDPR (General Data Protection Regulation) gibi düzenlemeler, veri mahremiyetinin önemini vurgulamakta ve kişisel verilerin korunmasına yönelik standartlar belirlemektedir (Voigt ve Von dem Bussche, 2017).

Veri mahremiyeti, bireylerin kendilerini ifade etme özgürlüğü ile doğrudan ilişkilidir. Kişisel verilerin kötüye kullanımı, bireylerin sosyal yaşamları üzerinde olumsuz etkiler yaratabilir ve bu durum demokratik değerlerin zayıflamasına yol açabilir.

Güçlü veri güvenliği önlemleri olmadan, kişisel verilerin korunması mümkün olmayabilir. Bir kuruluşun sahip olduğu kişisel veriler, güvenlik açıkları nedeniyle yetkisiz kişiler tarafından erişildiğinde, veri mahremiyeti ihlal edilmiş olur (Aswathy ve Tyagi, 2022). Bu tür ihlaller, bireylerin özel yaşamlarının tehlikeye girmesine ve kötüye kullanım durumlarına yol açabilir.

Öte yandan, veri güvenliği önlemlerinin uygulanması, veri mahremiyetinin korunmasına da katkıda bulunur. Güçlü güvenlik politikaları ve prosedürleri, kişisel verilerin yalnızca belirlenen ve izin verilen amaçlar doğrultusunda kullanılmasını sağlar (Hakkoymaz, Bakır ve Güçlü, 2019). Bu durum, bireylerin mahremiyet haklarının güvence altına alınmasını sağlamaktadır.

Veri güvenliği, verilerin fiziksel ve dijital ortamda korunmasını sağlarken, veri mahremiyeti, bireylerin haklarının ve özgürlüklerinin korunmasını hedefler. Bu iki kavram arasındaki denge, bireylerin ve kuruluşların güvenli bir dijital ortamda var olabilmesi ve güvenilir hizmetler sunabilmesi için kritik öneme sahiptir. Veri güvenliği ve veri mahremiyetinin entegrasyonu, siber güvenlik stratejilerinin ve veri yönetim politikalarının geliştirilmesi açısından önemli bir gereklilik olarak karşımıza çıkmaktadır.

2.6. Kamu Sektöründe Veri Yönetimi

Kamu sektörü, toplumun hizmet alımında kritik bir rol oynamaktadır. Kamu kurumları, topladıkları kişisel verilerin güvenliğini sağlamakla yükümlüdür. Bu nedenle, etkili bir veri yönetimi stratejisi geliştirmek, veri güvenliği ve mahremiyetinin sağlanması açısından büyük önem taşımaktadır.

Kamu sektörü, vatandaşların güvenliğini ve refahını sağlamak amacıyla büyük ölçekli veri toplama ve işleme faaliyetleri yürütmektedir. Bu bağlamda, etkili veri yönetimi stratejileri, yalnızca vatandaşların haklarını korumakla kalmaz, aynı zamanda kamu hizmetlerinin verimliliğini ve etkinliğini artırır. Veri yönetimi, veri toplama, saklama, işleme ve paylaşma süreçlerini düzenleyen politikalar ve uygulamalar bütünüdür (Labadie ve Legner, 2023).

Veri Yönetimi Süreçleri;

- 1. Veri Toplama:** Kamu kurumları, vatandaşların kişisel bilgilerini toplarken yalnızca ilgili amaçlara uygun verilerin toplanmasına dikkat etmelidir. Aşırı veri toplama, veri ihlalleri riskini artırabilir. Örneğin, yerel yönetimlerin e-belediye hizmetleri sırasında gereksiz bilgileri talep etmesi hem güvenlik hem de mahremiyet riskleri doğurabilir.
- 2. Veri Saklama:** Verilerin güvenli bir şekilde saklanması, özellikle büyük veri altyapılarında önemli bir maliyet ve yönetim sorumluluğu doğurur. Şifreleme, veri maskeleyme ve güvenli sunucu altyapıları, bu süreçte temel araçlar arasında yer almaktadır (İren ve Can, 2017).
- 3. Veri İşleme:** Kamu sektöründe işlenen verilerin analiz edilmesi ve raporlanması, stratejik karar alma süreçlerinde önemli bir rol oynamaktadır. Örneğin, sağlık sektöründe veri işleme, salgın hastalıkların izlenmesi ve sağlık politikalarının şekillendirilmesinde önemli katkılar sağlamaktadır.
- 4. Veri Paylaşımı:** Kamu kurumları arasında veya özel sektörle veri paylaşımı, hizmet uyumunu destekleyebilir. Ancak bu süreçlerde kişisel verilerin mahremiyeti ve güvenliği için sıkı protokoller uygulanmalıdır.

Veri yönetimi, kamu sektöründe üç temel amaç doğrultusunda önem arz etmektedir. Öncelikle vatandaşların haklarının korunması doğrultusunda veri mahremiyetine ilişkin ulusal ve uluslararası yasal düzenlemeler kamu kurumlarının vatandaş verilerini güvenli bir şekilde yönetmesini zorunlu kılar. Türkiye’de Kişisel Verilerin Korunması Kanunu (KVKK), kamu kurumlarına verilerin işlenmesinde açık rıza alma, amaçla sınırlı işleme ve yeterli güvenlik tedbirlerini alma yükümlülükleri getirmiştir (Şıracı, 2023).

Kamu hizmetlerinin etkin bir şekilde sunulabilmesi sebebiyle doğru, güncel ve analiz edilebilir verilerin elde edilmesi hizmet kalitesinin artırılmasıyla birlikte gerçekleşir. Veri yönetimi süreçlerinin iyileştirilmesi, karar alma mekanizmalarını güçlendirerek kamu yararına yönelik daha etkili politikalar geliştirilmesini sağlar (Tamer ve Övgün, 2023). Bununla birlikte Kamu kurumlarının veri yönetiminde şeffaflık ve hesap verebilirlik ilkelerine uyması, vatandaşların devlete duyduğu güveni artırır. Açık veri politikaları, kamu kaynaklarının nasıl kullanıldığını daha görünür hale getirebilir.

Kamu sektöründe etkili veri yönetimi, yalnızca yasal bir gereklilik değil, aynı zamanda vatandaşlara daha kaliteli hizmet sunmanın ve toplumun güvenini artırmanın bir yolu olarak görülmelidir. Veri yönetim süreçlerinin teknolojik altyapı, insan faktörü ve yasal düzenlemelerle desteklenmesi, kamu sektörünün dijitalleşme sürecindeki başarısını doğrudan etkileyen unsurlardır.

2.7. Kişisel Verilerin Korunması: Yasal Düzenlemeler ve Uygulamalar

Kişisel verilerin korunmasına yönelik yasal düzenlemeler, bireylerin haklarını güvence altına almak ve veri güvenliğini sağlamak amacıyla geliştirilmiştir. Bu düzenlemeler, ülkeden ülkeye değişiklik göstermekte olup, farklı yaklaşımlar içermektedir. Kamu sektöründe kişisel verilerin korunmasına ilişkin en önemli yasal düzenlemelerden ikisi Türkiye'deki Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği'nde uygulanan Genel Veri Koruma Tüzüğü (GDPR) olarak öne çıkmaktadır.

2.7.1. Türkiye'de Kişisel Verilerin Korunması Kanunu (KVKK)

Türkiye'de kişisel verilerin korunması, 24 Mart 2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu (KVKK) ile düzenlenmiştir. KVKK, bireylerin kişisel verileri

üzerindeki haklarını koruma altına almayı hedeflemektedir. Kanunda veri işleme süreçlerine dair şeffaflık, rıza ve hesap verebilirlik ilkeleri vurgulanmaktadır. Aynı zamanda, kamu kurumlarının veri güvenliği ve mahremiyetine ilişkin yükümlülükleri belirlenmektedir (Güdek, 2023).

KVKK'nın uygulamaları, kamu sektöründe veri işleme süreçlerinin düzenlenmesi açısından önemli bir rehber niteliği taşımaktadır. Bu doğrultuda, kamu kurumları KVKK'ya uyum sağlamak için gerekli adımları atmalı ve veri güvenliği politikalarını bu yasal çerçeveye göre geliştirmelidir.

KVKK'nın temel özellikleri şunlardır:

- **Kapsam:** KVKK, gerçek kişilere ait olan tüm kişisel verileri korumayı hedefler. Bu kapsamda, kişisel verilerin işlenmesi, saklanması ve aktarılmasıyla ilgili çeşitli düzenlemeler getirilmiştir.
- **Veri Sorumlusu Tanımı:** KVKK, kişisel verilerin işlenmesinden sorumlu olan gerçek veya tüzel kişileri "veri sorumlusu" olarak tanımlar. Veri sorumlusunun, kişisel verilerin korunması konusunda yükümlülükleri bulunmaktadır.
- **Veri İşleme İlkeleri:** Kanun, kişisel verilerin işlenmesinde uyması gereken ilkeleri belirler. Bu ilkeler arasında hukuka ve dürüstlük kurallarına uygunluk, belirli ve meşru amaçlar için işleme, veri minimizasyonu, doğruluk, güncellik ve saklama süreleri yer alır.
- **Veri Sahibinin Hakları:** KVKK, veri sahiplerine çeşitli haklar tanımaktadır. Bu haklar arasında kişisel verilere erişim hakkı, verilerin düzeltilmesi hakkı, silinme hakkı ve veri taşınabilirliği hakkı bulunmaktadır.

KVKK'nın olumlu özellikleri;

- **Bireylerin Mahremiyetinin Korunması:** KVKK, bireylerin kişisel verilerinin korunmasına dair yasal bir zemin oluşturur, bu da bireylerin mahremiyetini artırır.
- **Hukukun Üstünlüğü:** Kanun, kişisel veri ihlalleri durumunda uygulanabilir yaptırımlar öngörerek hukukun üstünlüğünü sağlar.

- **Uluslararası Standartlarla Uyum:** KVKK, Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği (GDPR) ile benzerlikler taşır. Bu da Türkiye'nin uluslararası alanda veri koruma standartlarına uyumunu kolaylaştırır.

KVKK'nın Hukuki Boşlukları:

- **Teknolojik Gelişmelere Uyum:** Teknolojik gelişmelerin hızına yetişemeyen düzenlemeler, KVKK'nın etkisini azaltmakta ve hukuki boşluklar yaratmaktadır.
- **Yetersiz Cezai Yaptırımlar:** KVKK, ihlaller için öngörülen cezaların yetersiz olması nedeniyle caydırıcılığı zayıflamaktadır. Özellikle büyük ölçekli veri ihlallerinde etkili yaptırımların olmaması, güvenlik açıklarını artırmaktadır.
- **Uygulama Zorlukları:** Kanunun uygulanmasında karşılaşılan zorluklar, özellikle veri güvenliği konusunda yetersiz denetim ve bilinç eksikliği gibi faktörler, hukuki boşlukların başında gelmektedir (Eltimur, 2022).
- **Özelleşmiş Düzenlemelerin Eksikliği:** Özellikle sektör bazında (örneğin sağlık, finans) özel düzenlemelerin yetersizliği, bazı alanlarda hukuki boşluklar yaratmaktadır.

2.7.2. Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

The General Data Protection Regulation (GDPR), Avrupa Birliği (AB) tarafından oluşturulan ve 25 Mayıs 2018'de yürürlüğe giren kapsamlı bir veri koruma yasasıdır. Bu yönetmelik, bireylerin kişisel verileri üzerindeki kontrolünü artırmayı ve uluslararası iş yapma ortamını basitleştirmeyi amaçlamaktadır.

GDPR, kişisel verilerin korunmasına yönelik en kapsamlı yasal düzenlemelerden biridir. GDPR, bireylerin kişisel verileri üzerindeki haklarını artırarak, veri işleyen kuruluşlara sıkı yükümlülükler getirmiştir. Bu düzenleme, veri ihlalleri durumunda yüksek cezalar uygulanması ve veri sahiplerine şeffaflık sağlanması gibi unsurları içermektedir. GDPR uygulamaları, dünya genelinde birçok ülkeye örnek teşkil etmektedir (Hoofnagle vd., 2019)

GDPR'nin birkaç temel özelliği ve avantajı şunlardır:

1. **Güçlendirilmiş Veri Koruma Hakları:** GDPR, bireylere kişisel verileriyle ilgili geliştirilmiş haklar sunar. Ana haklar arasında şunlar yer alır:
 - **Erişim Hakkı:** Bireyler, organizasyonlardan kişisel verilerinin işlenip işlenmediğine dair onay alma ve bu verilere erişme hakkına sahiptir (Madde 15).
 - **Silme Hakkı (Unutulma Hakkı):** Bireyler, kişisel verilerinin toplandığı amaçlar için artık gerekli olmadığı durumlarda silinmesini talep edebilirler (Madde 17).
 - **Veri Taşınabilirliği Hakkı:** Bireyler, kişisel verilerini yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilir bir formatta talep edebilir, bu da veri transferini kolaylaştırır (Madde 20).
2. **Hesap Verebilirlik ve Uyumluluk Yükümlülükleri:** Organizasyonlar, GDPR ilkelerine uyum sağladıklarını ve hesap verebilirliklerini göstermek zorundadırlar. Bu, veri minimizasyonu, amaç kısıtlaması ve saklama kısıtlaması gibi ilkelerin uygulanmasını gerektirir (Madde 5). Bu nedenle, kişisel verilerin korunması için uygun teknik ve organizasyonel önlemlerin alınması gerekmektedir.
3. **Veri Koruma Tasarımı ve Varsayılan Olarak Koruma:** GDPR, veri koruma önlemlerinin iş süreçleri ve sistemlerin geliştirilmesinde entegre edilmesini zorunlu kılar. Bu proaktif yaklaşım, gizliliğin baştan itibaren dikkate alınmasını sağlar (Madde 25).
4. **Uyumsuzluk İçin Artırılmış Cezalar:** GDPR, uyumsuzluk durumunda önemli cezalar öngörmektedir ki bu cezalar 20 milyon Euro'ya veya global yıllık cironun %4'üne kadar çıkabilmektedir; hangisi daha yüksekse o uygulanır (Madde 83). Bu, organizasyonları verilerin korunmasında öncelik vermesine teşvik eden güçlü bir motivasyondur.
5. **Tek Durdurma Mekanizması:** Birden fazla AB üye devletinde faaliyet gösteren organizasyonlar için GDPR, "tek durdurma" mekanizmasını tanıtır. Bu, şirketlerin sınır ötesi işleme faaliyetleri için tek bir denetleyici otoriteyle muhatap olmasını sağlayarak düzenleyici uyumu basitleştirir (Madde 56).

- 6. Artan Tüketici Güveni:** Verilerin korunmasına ve gizliliğine öncelik veren GDPR, organizasyonlara karşı tüketici güvenini artırır. Bireyler, verilerinin sorumlu bir şekilde yönetildiğini hissettiklerinde, işletmelerle ve hizmetlerle etkileşime geçmeye daha yatkın olurlar (URL-2).

GDPR, veri koruma mevzuatında önemli bir ilerlemeyi temsil etmektedir. Kapsamlı çerçevesi, bireylerin haklarını korumayı amaçlarken, organizasyonlar için net bir düzenleyici ortam sağlar. Sadece kişisel verilerin korunmasını artırmakla kalmaz, aynı zamanda dijital ekonomide hesap verebilirliği ve güveni teşvik eder (Voigt ve Von dem Bussche, 2017).

2.7.3. Uluslararası Diğer Yasal Düzenlemeler

Uluslararası veri güvenliği ve mahremiyeti konusunda birçok ülke, etkili yasalar ve düzenlemeler geliştirerek iyi uygulama örnekleri sergilemektedir. Bu örnekler, kamu sektöründeki veri koruma politikalarının geliştirilmesine katkıda bulunmaktadır. Kamu kurumları en iyi uygulamaları takip ederek veri güvenliği standartlarını yükseltebilir ve uluslararası düzeyde kabul görebilir. Uluslararası iş birlikleri, bilgi güvenliği konusundaki deneyimlerin paylaşılmasını sağlayarak, kamu sektöründeki veri güvenliğini güçlendirebilir.

Aşağıda, dünya genelinden bazı dikkat çekici örnekler ele alınmaktadır:

Güney Kore Kişisel Bilgi Koruma Yasası (PIPA)

Personal Information Protection Act (PIPA), 30 Eylül 2011 tarihinde yürürlüğe giren ve kişisel verilerin işlenmesine dair kapsamlı bir düzenleme getiren bir yasadır. PIPA, bireylerin kişisel verilerinin korunmasını sağlamayı ve bu verilerin işlenmesi sürecinde bireylerin haklarını güvence altına almayı amaçlamaktadır (Shahrullah vd., 2024).

PIPA'nın bazı temel özellikleri ve avantajları ise aşağıda özetlenmiştir;

- 1. Birey Haklarının Güçlendirilmesi:** PIPA, bireylere kişisel verileri üzerinde kapsamlı haklar sunar. Bu haklar arasında erişim, düzeltme, silme ve itiraz etme

hakları bulunmaktadır (Madde 35-37). Bu, bireylerin kendi verileri üzerindeki kontrolünü artırır ve şeffaflık sağlar.

2. **Veri Sorumlularının Yükümlülükleri:** PIPA, kişisel veri işleyen kuruluşlara önemli yükümlülükler getirir. Kuruluşlar, kişisel verileri yalnızca belirli ve meşru amaçlar için toplayabilir ve kullanabilir. Ayrıca, veri minimizasyonu ve verilerin güvenli bir şekilde korunması gibi ilkeleri uygulamak zorundadır (Madde 17).
3. **Veri İhlali Bildirimi:** PIPA, veri ihlalleri durumunda, veri sorumlusunun etkilenmiş bireyleri ve ilgili denetleyici otoriteyi bilgilendirme yükümlülüğünü getirir. Bu düzenleme, bireylerin olası zararları en aza indirmesine olanak tanır (Madde 34).
4. **Sektörel Düzenlemeler:** PIPA, belirli sektörlerde (örneğin, finans, sağlık) kişisel verilerin işlenmesine ilişkin özel düzenlemeler içerir. Bu, sektörel gereksinimlerin dikkate alınmasını ve güvenliğin artırılmasını sağlar (Madde 8).
5. **Hukuki Yaptırımlar:** PIPA, ihlallere karşı önemli yaptırımlar öngörmektedir. Veri ihlalleri durumunda, kuruluşlar para cezalarıyla karşı karşıya kalabilir ve bu cezalar, kuruluşların yıllık cirosuna bağlı olarak artış gösterebilir (Madde 75).
6. **Uluslararası İşlem Güvenceleri:** PIPA, kişisel verilerin yurtdışına aktarılmasıyla ilgili belirli kurallar içermektedir. Veri sorumluları, verilerin yeterli koruma düzeyine sahip bir ülkeye aktarılması gerektiğini bilmelidir. Bu, bireylerin verilerinin yurt dışında korunmasını sağlamak için önemlidir (Madde 23).
7. **Kişisel Bilgi Koruma Kurulu:** PIPA, kişisel verilerin korunmasını denetlemekle görevli bir otorite olan Kişisel Bilgi Koruma Kurulu'nu (Personal Information Protection Commission) kurmuştur. Bu kurul, yasaya uyumu denetlemek, bireylerin şikayetlerini değerlendirmek ve veri ihlallerine karşı önlemler almakla sorumludur (Madde 3) (URL-3).

PIPA, Güney Kore'deki kişisel veri koruma çerçevesini güçlendiren ve bireylerin haklarını korumaya yönelik kapsamlı bir yasadır. Bu yasa, bireylerin veri güvenliği konusunda daha

fazla koruma sağlamanın yanı sıra, işletmelere de veri işleme süreçlerini şeffaf ve hesap verebilir bir şekilde yürütme yükümlülüğü getirmektedir.

Singapur Kişisel Verilerin Korunması Yasası (PDPA)

Singapur'un 2012 yılında yürürlüğe giren PDPA, kişisel verilerin korunmasını sağlamak amacıyla oluşturulmuştur. PDPA, veri sahiplerine kendi verileri üzerinde daha fazla kontrol sağlamakta ve kuruluşlara veri güvenliği önlemleri alma yükümlülüğü getirmektedir. Singapur'un bu yasası, verilerin toplanması, kullanılması ve paylaşılması konusunda net kurallar belirleyerek bireylerin mahremiyetini korumaktadır.

Bazı temel özellikleri ise:

- **Veri Koruma Görevlisi (DPO):** Her kuruluşun, kişisel veri koruma süreçlerini yönetmek için bir veri koruma görevlisi ataması gerekmektedir.
- **Esnek Uyumluluk:** PDPA, küçük ve orta ölçekli işletmelerin (KOBİ) uyum süreçlerini kolaylaştıracak şekilde tasarlanmıştır.
- **Güvenlik Standartları:** Kişisel verilerin işlenmesi sırasında veri sızıntılarına karşı güçlü teknik ve idari önlemler alınmasını zorunlu kılar (URL-4).

Kanada Kişisel Bilgilerin Korunması ve Elektronik Belgeler Yasası (PIPEDA)

Kanada'nın PIPEDA'sı, ticari faaliyetlerde kişisel bilgilerin korunmasına yönelik önemli bir yasadır. PIPEDA, bireylerin kişisel bilgilerinin nasıl toplandığını, kullanıldığını ve saklandığını belirlemekte ve veri sahiplerine bu bilgiler üzerinde kontrol sağlamaktadır. Bu yasa, veri güvenliği ihlalleri durumunda kuruluşların nasıl hareket etmesi gerektiği konusunda açık kurallar sunmaktadır.

Bazı temel özellikleri;

- **Sektörler Arası Uygulama:** PIPEDA, hem kamu hem de özel sektör kuruluşlarında veri koruma standartları oluşturur.

- **Etkin Şikayet Mekanizması:** Veri ihlalleri durumunda bireylerin şikayetlerini hızlı bir şekilde ele alan bir sistem sunar.
- **Bilgi Doğruluğu:** Şirketlerin, topladıkları bilgilerin doğru, eksiksiz ve güncel olmasını sağlama yükümlülüğü vardır (URL-5).

Avustralya'nın Kişisel Verilerin Korunması Yasası

Avustralya'da 1988'de yürürlüğe giren Kişisel Verilerin Korunması Yasası, bireylerin kişisel verilerini koruma amacı taşımaktadır. Bu yasada, verilerin nasıl toplanması, kullanılması ve saklanması gerektiğine dair kurallar belirlenmiştir. Ayrıca, yasaya aykırı durumlarda cezai yaptırımlar da öngörülmektedir. Avustralya'nın veri koruma yasası, diğer ülkeler için iyi bir örnek oluşturmaktadır (Walters vd.,2019).

Öne Çıkan Özellikleri ise;

- **13 Gizlilik İlkesi:** Avustralya, kişisel bilgilerin toplanması, kullanılması ve saklanması için 13 temel gizlilik ilkesini (APPs) benimsemiştir. Bu 13 temel ilke; *“Bilgilendirme, Kullanım ve ifşa, Doğrudan pazarlama, Yurtdışına aktarım, Doğruluk, Güvenlik, Erişim, Düzeltme, Hassas bilgiler, Bilgilendirme, Kullanım ve ifşa, Doğrudan pazarlama, Yurtdışına aktarım, Doğruluk, Güvenlik, Erişim, Düzeltme, Hassas bilgiler”* ilkelerinden oluşmaktadır.
- **Veri İhlali Bildirimi:** Veri ihlalleri durumunda kuruluşların, Avustralya Bilgi Komisyonu'na (OAIC) rapor sunması zorunludur.
- **Açık Amaç İlkesi:** Toplanan veriler yalnızca belirli ve açık bir amaç için kullanılmalıdır (URL-6).

ABD'de HIPAA (Health Insurance Portability and Accountability Act)

ABD'de sağlık verilerinin korunmasına yönelik olarak 1996'da yürürlüğe giren HIPAA, sağlık hizmeti sağlayıcılarının hastaların kişisel sağlık bilgilerini korumasını zorunlu kılmaktadır. HIPAA, sağlık verilerinin gizliliğini sağlamak amacıyla bir dizi güvenlik önlemi ve yükümlülük getirmektedir. Bu düzenleme, sağlık sektörü için veri güvenliğini artıran önemli bir örnektir.

Öne çıkan bazı özellikleri;

- **Sağlık Verilerinin Korunması:** HIPAA, özellikle sağlık sektöründe çalışan kuruluşların hastaların tıbbi verilerini koruma yükümlülüğünü vurgular.
- **Güvenlik Standartları:** Elektronik Sağlık Kayıtları (EHR) gibi dijital sağlık verilerini korumak için teknik, idari ve fiziksel önlemler uygulanır.
- **Eğitim ve Farkındalık:** Sağlık çalışanlarına veri güvenliği konusunda sürekli eğitim verilmesi zorunludur (URL-7).

2.8. Dijitalleşmenin Kamu Sektöründeki Rolü

Dijitalleşme, kamu sektöründe veri güvenliği ve mahremiyeti üzerinde önemli bir etkiye sahiptir. Teknolojik gelişmeler, veri yönetimi süreçlerini kolaylaştırmakla birlikte yeni güvenlik risklerini de beraberinde getirmektedir. Kamu kurumları, dijitalleşmenin sunduğu fırsatları değerlendirirken, veri güvenliği ve mahremiyetine yönelik etkili stratejiler geliştirmek zorundadır (Eyüpgiller, 2023).

Dijitalleşme, kamu sektöründe hizmet sunumundan yönetim süreçlerine kadar birçok alanda köklü değişiklikler yaratmıştır. Bu süreç, yalnızca hizmetlerin daha hızlı ve etkili bir şekilde sunulmasını sağlamakla kalmaz, aynı zamanda veri güvenliği ve mahremiyeti konularında yeni zorluklar da ortaya çıkarır. Teknolojik gelişmelerin sağladığı bu dönüşüm, veri güvenliği ve mahremiyeti üzerinde önemli etkiler doğurmuştur. Dijitalleşmenin kamu sektörü üzerindeki rolü, daha etkin hizmet sunumu, maliyetlerin azaltılması ve vatandaş memnuniyetinin artırılması gibi olumlu etkiler yaratırken, aynı zamanda veri güvenliği ve mahremiyeti açısından yeni riskleri ve zorlukları da beraberinde getirmektedir. Bu bağlamda, kamu kurumları dijitalleşme sürecinde güvenlik risklerini yönetmek için proaktif yaklaşımlar benimsemelidir.

Dijitalleşmenin Kamu Hizmetlerine Katkıları;

1. **Hizmet Süreçlerinin Otomasyonu:** Dijitalleşme, kamu hizmetlerinin daha hızlı ve verimli bir şekilde sunulmasını sağlamaktadır. E-devlet sistemleri vatandaşların birçok hizmete çevrim içi erişimini kolaylaştırarak bürokratik süreçleri azaltmıştır.

Bu sistemler, kamu hizmetlerine erişimi hızlandırırken vatandaşların veri paylaşım süreçlerinde şeffaflık talebini artırmaktadır.

2. **Büyük Veri ve Analitik Kullanımı:** Kamu sektörü, büyük veri analitiği ile vatandaşların ihtiyaçlarını daha iyi anlayabilir ve daha etkili politikalar geliştirebilir. Sağlık sektöründe dijitalleşme hastalık trendlerini izlemek ve kaynak tahsisini optimize etmek için kullanılmaktadır (Altun, Şahin ve Öztaş, 2017). Ancak bu süreçlerde verilerin güvenliği ve anonimleştirilmesi önemli bir gereklilik olarak öne çıkmaktadır.
3. **Kaynak Yönetiminde Verimlilik:** Dijitalleşme sayesinde kamu kurumları, kaynak yönetimini daha etkin bir şekilde gerçekleştirebilmektedir. Enerji tüketiminin izlenmesi ve yönetilmesi, akıllı şehir projelerinde dijital teknolojilerin kullanımıyla daha etkili hale gelmiştir.

Dijitalleşmenin Veri Güvenliği ve Mahremiyetine Olumsuz Etkileri;

1. **Yeni Güvenlik Tehditleri:** Dijitalleşme, kamu sektöründe yeni güvenlik açıkları yaratmıştır. Özellikle siber saldırılar, kamu kurumlarının dijital altyapılarına yönelik en büyük tehditlerden biridir. 2020 yılında kamu kurumlarına yönelik DDoS saldırıları, birçok hizmetin geçici olarak durmasına neden olmuştur (Uslu, 2023).
2. **Karmaşık Veri Yönetimi:** Dijitalleşme ile birlikte toplanan veri miktarının artması, veri yönetimini daha karmaşık hale getirmiştir. Özellikle kamu sektöründe, verilerin anonimleştirilmesi ve veri işleme süreçlerinde şeffaflık sağlanması gerekmektedir.
3. **Güvenlik ve Mahremiyet Arasında Denge:** Dijitalleşme sürecinde kamu kurumları, vatandaşların verilerini korurken, hizmetlerin erişilebilirliğini ve kullanılabilirliğini sağlamak zorundadır. Bu denge hem teknik hem de yasal düzenlemelerle desteklenmelidir.

Kamu kurumlarının dijitalleşme sürecinde karşılaşılabilecekleri riskleri minimize etmek ve fırsatları en iyi şekilde değerlendirmek için hem teknolojik altyapılarını güçlendirmeleri hem de yasal ve etik çerçevede hareket etmeleri gerekmektedir. Bu süreçte proaktif yaklaşımlar yalnızca kurumların başarısını artırmakla kalmayacak aynı zamanda vatandaşların devlete olan güvenini de güçlendirecektir.

2.9. Kamu Sektöründe Veri Güvenliği ve Mahremiyeti

Kamu kurumları, topluma sundukları hizmetlerin yanı sıra bireylerin kişisel verilerini toplamak, saklamak ve işlemek zorundadır. Bu sebeple veri güvenliği, kamu kurumlarının en önemli sorumluluklarından birini oluşturmaktadır. Veri güvenliği, hem bireylerin mahremiyetinin korunması hem de kamu güvenliğinin sağlanması açısından kritik bir öneme sahiptir. Özellikle devletin sağladığı hizmetlerin kalitesi ve güvenilirliği, veri güvenliği uygulamalarının etkinliği ile doğrudan ilişkilidir.

Kamu kurumları, vatandaşların kişisel verilerini koruma yükümlülüğü altındadır ve bu verilerin kötüye kullanılmasını önlemek için çeşitli güvenlik önlemleri almak zorundadır. Veri güvenliğinin sağlanması, kamu kurumlarının itibarını ve güvenilirliğini artırmakta, dolayısıyla vatandaşların devlete olan güvenini pekiştirmektedir. Ancak veri güvenliği yalnızca teknolojik önlemlerle sağlanamaz; aynı zamanda insan faktörü ve organizasyonel yapıların da dikkate alınması gerekmektedir. Çalışanların veri güvenliği politikalarını anlaması ve bu politikaları uygulamada etkin bir şekilde yer alması, veri güvenliğini sağlamak adına kritik öneme sahiptir.

Kamu kurumlarının veri güvenliği stratejileri, genellikle çok katmanlı bir yaklaşım gerektirir. Bu stratejiler arasında veri şifreleme, erişim kontrol sistemleri, düzenli güvenlik denetimleri ve çalışan eğitim programları bulunmaktadır. Veri şifreleme, verilerin yetkisiz erişimlere karşı korunmasına yardımcı olurken, erişim kontrol sistemleri, yalnızca yetkili kişilerin verilere ulaşmasını sağlamaktadır. Ayrıca çalışan eğitim programları, insan hatalarından kaynaklanan veri ihlallerini en aza indirmek için gereklidir. Tüm bu önlemler, kamu kurumlarının veri güvenliğini sağlamada önemli bir rol oynamaktadır.

Kamu kurumlarında veri güvenliğinin önemi, yalnızca bireylerin mahremiyetinin korunmasıyla sınırlı kalmayıp, aynı zamanda kamu güvenliğinin sağlanması ve devletin

itibarının korunması açısından da kritik bir unsur teşkil etmektedir. Bu nedenle, veri güvenliği politikalarının etkin bir şekilde uygulanması kamu kurumlarının en öncelikli hedeflerinden biri olmalıdır.

2.10. Kamu Sektöründe Veri Güvenliği Sorunları

Kamu sektöründe veri güvenliği ile ilgili birçok sorun bulunmaktadır. Bu sorunlar genellikle iç ve dış tehditlerden kaynaklanmaktadır. İç tehditler, çalışanlar veya sisteme yetkili erişimi olan kişiler tarafından gerçekleştirilen veri ihlalleri olarak tanımlanırken, dış tehditler siber saldırılar gibi dış kaynaklı tehditleri kapsamaktadır. Her iki tehdit türü de kamu kurumlarının veri güvenliğini ciddi şekilde tehlikeye atmaktadır (Ener ve Demircan, 2008).

2.10.1. İç Tehditler

İç tehditler, kamu kurumlarında veri güvenliği sorunlarının önemli bir kısmını oluşturmaktadır. Çalışanların kötü niyetli davranışları veya iş süreçleri sırasında yapılan hatalar, veri sızıntısına yol açabilir. Araştırmalar iç tehditlerin, özellikle kamu sektöründe dış tehditlerden daha fazla veri ihlaline neden olduğunu göstermektedir (Akmeşe, 2020). Bir çalışan yanlışlıkla kritik verilere erişim izni olmayan bir kişiye veri gönderebilir veya güvenlik protokollerini ihlal edebilir.

Bu nedenle, iç tehditlerin önlenmesi için kamu kurumlarının çalışanlarına düzenli olarak veri güvenliği eğitimi vermeleri gerekmektedir. Çalışanların veri güvenliği politikalarını ve prosedürlerini anlamaları, iç tehditlerin etkisini azaltmada önemli bir rol oynamaktadır. Ayrıca, kurum içindeki güvenlik kültürünü güçlendirmek çalışanların veri güvenliği konusundaki sorumluluklarını daha iyi anlamalarına yardımcı olabilir.

2.10.2. Dış Tehditler

Dış tehditler, siber saldırılar veya diğer dış kaynaklı tehditler aracılığıyla verilerin ele geçirilmesini ifade eder. Kamu kurumları, siber suçluların hedefi haline gelmekte ve bu durum büyük veri ihlallerine sebep olmaktadır. Devlet kurumlarına yönelik siber saldırılar, ulusal güvenlik açısından ciddi riskler oluşturabilmektedir. Dış tehditler, genellikle kötü

niyetli yazılımlar, phishing saldırıları ve sosyal mühendislik teknikleri gibi yöntemlerle gerçekleştirilmektedir.

Kamu kurumları, genellikle büyük miktarda hassas veri işlemekte ve bu durum onları siber saldırılara karşı daha savunmasız hale getirmektedir. Özellikle sağlık, mali ve kimlik bilgileri gibi kişisel verilerin ele geçirilmesi, bireylerin mahremiyetine ciddi zararlar verebilir. Siber saldırılar sonucunda ortaya çıkan veri ihlalleri yalnızca bireylerin gizliliğini tehdit etmekle kalmaz, aynı zamanda kamu kurumlarının itibarını da zedeleyebilir. 2017 yılında yaşanan WannaCry ransomware saldırısı, dünya genelinde birçok kamu kurumunu etkileyerek, kritik verilerin kaybına ve hizmetlerin aksamasına neden olmuştur (Solmaz, 2023).

Dış tehditlerle başa çıkmak için Kamu kurumlarının siber güvenlik stratejilerini güçlendirmeleri gerekmektedir. Bu stratejiler ağ güvenliği, veri şifreleme, sürekli izleme ve siber olay müdahale planlarını içermelidir. Ayrıca kamu kurumları, güncel siber güvenlik tehditlerini takip etmeli ve bu tehditlere karşı proaktif bir yaklaşım benimsemelidir. Çalışanların, dış tehditlere karşı farkındalığını artırmak amacıyla düzenli eğitimler verilmesi de büyük önem taşımaktadır.

Kamu sektöründe veri güvenliği sorunları, iç ve dış tehditler arasında bir denge gözetilerek ele alınmalıdır. İç tehditlerin önlenmesi için çalışanların eğitilmesi ve güvenlik kültürünün geliştirilmesi, dış tehditlerle başa çıkmak içinse siber güvenlik stratejilerinin güçlendirilmesi gerekmektedir.

2.10.3. Veri Mahremiyeti İhlalleri ve Sonuçları

Veri mahremiyeti ihlalleri, günümüz bilgi toplumunda bireyler ve kurumlar için ciddi bir tehdit oluşturmaktadır. Bu ihlaller, yalnızca bireylerin temel hak ve özgürlüklerini ihlal etmekle kalmaz, aynı zamanda kamu kurumlarının itibarını zedeleyerek kamu güvenini sarsar.

Veri mahremiyeti ihlali, kişisel verilerin yetkisiz erişim, ifşa, değiştirme veya imha edilmesi gibi çeşitli şekillerde gerçekleşebilir. Bu ihlallerin sonuçları, ihlalin kapsamı, etkilenen veri türü ve alınan önlemlere bağlı olarak değişebilir.

2.10.3.1. Kişisel Veri İhlallerinin Bireyler Üzerindeki Etkileri

Kişisel verilerin ihlali, bireyler üzerinde yıkıcı sonuçlar doğurabilir. Özellikle sağlık, mali ve kimlik bilgileri gibi hassas verilerin ele geçirilmesi, bireylerin mahremiyetini ihlal etmekle kalmaz, aynı zamanda onları ayrımcılık, manipülasyon ve hatta fiziksel tehditlere karşı savunmasız hale getirebilir.

Sağlık verilerinin ele geçirilmesi, bireylerin sağlık sigortası primlerinin artmasına, iş başvurularının reddedilmesine veya sosyal damgalanmaya maruz kalmasına yol açabilir (Stangl vd., 2019). Benzer şekilde, finansal verilerin çalınması, kimlik hırsızlığına, mali kayıplara ve uzun süreli ekonomik zorluklara neden olabilir.

Kişisel veri ihlallerinin bireyler üzerindeki etkileri sadece maddi kayıplarla sınırlı değildir. Bu ihlaller, aynı zamanda bireylerin güvenlik, kontrol ve özerklik duygularını derinden etkileyerek psikolojik sıkıntıya, güven kaybına ve sosyal izolasyona yol açabilir.

2.10.3.2. Veri İhlallerinin Kurum İmajı ve Güvenilirliği Üzerindeki Etkiler

Veri mahremiyeti ihlalleri, kamu kurumlarının itibarını ve güvenilirliğini ciddi şekilde zedeleyebilir. Bir veri ihlali olayı, kamuoyunda kurumun yetersiz güvenlik önlemleri aldığı, vatandaşlarının mahremiyetini koruyamadığı ve şeffaflık ilkesine bağlı kalmadığı algısını yaratabilir.

Bu durum, özellikle halkın güvenine dayalı hizmetler sunan kamu kurumları için son derece zararlı olabilir. Sağlık, eğitim veya sosyal hizmetler gibi alanlarda faaliyet gösteren kamu kurumları, bir veri ihlali sonrasında vatandaşların güvenini kaybetmesi durumunda hizmet sunma kapasitelerini ciddi şekilde sekteye uğratabilir.

Araştırmalar, bir veri ihlali sonrasında kamu kurumlarının halkla ilişkiler çabalarıyla itibar kaybını telafi etmesinin zor olduğunu göstermektedir (Kuipers ve Schonheit, 2022). Bu nedenle, kamu kurumlarının veri ihlallerini önlemek için proaktif önlemler alması ve veri güvenliği kültürünü kurumsal yapılarının ayrılmaz bir parçası haline getirmesi hayati önem taşımaktadır.

2.11. Siber Saldırıları ve Kamu Sektörü

Siber saldırılar, kamu sektöründe veri güvenliği açısından en büyük tehditlerden birini oluşturmaktadır. Bu tür saldırılar, devletin kritik altyapılarına, hizmetlerine ve veri tabanlarına yönelik gerçekleştirilen kötü niyetli eylemleri ifade eder. Siber saldırılar, yalnızca verilerin kaybına veya ihlaline yol açmakla kalmayıp, aynı zamanda kamu güvenliğini tehdit eden durumlar da yaratabilir.

2.11.1. Kamu Kuruluşlarına Yönelik Yaygın Siber Tehditler

Kamu kuruluşlarına yönelik yaygın siber tehditler arasında kötü amaçlı yazılımlar, phishing saldırıları ve DDoS (Dağıtılmış Hizmet Reddi) saldırıları yer almaktadır. Kötü amaçlı yazılımlar, sistemleri etkisiz hale getirerek verilerin ele geçirilmesine veya silinmesine neden olabilir. Phishing saldırıları, kullanıcıların kimlik bilgilerini çalmayı amaçlayan sosyal mühendislik teknikleridir ki bu tür saldırılar, kullanıcı dikkatsizliği nedeniyle sıklıkla başarıya ulaşmaktadır (Alkhalil vd., 2021). DDoS saldırıları ise, bir hedefe aşırı miktarda trafik göndererek hizmetin aksıyormuş gibi görünmesine neden olur ve bu kamu hizmetlerinin sürekliliğini tehdit eder. Bu tür siber tehditler, kamu sektöründeki veri güvenliğini ciddi şekilde tehdit etmekte ve devletin kritik hizmetlerinin kesintiye uğramasına yol açabilmektedir (Shaar ve Efe, 2018). Özellikle sağlık hizmetleri, ulaşım sistemleri ve enerji altyapıları gibi kritik alanlar, siber saldırılara karşı daha savunmasızdır.

2.11.2. Kamu Sektörüne Yönelik Saldırılarda Siber Savunma Stratejileri

Kamu kurumları, siber saldırılara karşı etkili savunma stratejileri geliştirmek zorundadır. Bu stratejiler, öncelikle siber güvenlik altyapısının güçlendirilmesine odaklanmalıdır. Güçlü bir siber güvenlik altyapısı, ağ güvenliği sistemleri, veri şifreleme, sürekli izleme ve güncel yazılım kullanımı gibi unsurları içermelidir. Ayrıca, siber güvenlik farkındalığını artırmak amacıyla çalışanlara düzenli eğitim programları sunmak büyük önem taşımaktadır. Çalışanların siber tehditlere karşı bilinçlendirilmesi, potansiyel ihlallerin önlenmesine yardımcı olabilir (Çakır ve Yaşar, 2015).

Kamu kurumları, siber olay müdahale planları geliştirerek, bir saldırı durumunda hızlı ve etkili bir şekilde tepki verebilmelidir. Bu tür planlar, olası bir siber saldırının etkilerini

azaltmaya ve kurtarma sürecini hızlandırmaya yardımcı olur. Ayrıca kamu kurumları diğer kamu kurumları ve özel sektörle iş birliği yaparak, siber güvenlik alanında bilgi paylaşımını teşvik etmelidir. Bu tür iş birlikleri, siber tehditlerin daha iyi anlaşılmasına ve siber saldırılara karşı kolektif bir savunma mekanizması oluşturulmasına katkı sağlar.

Siber saldırılar kamu sektörü için ciddi bir tehdit oluşturmaktadır. Kamu kurumlarının, bu tehditlere karşı etkili bir savunma mekanizması geliştirmesi hem verilerin güvenliğini sağlamak hem de kamu hizmetlerinin sürekliliğini korumak açısından kritik öneme sahiptir. Güçlü bir siber güvenlik altyapısı, eğitim programları ve iş birlikleri, siber saldırılara karşı dayanıklılığı artıracak unsurlar arasında yer almaktadır.

2.12. Kamu Sektöründe Veri Güvenliği Politikaları ve Uygulamaları

Kamu sektöründe veri güvenliği, bireylerin mahremiyetinin korunmasının yanı sıra kamu güvenliğinin sağlanmasını da kapsamaktadır. Bu nedenle, kamu kurumları, veri güvenliğini sağlamak amacıyla etkili politikalar ve uygulamalar geliştirmek zorundadır. Bu politikalar, veri güvenliğini artırmak ve kamu hizmetlerinin sürdürülebilirliğini sağlamak için gereklidir.

2.12.1. Mevcut Politikalar ve Stratejiler

Kamu kurumları, veri güvenliği politikalarını oluştururken ulusal ve uluslararası yasal düzenlemeleri göz önünde bulundurmalıdır. Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR), veri güvenliği politikalarında dikkate alınması gereken önemli bir çerçeve sunmaktadır. Bu tür yasal düzenlemeler, bireylerin veri haklarını korumayı amaçlamakta ve kamu kurumlarının veri işleme süreçlerini düzenlemektedir.

Kamu kurumları, veri güvenliği politikalarını geliştirirken risk analizi yapmalı ve potansiyel tehditleri belirlemelidir. Bu analizleri hangi verilerin korunması gerektiğini, hangi güvenlik önlemlerinin alınması gerektiğini ve olası ihlallerin nasıl önlenilebileceğini belirlemede yardımcı olacaktır. Ayrıca, teknoloji ve inovasyonun hızla geliştiği günümüzde, kamu kurumları sürekli güncellenen bir yaklaşım benimsemelidir (Cooke vd., 2024).

Veri güvenliği uygulamaları genellikle çok katmanlı bir stratejiyi içermektedir. Bu stratejiler arasında veri şifreleme, erişim kontrol sistemleri, düzenli güvenlik denetimleri ve çalışan eğitim programları yer almaktadır. Ayrıca, veri kaybını önlemek için yedekleme çözümleri de kritik öneme sahiptir; bu sistemler, verilerin kaybı durumunda hızlı bir şekilde geri yüklenmesine olanak tanır.

Kamu sektöründe veri güvenliği politikaları ve uygulamaları, bireylerin mahremiyetini korumak ve kamu güvenliğini sağlamak açısından büyük önem taşımaktadır. Kamu kurumlarının etkili ve güncel veri güvenliği politikaları geliştirmesi, yalnızca yasal uyumluluk açısından değil, aynı zamanda halkın güvenini kazanmak bakımından da kritik bir unsurdur.

2.13. Veri Güvenliği ve Mahremiyetine Yol Açan Sorunlar

Kamu sektöründe veri güvenliği ve mahremiyetine yol açan sorunların başlıcaları aşağıdaki başlıklarda ele alınmıştır.

2.13.1. Teknolojik Altyapının Yetersizliği

Kamu sektöründe veri güvenliği ve mahremiyeti sorunlarının başında teknolojik altyapının yetersizliği gelmektedir. Birçok kamu kurumu güncel teknolojinin gerisinde kalan sistemler kullanmakta ve bu sistemler günümüzün siber tehditlerine karşı savunmasız durumdadır. Eski yazılımlar, geliştirici desteğini kaybetmiş olabileceğinden güvenlik güncellemeleri alamaz ve bu da güvenlik açıkları oluşturur.

Ayrıca, veri yedekleme ve kurtarma süreçleri genellikle yetersiz kalmaktadır. Birçok kamu kurumu, veri kaybı durumlarında etkili yedekleme ve kurtarma stratejileri geliştirmemiştir. Veri kaybı, yalnızca finansal kayıplara neden olmakla kalmayıp aynı zamanda kamu güvenini de sarsar. Araştırmalara göre, etkili bir veri yedekleme stratejisi eksikliği, veri kaybı riskini önemli ölçüde artırmaktadır (Çelik, 2023). Kamu kurumları, veri kaybı yaşandığında geri dönüşü sağlamanın yanı sıra, veri bütünlüğünü de korumak zorundadır.

Kamu sektöründeki teknolojik altyapının yetersizliği, veri güvenliği ve mahremiyeti açısından ciddi sorunlar yaratmaktadır. Eski sistemlerin güncellenmesi ve veri yedekleme süreçlerinin iyileştirilmesi, bu sorunların çözümüne yönelik atılacak önemli adımlardır.

2.13.1.1. Eski Sistemler ve Güvenlik Açıkları

Birçok kamu kurumu finansal kaynaklar ve bütçe kısıtlamaları nedeniyle eski sistemler kullanmaya devam etmektedir. Eski yazılımlar ve donanımlar, güvenlik güncellemeleri ve yamaları alamaz ki bu da siber saldırganlar için önemli bir açık yaratır. Bu tür eski sistemlerin siber tehditlere karşı savunmasız kalması kamu kurumlarının güvenlik risklerini artırmaktadır.

Kamu sektöründeki birçok kurum, eski teknolojilere dayalı sistemler kullanmaktadır. Bu sistemler, zamanla güncellenmemiş ve modern siber güvenlik standartlarını karşılamaktan uzak kalmıştır. Eski yazılımlar, güncel güvenlik açıkları ve tehditlere karşı savunmasız hale gelir. Siber suçlular, bu zayıflıkları hedef alarak sistemlere sızabilir ve hassas verilere erişebilir. 2017’de gerçekleşen WannaCry fidye yazılımı saldırısı, eski işletim sistemlerine sahip kurumları ciddi şekilde etkileyerek birçok kamu kurumunun veri kaybı yaşamasına neden olmuştur (Minnaar ve Herbig, 2021). Bu tür olaylar, eski sistemlerin güvenlik açığını açıkça göstermektedir.

Eski sistemlerin yanı sıra yazılım güncellemelerinin yapılmaması da önemli bir sorundur. Yazılım güncellemeleri, güvenlik yamaları ve yeni özellikler içermekte olup sistemin güvenliğini artırmaktadır. Ancak birçok kamu kurumu, bütçe kısıtlamaları veya teknik yetersizlikler nedeniyle bu güncellemeleri ihmal etmektedir. Bunun sonucunda, sistemler güncel tehditlere karşı savunmasız kalmaktadır.

Ayrıca eski sistemlerin entegrasyonu ve veri yönetimi sorunları da yaşanabilmektedir. Farklı sistemlerin bir arada çalışması, veri bütünlüğünü bozabilir ve güvenlik açıklarını artırabilir. Kamu kurumlarının, eski sistemleri modernize etmesi ve siber tehditlere karşı daha dayanıklı hale getirmesi gerekmektedir.

2.13.1.2. Veri Yedekleme ve Kurtarma Eksiklikleri

Kamu kurumlarında veri kaybı durumunda etkili bir kurtarma planının eksik olması ciddi sorunlara yol açabilir. Bu tür eksiklikler, sistem arızaları veya siber saldırılar sonrasında verilerin kurtarılamamasıyla sonuçlanabilir. 2020 yılında bir kamu hastanesine yapılan siber saldırı sonrası, yedekleme sistemi düzgün çalışmadığı için hastane verilerini kaybetmiş ve

ciddi hizmet aksaklıkları yaşanmıştır. Bu tür durumlar, kamu hizmetlerinin aksamasına ve vatandaşların güvenliğinin tehlikeye girmesine neden olabilir.

Veri yedekleme ve kurtarma süreçleri, veri güvenliğinin kritik bir parçasıdır. Ancak, birçok kamu kurumu, bu süreçleri yeterince etkin bir şekilde uygulamamaktadır. Yedekleme stratejilerinin eksikliği, veri kaybı durumunda geri dönüşü imkansız hale getirebilir. Özellikle siber saldırılar, doğal afetler veya teknik arızalar gibi durumlarda etkili bir veri kurtarma planının olmaması kurumun iş sürekliliğini tehlikeye atar (Wallace ve Webber, 2017).

Veri yedekleme süreçlerinin yetersizliği genellikle yedekleme sıklığı, yedekleme yöntemleri ve veri bütünlüğünün sağlanması konularındaki eksikliklerden kaynaklanmaktadır. Bazı kurumlar, yedeklemeleri yalnızca belirli aralıklarla yapmaktadır, ki bu durum veri kaybı riskini artırmaktadır. Ayrıca, yedekleme verilerinin güvenli bir şekilde saklanmaması, bu verilerin de saldırılara maruz kalmasına neden olabilir.

Veri kurtarma süreçleri de çoğu zaman belirli bir plan çerçevesinde yürütülmemektedir. Bu, geri dönüş sürecinin karmaşıklaşmasına ve zaman kaybına yol açabilir. Kamu kurumları, etkili bir yedekleme ve kurtarma planı geliştirerek, veri kaybı durumunda hızlı ve etkili bir şekilde geri dönebilmelidir. Ayrıca, bu süreçlerin düzenli olarak test edilmesi, olası sorunların önceden tespit edilmesine yardımcı olacaktır.

2.13.2. Kamu Çalışanlarının Farkındalık ve Eğitim Eksikliği

Veri güvenliği, yalnızca teknolojik önlemlerle sağlanamaz, aynı zamanda çalışanların bilgi güvenliği konusunda eğitilmesi gerekmektedir. Kamu çalışanlarının veri güvenliği ve mahremiyeti konusundaki düşük farkındalıkları, veri ihlalleri ve güvenlik açıklarının başlıca nedenlerinden biridir.

Kamu sektöründe veri güvenliği ve mahremiyeti konusundaki en büyük zorluklardan biri, kamu çalışanlarının bu konudaki farkındalık ve eğitim eksikliğidir. Çoğu zaman, çalışanlar veri güvenliği protokollerine uymak için gerekli bilgi ve becerilere sahip değildir. Eğitim programlarının yetersizliği, çalışanların güvenlik ihlallerine karşı savunmasız kalmalarına

neden olmaktadır. Üstelik, birçok kamu kurumu veri güvenliği eğitimlerini sık sık güncellemiyor ya da çalışanların katılımını teşvik etmemektedir.

Eğitim programları, yalnızca temel güvenlik bilgilerini sunmakla kalmamalı, aynı zamanda çalışanların mevcut tehditler hakkında bilgi sahibi olmalarını sağlamalıdır. Özellikle siber saldırıların artmasıyla birlikte, çalışanların bu tür tehditlere karşı nasıl bir tutum sergilemeleri gerektiği konusunda bilgi sahibi olmaları önem kazanmaktadır. Yapılan çalışmalar, düzenli olarak güncellenen ve uygulamalı eğitim programlarına katılan çalışanların, güvenlik protokollerine uyum oranlarının önemli ölçüde arttığını göstermektedir (Aksoy ve Özkan, 2023).

Ayrıca, güvenlik protokollerinin uygulanması konusunda çalışanların motivasyonunu artırmak için kurum içi güvenlik kültürünün oluşturulması gerekmektedir. Çalışanların veri güvenliği konusunu yalnızca bir görev olarak değil, aynı zamanda bir sorumluluk olarak görmeleri sağlanmalıdır. Bu nedenle liderlik desteği ve kurum içindeki iletişim kanallarının etkin kullanımı, güvenlik bilincinin artırılmasında önemli bir rol oynamaktadır.

Kamu çalışanlarının veri güvenliği konusundaki farkındalık ve eğitim eksikliği ciddi bir sorun teşkil etmektedir. Eğitim programlarının güçlendirilmesi ve güvenlik kültürünün oluşturulması, bu sorunun çözümünde kritik bir rol oynamaktadır. Kamu kurumları, çalışanların güvenlik protokollerine uyumlarını artırmak için daha etkili eğitim stratejileri geliştirmeli ve bu eğitimleri sürekli hale getirmelidir.

Eğitim programlarının etkili olması için, çalışanların farklı öğrenme stillerine hitap eden çeşitli yöntemler kullanılabilir. Çevrimiçi eğitim modülleri, atölye çalışmaları ve simülasyonlar gibi farklı eğitim yöntemleri, çalışanların katılımını artırabilir. Ayrıca, güvenlik konusundaki güncel gelişmelerin paylaşılması ve çalışanların bu konudaki bilgi seviyelerinin düzenli olarak değerlendirilmesi, farkındalığın artırılmasına katkı sağlayacaktır.

Kamu sektöründe veri güvenliği ve mahremiyetinin sağlanması için, kamu çalışanlarının eğitimine ve farkındalığına gereken önemin verilmesi hayati bir gereklilik olarak karşımıza çıkmaktadır. Bu alandaki eksikliklerin giderilmesi, yalnızca güvenlik ihlallerinin önlenmesine değil aynı zamanda kamu güveninin artırılmasına da katkı sağlayacaktır.

2.13.2.1. Eğitim Programlarının Yetersizliği

Kamu kurumlarında veri güvenliği eğitimleri genellikle yetersiz kalmaktadır. Çalışanlar, yeni güvenlik tehditlerine karşı doğru önlemleri alabilmek için gerekli eğitimleri alamayabilirler. Eğitimlerin düzenli olarak güncellenmemesi, çalışanların sürekli değişen siber tehditler hakkında bilgi sahibi olmamalarına yol açmaktadır. 2018 yılında ABD’deki bir kamu sağlık kurumunda gerçekleşen veri ihlali, çalışanların phishing saldırıları konusunda eğitim almadıkları için meydana gelmiştir. Bu durum, eğitim eksikliklerinin veri güvenliği üzerindeki olumsuz etkilerini açıkça göstermektedir (Çakır ve Taşer, 2023).

Kamu sektöründeki çalışanların veri güvenliği konusundaki bilgi ve farkındalığı, kurumların genel güvenlik duruşunu doğrudan etkilemektedir. Ancak birçok kamu kuruluşunda uygulanan veri güvenliği eğitim programları yetersizdir. Çalışanlar, siber tehditler ve veri güvenliği protokolleri hakkında yeterli bilgiye sahip olmadıklarında, bu durum veri ihlalleri için büyük bir risk oluşturmaktadır.

Eğitim programlarının etkinliği, çalışanların bu programlara katılımı ve uygulama aşamasında gösterdikleri başarı ile doğrudan ilişkilidir. Eğitimler, teorik bilgilerin yanı sıra pratik uygulamalarla desteklenmeli ve çalışanların gerçek hayatta karşılaştıkları senaryolar üzerinde çalışmalar yapmaları sağlanmalıdır.

2.13.2.2. Çalışanların Güvenlik Protokollerine Uyumu

Kamu çalışanlarının güvenlik protokollerine uyumsuzluğu, veri güvenliği ihlallerine yol açan önemli bir sorundur. Çalışanların şifre güvenliğine dikkat etmemesi, kişisel cihazları kurumsal verilerle kullanması veya güvenli olmayan ağlar üzerinden veri iletmesi gibi durumlar yaygın hatalar arasındadır.

Kamu sektöründe çalışanların güvenlik protokollerine uyumu, veri güvenliğinin sağlanmasında kritik bir rol oynamaktadır. Güvenlik protokollerinin etkili bir şekilde uygulanabilmesi için, çalışanların bu kurallara olan bağlılıklarının artırılması gerekmektedir. Ancak eğitim eksiklikleri ve farkındalık yetersizlikleri nedeniyle birçok çalışan, güvenlik protokollerini göz ardı etme eğilimindedir. Bu durum, veri ihlalleri ve siber saldırılara zemin hazırlamaktadır.

Çalışanların güvenlik protokollerine uyumunu artırmak amacıyla, organizasyonel bir kültür oluşturulması önemlidir. Bu kültür, güvenliği önceliklendiren bir yaklaşımı benimsemeli ve çalışanların katkılarını teşvik etmelidir. Ayrıca güvenlik ihlalleri ile sonuçlanan durumların, çalışanlara açıklanması ve sonuçlarının paylaşılması, benzer hataların tekrarlanmaması adına önemli bir öğrenme fırsatı sunmaktadır. Çalışanların veri güvenliği konusunda sorumluluk almaları teşvik edilmeli ve bu süreçte ödüllendirme mekanizmaları devreye sokulmalıdır. Güvenlik protokollerine uyum gösteren çalışanlara tanınan ödüller veya takdir belgeleri, motivasyonlarını artırabilir (Dayıoğlu, 2016).

Üst düzey yönetimin güvenlik protokollerine olan bağlılığı, tüm çalışanların bu kurallara uyum göstermesi açısından kritik bir unsur olarak öne çıkmaktadır. Yönetim, güvenlik kültürünü destekleyici bir yaklaşım sergilediğinde, bu tutum çalışanlar arasında da benimsenmektedir. Bu nedenle, yönetim takımları, veri güvenliğini önceliklendiren stratejilerin oluşturulmasında ve uygulanmasında aktif bir rol almalıdır.

2.13.3. Yasal Boşluklar ve Düzenleme Eksiklikleri

Kamu sektöründe veri güvenliği ve mahremiyeti konusunda karşılaşılan sorunlardan biri yasal boşluklar ve düzenleme eksiklikleridir. Veri koruma yasalarının ve düzenlemelerinin yetersizliği, kamu kurumlarının veri güvenliği uygulamalarını olumsuz etkilemektedir. Birçok ülke, veri koruma konusunda belirli yasalar oluşturmuş olsa da bu yasaların kapsamı genellikle yetersiz kalmakta ve güncel siber tehditlerle başa çıkmakta zorlanmaktadır (Aydoğdu, 2021).

Yasal düzenlemelerde eksik kalan alanlar, kamu kurumlarının veri güvenliği stratejilerini zayıflatmaktadır. Özellikle veri ihlali durumunda uygulanacak yaptırımların belirsizliği, kurumların güvenlik önlemlerini ciddiye almamalarına yol açmaktadır. Araştırmalar, yasal yaptırımların etkin bir şekilde uygulanmadığı durumlarda kurumların veri güvenliği önlemlerini artırma konusunda isteksiz olduklarını göstermektedir (Voss ve Bouthinon-Dumas, 2021). Veri ihlali sonrasında yasal yaptırımların etkili olabilmesi için yasaların güncellenmesi ve yaptırımların belirgin hale getirilmesi gerekmektedir. Kamu kurumları, veri güvenliği ihlallerinin sonuçlarını ve bu sonuçların ciddiyetini anlamalıdır. Ayrıca, yasal boşlukların giderilmesi için düzenleyici kurumların iş birliği yaparak kapsamlı ve etkili düzenlemeler geliştirmesi önem taşımaktadır.

Kamu sektöründeki yasal boşluklar ve düzenleme eksiklikleri, veri güvenliği ve mahremiyeti konusunda ciddi sorunlar yaratmaktadır. Yasal çerçevenin güçlendirilmesi ve düzenleyici kurumların etkinliği bu sorunların çözümünde önemli bir rol oynamaktadır.

2.13.3.1. Yasal Düzenlemelerde Eksik Kalan Alanlar

Birçok kamu kurumunda, veri güvenliği ve mahremiyetine ilişkin yasal düzenlemeler hala eski kalmaktadır. Dijitalleşmenin hızla arttığı günümüzde, yasal çerçeveler yeni tehditlere karşı yetersiz kalmaktadır. Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği (GDPR) düzenlemesi, bu alanda önemli bir adım olsa da, tüm ülkeler ve kamu kurumları için geçerli olabilecek evrensel düzenlemeler hala eksiktir. Ayrıca bazı kamu kurumları, GDPR veya KVKK gibi yasal düzenlemelerle uyum sağlama konusunda eksiklikler yaşayabilmektedir. Bu eksiklikler, yasal boşluklardan, finansal kaynak eksikliklerinden veya personel eğitimi yetersizliklerinden kaynaklanabilmektedir.

Veri güvenliği ve mahremiyeti konusunda yeterli yasal düzenlemelerin olmaması, kamu sektöründeki en büyük sorunlardan biridir. Birçok ülkede veri koruma yasaları hâlâ gelişim aşamasındadır ve bu durum, kamu kurumlarının veri güvenliğini sağlama çabalarını olumsuz etkilemektedir. Mevzuattaki eksiklikler, özellikle yeni teknolojilerin ve siber tehditlerin hızla geliştiği bir ortamda, kurumların kendilerini koruma altına almalarını zorlaştırmaktadır. Avrupa Birliği'nin GDPR gibi düzenlemeleri, veri koruma alanında önemli adımlar atılmasını sağlasa da, birçok ülkenin bu tür düzenlemeleri kendi yasalarına entegre etmesi zaman alabilmektedir.

Yasal boşluklar, veri ihlalleri sonrası yaptırımların uygulanabilirliğini de zayıflatmaktadır. Yetersiz yasalar, veri ihlali sonrası sorumluluğu belirsiz hale getirirken, bu durum kamu kurumlarının siber saldırılara karşı daha savunmasız hale gelmesine neden olmaktadır (Eichensehr, 2020).

2.13.3.2. Veri İhlali Sonrasında Yasal Yaptırımlar

Veri ihlali sonrası uygulanan yasal yaptırımlar, birçok kurum için yeterince caydırıcı değildir. Veri ihlali sonrası yalnızca mali cezalar ve itibar kaybı gibi sonuçlarla karşılaşmak,

kurumları daha dikkatli olmaktan alıkoyabilmektedir. Bu durum, kurumların daha fazla veri güvenliği önlemi almalarını engelleyebilir (Çiçek, 2024).

Veri ihlalleri sonrasında uygulanacak yasal yaptırımlar, kamu sektöründe veri güvenliği açısından kritik bir mekanizma oluşturmaktadır. Ancak birçok ülkede, veri ihlalleri sonrası uygulanacak yaptırımların belirsizliği, kurumların bu tür olaylara karşı hazırlıklarını zayıflatmaktadır. Yasal yaptırımların etkinliği, aynı zamanda kurumların bu tür durumları önlemek için alacakları önlemlerin ciddiyetini artırmaktadır.

Veri ihlalleri sonrası uygulanacak yaptırımların belirlenmesi, yalnızca cezai boyutla sınırlı kalmamalıdır; aynı zamanda finansal, itibar ve operasyonel kayıpları da kapsamalıdır. Kamu kurumları, veri güvenliği ihlalleri nedeniyle karşılaşacakları sonuçları önceden değerlendirerek etkili bir risk yönetimi stratejisi geliştirmelidir. Bu yaklaşım, hem yasal yaptırımlara karşı hazırlıklı olmalarını sağlarken hem de veri güvenliği ihlallerini en aza indirmek için gerekli önlemleri almaları konusunda motive edici bir rol oynamaktadır.

2.13.4. Finansal Kısıtlamalar

Veri güvenliği, yüksek maliyetler gerektiren bir alandır ve birçok kamu kurumu, bütçe kısıtlamaları nedeniyle yeterli güvenlik önlemleri alamamaktadır. Finansal kısıtlamalar, yeni güvenlik teknolojilerine yatırım yapmayı ve mevcut altyapıyı güçlendirmeyi zorlaştırmaktadır. Kamu sektöründe veri güvenliği ve mahremiyeti ile ilgili sorunların bir diğer önemli boyutu, finansal kısıtlamalardır.

Özellikle, güvenlik yazılımları, donanımlar ve eğitim programları gibi gerekli unsurlar, sınırlı bütçeler nedeniyle yeterince finanse edilememektedir. Kamu kurumlarının karşılaştığı bu finansal engeller, güvenlik açıklarının ve veri ihlallerinin artmasına zemin hazırlamaktadır.

Finansal kısıtlamaların bir diğer etkisi, kurumların güvenlik teknolojilerine yatırım eksikliği yaşamasıdır. İleri düzey güvenlik sistemleri ve teknolojileri, büyük maliyetler gerektirebilir ve bu nedenle birçok kamu kurumu bu yatırımları yapmaktan kaçınmaktadır. Günümüzde, siber tehditlerin hızla evrim geçirmesi ve karmaşık hale gelmesi, kurumların güvenlik

teknolojilerine yatırım yapmalarını zorunlu kılmaktadır. Ancak, bütçe kısıtlamaları bu yatırımların önünde büyük bir engel oluşturmaktadır.

Finansal kısıtlamaların üstesinden gelmek için kamu kurumlarının, veri güvenliği bütçelerini artırmak üzere stratejiler geliştirmesi gerekmektedir. Ayrıca, kamu-özel ortaklıklar gibi alternatif finansman modellerinin kullanılması, veri güvenliği yatırımlarını desteklemek için önemli bir yöntemdir (Eriçok, 2023). Bu tür ortaklıklar, finansal kaynakların etkin bir şekilde yönetilmesini sağlayarak, kurumların güvenlik altyapılarını güçlendirmelerine yardımcı olabilir.

Kamu sektöründe veri güvenliği için finansal kısıtlamalar önemli bir sorun teşkil etmektedir. Bu sorunların aşılması için bütçelerin artırılması ve alternatif finansman yöntemlerinin kullanılması gerekmektedir. Böylece, kamu kurumları veri güvenliği önlemlerini güçlendirerek, siber tehditlere karşı daha dayanıklı hale gelebilir.

2.13.4.1. Veri Güvenliği için Ayrılan Kaynakların Azlığı

Bütçe kısıtlamaları, kamu kurumlarının veri güvenliği için gerekli yatırımları yapmalarını engellemektedir. Özellikle gelişen teknoloji ve artan tehditler karşısında, kurumların veri güvenliğine yönelik finansal kaynak ayırmaları kritik öneme sahiptir. Ancak birçok kurum, bu konuda kaynak eksikliği yaşamaktadır. 2019 yılında ABD’de yapılan bir araştırma, kamu sektörü kurumlarının yalnızca %40’ının güvenlik bütçesini yeterli seviyeye çıkardığını göstermektedir (Rosenbloom, Kravchuk ve Clerkin, 2022).

Finansal kısıtlamalar, kamu sektöründe veri güvenliği alanında karşılaşılan en büyük zorluklardan biridir. Birçok kamu kurumu, bütçe sınırlamaları nedeniyle yeterli kaynak ayıramamakta ve bu durum, veri güvenliği önlemlerinin uygulanmasını zorlaştırmaktadır. Veri güvenliği için yeterli bütçenin ayrılmaması, hem teknolojik altyapının güncellenmesini hem de personel eğitimini olumsuz yönde etkilemektedir.

Yetersiz finansman, güvenlik yazılımlarının edinilmesi veya güncellenmesi gibi kritik ihtiyaçların karşılanmasını engelleyebilir. Bu durumda, siber tehditlere karşı hazırlıksız kalmak kaçınılmaz hale gelir. Dolayısıyla, kamu kurumları veri güvenliği için bütçelerini yeniden değerlendirmeli ve bu alana daha fazla kaynak ayırma yoluna gitmelidir.

2.13.4.2. Güvenlik Teknolojilerine Yatırım Eksikliği

Yetersiz finansal kaynaklar, yeni güvenlik teknolojilerine yatırım yapmayı zorlaştırmaktadır. Güvenlik yazılımlarının, donanımlarının ve ağ güvenliği araçlarının eksikliği, siber saldırılara karşı zayıf bir savunma oluşturmaktadır.

Güvenlik teknolojilerine yatırım eksikliği, kamu sektöründeki veri güvenliği sorunlarının derinleşmesine yol açan bir diğer önemli faktördür. Modern siber tehditler sürekli olarak evrim geçirirken, kamu kurumları çoğu zaman bu tehditlerle başa çıkmak için gerekli olan güncel güvenlik çözümlerini edinmekte zorlanmaktadır. Özellikle yapay zeka ve makine öğrenimi gibi yenilikçi çözümlerin uygulanması, siber saldırılara karşı etkili bir savunma hattı oluşturmak için kritik öneme sahiptir (Ozkan-Okay vd., 2024).

Ancak sınırlı bütçeler nedeniyle birçok kamu kurumu, bu tür teknolojilere yatırım yapmaktan kaçınmakta veya ertelemektedir. Güvenlik yazılımlarının güncellenmesi, güvenlik duvarlarının iyileştirilmesi ve sızma testleri gibi önlemler, yeterli finansman sağlanmadığı takdirde hayata geçirilememektedir. Bu durum, kurumların siber saldırılara karşı savunmasız kalmasına ve veri ihlallerinin artmasına neden olmaktadır (Tudosı vd., 2023).

Kamu sektöründe güvenlik teknolojilerine yatırım yapılması, sadece mevcut tehditlere karşı bir savunma oluşturmakla kalmaz, aynı zamanda gelecekte ortaya çıkabilecek yeni tehditlere karşı da hazırlıklı olmayı sağlar. Dolayısıyla kamu kurumları, veri güvenliği yatırımlarını öncelik vermeli ve bu alanda stratejik planlamalar yaparak bütçelerini yeniden gözden geçirmelidir.

2.13.5. Kurum İçi Güvenlik Kültürünün Eksikliği

Kurum içindeki güvenlik kültürünün eksikliği, veri güvenliği ihlallerinin önlenmesinde büyük bir engel teşkil etmektedir. Güvenlik kültürü, çalışanların güvenlik önlemlerini benimsemelerini ve güvenlik ihlallerini önlemelerini sağlayan önemli bir faktördür (Sawiz, 2024). Kamu sektöründe veri güvenliği ve mahremiyeti açısından karşılaşılan sorunlardan biri de kurum içindeki güvenlik kültürünün eksikliğidir. Güvenlik kültürü, bir organizasyonun güvenlik konusundaki tutumunu, değerlerini ve davranışlarını yansıtır.

Kamu kurumlarında güvenlik kültürünün eksik olması, çalışanların veri güvenliği protokollerine uyumunu olumsuz etkileyebilir. Çalışanlar, güvenlik önlemlerinin önemini kavrayamadıklarında, bu önlemleri dikkate almayabilirler.

Yönetimsel destek eksikliği, güvenlik kültürünün zayıf olmasının bir başka nedenidir. Üst yönetim, güvenlik konularına yeterince önem vermezse, çalışanlar da bu konuyu ciddiye almayabilir. Güvenlik kültürünün oluşturulması için yöneticilerin aktif bir şekilde bu konulara katılması gerekmektedir. Üst yönetim, güvenlik politikalarını destekleyerek, çalışanların güvenlik bilincini artırmada önemli bir rol oynayabilir.

Çalışanların güvenlik sorunlarına yaklaşımı da kurum içi güvenlik kültürünün bir yansımasıdır. Çalışanlar, güvenlik tehditlerine karşı proaktif bir yaklaşım sergilemediklerinde, veri güvenliği açıklarını artırabilirler (Loukaka ve Rahman, 2020). Güvenlik sorunlarıyla karşılaşıldığında, bu sorunların çözümüne yönelik bir yaklaşım geliştirilmesi, güvenlik kültürünün güçlendirilmesine katkı sağlayacaktır. Bu doğrultuda, kurum içindeki iletişim kanallarının etkin kullanılması, güvenlik konularında bilgi paylaşımını teşvik edebilir.

Güvenlik kültürü oluşturulurken, çalışanların katılımını teşvik etmek de oldukça önemlidir. Çalışanlar, güvenlik sorunlarıyla ilgili olarak düşüncelerini ifade edebilmelidir. Bu tür bir katılım, çalışanların güvenlik protokollerine daha fazla sahip çıkmalarını ve bu konudaki farkındalıklarını artırmalarını sağlayacaktır. Düzenli olarak yapılan güvenlik toplantıları ve eğitimler aracılığıyla çalışanların güvenlik konusundaki görüşleri alınabilir ve bu görüşler doğrultusunda yeni stratejiler geliştirilebilir (Flowerday ve Tuyikeze, 2016).

Bununla birlikte, kurum içinde güvenlik kültürünün güçlendirilmesi için, güvenlik sorunlarının nasıl ele alınacağına dair net bir iletişim stratejisi de geliştirilmelidir. Çalışanların, güvenlik ihlalleri veya olası tehditler hakkında bilgi vermeleri teşvik edilmelidir. Güvenlik olaylarının gizli tutulması, çalışanların bu tür durumları rapor etmelerini engelleyebilir (Schneier, 2015). Bu nedenle, güvenlik ihlallerinin açık bir şekilde ele alındığı bir ortamın yaratılması, güvenlik kültürünün güçlendirilmesine yardımcı olacaktır.

Kamu sektöründe kurum içi güvenlik kültürünün eksikliği, veri güvenliği ve mahremiyetinin sağlanmasında önemli bir engel teşkil etmektedir. Yönetimsel destek, çalışan katılımı ve etkili iletişim stratejileri, güvenlik kültürünün güçlendirilmesinde kritik unsurlar olarak öne çıkmaktadır. Bu unsurların bir araya gelmesi, kamu kurumlarının veri güvenliği ve mahremiyetini artırmalarına yardımcı olacaktır.

2.13.5.1. Yönetimsel Destek Eksikliği

Veri güvenliği önlemleri, üst düzey yönetimin desteğini gerektirir. Ancak birçok kamu kurumunda, yöneticiler bu konuda yeterince aktif değildir. Yönetimin güvenlik kültürünü teşvik etmemesi, çalışanların veri güvenliği ihlalleri konusunda duyarsız kalmasına yol açabilir. 2018 yılında yapılan bir araştırma, kamu sektörü kurumlarının yalnızca %30'unun yönetimden veri güvenliği konusunda gerekli desteği aldığını ortaya koymuştur (Waind, 2020).

Kamu sektöründe veri güvenliği kültürü oluşturmak, yönetimsel destekle doğrudan ilişkilidir. Üst düzey yönetimin veri güvenliği konusundaki tutumu, tüm organizasyonun güvenlik anlayışını şekillendirir. Yönetim, veri güvenliği politikalarının oluşturulması, uygulanması ve sürdürülmesi süreçlerinde aktif bir rol almalıdır. Ancak birçok kurumda, üst yönetimin veri güvenliği konularına yeterince önem vermemesi, çalışanların da bu konudaki motivasyonunu düşürmektedir.

Araştırmalar, yönetim desteğinin yüksek olduğu kurumlarda çalışanların veri güvenliği konusundaki sorumluluklarını daha ciddiye aldıklarını göstermektedir (Stewart ve Jürjens, 2017). Yönetim, güvenlik kültürünün benimsenmesi için gerekli kaynakları sağlamalı ve güvenlik politikalarını aktif bir şekilde desteklemelidir. Ayrıca, yönetimin veri güvenliği konusundaki farkındalığını artırmak için düzenli eğitim programları ve bilgilendirme toplantıları düzenlenmelidir.

2.13.5.2. Çalışanların Güvenlik Sorunlarına Yaklaşımı

Çalışanların güvenlik sorunlarına yaklaşımı, bir kurumun güvenlik kültürünün gücünü belirler. Kamu kurumlarındaki çalışanlar, güvenlik önlemlerini genellikle ikinci planda tutabilirler, bu da ihlallere neden olabilir. 2019 yılında yapılan bir araştırma, çalışanların

%50'sinin, kurumlarındaki veri güvenliği politikasına tamamen uymadığını göstermektedir (Alraja vd., 2023).

Kurum içindeki güvenlik kültürü, sadece yönetimle sınırlı kalmaz; aynı zamanda çalışanların güvenlik sorunlarına yaklaşımını da içerir. Çalışanların, veri güvenliği konusundaki farkındalıkları ve bu konudaki tutumları, organizasyonun genel güvenlik duruşunu belirler. Ancak birçok durumda, çalışanlar veri güvenliği konularını göz ardı etmekte veya önemsememektedir. Bu durum, veri ihlallerine zemin hazırlayan bir atmosfer yaratır.

Çalışanların güvenlik sorunlarına yaklaşımını iyileştirmek için, kurum içindeki iletişim kanallarının güçlendirilmesi gerekmektedir. Çalışanlar, veri güvenliği ile ilgili endişelerini açıkça dile getirebilmeli ve bu konudaki önerilerini iletebilmelidir. Ayrıca, çalışanların veri güvenliği konusundaki katkılarının takdir edilmesi, güvenlik kültürünün pekişmesine yardımcı olacaktır. Güvenlik konularında farkındalık oluşturan çalışanlar için ödüller veya teşvikler sunulabilir.

Kamu sektöründe veri güvenliği ve mahremiyeti ile ilgili sorunlar, çok boyutlu bir yaklaşım gerektirmektedir. Teknolojik altyapının güçlendirilmesi, çalışanların eğitime yatırım yapılması, yasal düzenlemelerin güncellenmesi ve güvenlik kültürünün oluşturulması gibi unsurlar, bu sorunların üstesinden gelinmesine yardımcı olacaktır. Her bir kurum, kendi özel koşullarını değerlendirerek, veri güvenliği stratejilerini bu doğrultuda geliştirmelidir.

2.14. Türkiye'de Kamu Kurumlarına Yönelik Siber Saldırı Örnekleri

Türkiye, son yıllarda siber saldırılara maruz kalan ülkeler arasında yer almaktadır. Kamu kurumları, bu saldırılardan en fazla etkilenen yapılar arasında bulunmaktadır (Karasoy ve Gezici, 2023). Siber saldırılar, yalnızca veri ihlalleri veya sistem çöküşleri ile sınırlı kalmayıp, kamu güvenliği ve ulusal savunma açısından da ciddi tehditler oluşturmaktadır. Aşağıda, Türkiye'deki bazı önemli siber saldırı örnekleri sunulmaktadır.

2.14.1. 2016 Türkiye Cumhuriyeti Bilgi Teknolojileri ve İletişim Kurumu (BTK) Saldırısı

2016 yılında Türkiye Cumhuriyeti Bilgi Teknolojileri ve İletişim Kurumu (BTK), siber saldırılara uğramıştır. Saldırının arkasında, "Anonymous" isimli hacker grubu olduğu iddia edilmiştir. Bu saldırı, BTK'nın web sitesinin çökmesine ve çeşitli hizmetlerin aksamasına neden olmuştur. Saldırının gerekçesi olarak, Türkiye'nin internet üzerindeki sansür politikaları ve kullanıcı verilerinin korunmaması gösterilmiştir (URL-8)

Saldırının ardından BTK, siber güvenlik alanında alınan tedbirleri artırmış ve internet güvenliğini sağlamak için yeni stratejiler geliştirmiştir. Bu olay, kamu kurumlarının siber güvenlik önlemlerinin ne denli önemli olduğunu bir kez daha gözler önüne sermiş ayrıca kamu kurumlarının siber güvenlik alanında daha fazla önlem alması gerektiğini ortaya koymuştur.

2.14.2. 2020 Sağlık Bakanlığı Saldırısı

2020'nin başlarında, Türkiye Sağlık Bakanlığı, COVID-19 pandemisi sürecinde kritik bir dönemde siber saldırıya uğramıştır. Bu saldırıda, sağlık verileri hedef alınmış ve bazı sağlık verilerine izinsiz erişim sağlanmıştır. Saldırının ardından, uluslararası bir siber suç örgütü olduğu belirtilmiştir (URL-9).

Sağlık Bakanlığı, saldırının ardından sistemlerini güçlendirmek ve siber güvenlik önlemlerini artırmak amacıyla hızlı bir şekilde harekete geçmiştir. Bu olay, sağlık sektörü verilerinin korunmasının ve güvenliğinin ne kadar hayati bir öneme sahip olduğunu ortaya koymuştur. Ayrıca, sağlık hizmetleri sağlayıcılarının siber tehditlere karşı hazırlıklı olmaları gerektiği gerçeğini vurgulamaktadır.

2.14.3. 2018 Türkiye Cumhuriyeti Merkez Bankası Saldırısı

2018 yılında, Türkiye Cumhuriyeti Merkez Bankası, önemli bir siber saldırıya maruz kalmıştır. Saldırıda, bankanın dijital hizmetleri hedef alınmış ve bazı hizmetlerde kesintilere neden olmuştur. Bu olay, Merkez Bankası'nın sistemlerinin güvenliğini sorgulanır hale

getirmiştir. Saldırının ardından bankanın, siber güvenlik önlemlerini yeniden gözden geçirmesi ve güncellemesi gerektiği anlaşılmıştır (URL-10).

Siber saldırılar, finansal kurumların itibarını zedelemenin yanı sıra, ekonomiye de zarar verebilecek sonuçlar doğurabilir. Bu nedenle, Merkez Bankası ve benzeri kuruluşların, siber güvenlik stratejilerini geliştirmeleri ve sıkı güvenlik protokolleri uygulamaları gerekmektedir.

2.14.4. 2022 Belediyelere Yapılan Fidyeye Yazılım Saldırıları

2022 yılında, Türkiye’de bazı belediyelerin sistemlerine yönelik fidye yazılım saldırıları gerçekleşmiştir. Bu saldırılarda, belediye hizmetlerinin sunumunda kullanılan veriler şifrelenmiş ve saldırganlar tarafından fidye talep edilmiştir. Bu tür saldırılar, kamu hizmetlerinin duraksamasına ve vatandaşların temel hizmetlere erişiminde zorluklara yol açmıştır (URL-11).

2.15. Veri Güvenliği ve Mahremiyetine Yönelik Çözüm Önerileri

Kamu sektöründe veri güvenliği ve mahremiyetine yönelik başlıca çözüm önerileri aşağıdaki başlıklarda ele alınmıştır.

2.15.1. Teknolojik Altyapının Güçlendirilmesi

Kamu kurumlarının dijitalleşme süreçleri, veri güvenliğini sağlamada güçlü ve sürdürülebilir teknolojik altyapılara ihtiyaç duyulmasını zorunlu kılmıştır. Siber tehditlerin giderek karmaşıklaşması ve özellikle kamu kurumlarını hedef alan fidye yazılım saldırıları gibi saldırılar, altyapının modernizasyonunu zorunlu hale getirmiştir (Uysal ve Malkoç Yılmaz, 2025). Dolayısıyla teknolojik altyapının güçlendirilmesi, yalnızca mevcut tehditlere karşı bir savunma hattı oluşturmakla kalmaz, aynı zamanda gelecekte ortaya çıkabilecek tehditlere karşı dayanıklılığı artıracaktır.

2.15.1.1. Bulut Teknolojilerinin Kullanımı

Bulut teknolojileri, kamu kurumlarının veri yönetimi ve güvenliği konusunda önemli avantajlar sunmaktadır. Bu teknolojiler, verilerin merkezi bir şekilde depolanmasını, yönetilmesini ve korunmasını sağlayarak, geleneksel kurumiçi sistemlere kıyasla daha

yüksek güvenlik standartları sunabilmektedir. Bulut hizmet sağlayıcıları, genellikle en son güvenlik protokollerini ve şifreleme teknolojilerini kullanmakta, bu da kamu kurumlarının veri güvenliği seviyesini artırmaktadır (Aytekin, Erdoğan ve Kavalcı, 2016). Ancak bulut teknolojilerinin kullanımında dikkat edilmesi gereken bazı hususlar vardır ki veri lokalizasyonu konusu büyük önem taşımaktadır. Kamu kurumları, hassas verilerin ülke sınırları içinde tutulmasını sağlayacak yerel bulut hizmetlerini tercih etmelidir. Ayrıca, bulut hizmet sağlayıcılarıyla yapılacak anlaşmalarda, veri güvenliği ve mahremiyet konularında net standartlar ve sorumluluklar belirlenmelidir.

Bulut teknolojilerinin bir diğer avantajı da ölçeklenebilirlik ve maliyet etkinliğidir. Kamu kurumları, ihtiyaçlarına göre kaynaklarını hızlı bir şekilde artırıp azaltabilir, bu da hem operasyonel verimliliği artırır hem de maliyetleri optimize eder.

2.15.1.2. Güncel Güvenlik Sistemleri ve Yazılımlar

Kamu kurumlarının veri güvenliği ve mahremiyetini sağlamak için güncel güvenlik sistemleri ve yazılımları kullanmaları gerekmektedir (Tüminçin vd., 2019). Bu sistemler arasında gelişmiş güvenlik duvarları, saldırı tespit ve önleme sistemleri (IDS/IPS), veri kaybı önleme (DLP) çözümleri ve gelişmiş uç nokta koruma yazılımları yer almaktadır (Paşaoğlu, Güler ve Jafari, 2019).

Özellikle yapay zeka ve makine öğrenimi tabanlı güvenlik çözümleri, geleneksel sistemlere göre daha etkili bir koruma sağlamaktadır. Bu sistemler, normal davranış kalıplarını öğrenerek anormal aktiviteleri hızlı bir şekilde tespit edebilmekte ve potansiyel tehditlere karşı proaktif önlemler alabilmektedir. Güncel antivirüs yazılımları, tehdit algılama sistemleri ve güvenlik duvarlarının kullanımı siber tehditlere karşı etkili bir savunma mekanizması sağlar.

Veri şifreleme teknolojileri de güncel güvenlik sistemlerinin önemli bir bileşenidir. Hem durağan haldeki (at rest) hem de hareket halindeki (in transit) verilerin şifrlenmesi, veri güvenliği açısından kritik öneme sahiptir (Swanzy vd., 2024). Kamu kurumları, en son şifreleme standartlarını (örneğin, AES-256) kullanmalı ve düzenli olarak bu standartları güncellemelidir.

Ayrıca, düzenli güvenlik denetimleri ve penetrasyon testleri yapılması, sistemlerdeki zafiyetlerin tespit edilmesi ve giderilmesi açısından önemlidir. Bu testler, potansiyel

saldırganların kullanabileceği güvenlik açıklarını ortaya çıkararak, kamu kurumlarının proaktif bir şekilde önlem almasını sağlar.

2.15.2. Kamu Çalışanlarının Eğitim ve Farkındalık Programları

Kamu çalışanlarının veri güvenliği ve mahremiyet konularında farkındalığını artırmak, kamu kurumlarının siber güvenlik kapasitesini güçlendirmek için hayati önem taşır. Çalışanların bilgi güvenliği protokollerine uyumu, sadece teknik altyapının yeterliliği ile sınırlı değildir; aynı zamanda eğitim programlarının etkili şekilde uygulanmasıyla mümkün olur.

Kamu çalışanlarının bilinçlendirilmesi, veri güvenliği politikalarının başarısında kritik bir rol oynar. İnsan hatası, birçok veri ihlalinin temel nedenidir ve bu durum eğitimin önemini vurgulamaktadır.

2.15.2.1. Farkındalık Yaratma Stratejileri

Farkındalık yaratma, bilgi güvenliğinin temelini oluşturur. Kamu çalışanlarına yönelik düzenli farkındalık kampanyaları, özellikle sosyal mühendislik saldırılarına karşı etkili bir savunma mekanizması sağlayabilir. Kamu kurumlarında veri güvenliği ve mahremiyet konularında farkındalık yaratmak için çeşitli stratejiler uygulanabilir. Bu stratejiler arasında (Özdemir ve Uluyol, 2021):

- **Düzenli bilgilendirme e-postaları ve bültenler:** Çalışanlara güncel tehditler ve güvenlik uygulamaları hakkında bilgi verilmesi.
- **İnteraktif eğitim modülleri:** Çalışanların aktif katılımını sağlayan, senaryoya dayalı online eğitimler.
- **Poster ve infografikler:** Ofis ortamında görsel hatırlatıcıların kullanılması.
- **Simülasyon tabanlı phishing testleri:** Çalışanların gerçek hayattaki tehditlere karşı hazırlıklı olmalarını sağlayan uygulamalı testler.
- **Güvenlik şampiyonları programı:** Her müdürlükten seçilen çalışanların veri güvenliği konusunda lider rol üstlenmesi.

Bu stratejilerin etkin bir şekilde uygulanması, çalışanların günlük iş rutinlerinde veri güvenliği ve mahremiyet konularını öncelikli hale getirmelerini sağlayacaktır.

ABD'nin "Stop. Think. Connect." kampanyası, çalışanların siber tehditler konusunda bilinçlenmesini sağlamıştır (Rama ve Keevy, 2023). Türkiye'de de benzer farkındalık kampanyaları, kamu çalışanlarının güvenlik protokollerine uyumunu artırabilir.

2.15.2.2. Düzenli Güvenlik Eğitimi ve Sertifikasyon Programları

Kamu çalışanlarının veri güvenliği ve mahremiyet konularında sürekli eğitim almaları kritik öneme sahiptir (Toros, 2025). Bu eğitimler; Temel veri güvenliği ve mahremiyet kavramları, Güncel tehdit türleri ve korunma yöntemleri, Yasal ve etik sorumluluklar, Güvenli veri işleme ve paylaşım uygulamalar, Olay müdahale prosedürleri gibi konuları kapsamalıdır.

Eğitimlerin etkinliğini artırmak ve çalışanların motivasyonunu yükseltmek için sertifikasyon programları uygulanabilir. Bu sertifikalar, çalışanların kariyer gelişimlerinde bir avantaj olarak değerlendirilebilir ve kurumsal güvenlik kültürünün oluşmasına katkı sağlayabilir.

Düzenli eğitim ve sertifikasyon programları, çalışanların sadece güncel tehditlere karşı hazırlıklı olmalarını sağlamakla kalmaz, aynı zamanda veri güvenliği ve mahremiyeti konularında proaktif bir yaklaşım geliştirmelerine de yardımcı olur. Potansiyel risklerin erken tespit edilmesi ve önlenmesi açısından kritik öneme sahiptir. Kamu kurumlarında ISO 27001 gibi uluslararası standartlara dayalı eğitim programlarının uygulanması, veri güvenliğini güçlendirebilir (Çakır ve Tuygun, 2019).

2.15.3. Güçlendirilmiş Yasal Düzenlemeler

Kamu sektörü, veri güvenliği ve mahremiyetine yönelik güçlü bir yasal çerçeve olmadan, siber tehditlere karşı savunmasız kalabilir. Yasal düzenlemeler, veri ihlallerini önlemede caydırıcı bir rol oynar. Veri güvenliği için güçlü bir yasal çerçeve, kamu kurumlarının sorumluluklarını ve görevlerini netleştirir.

2.15.3.1. KVKK ve GDPR Kapsamındaki Düzenlemelerin İyileştirilmesi

Türkiye'de Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği'nde Genel Veri Koruma Yönetmeliği (GDPR), veri güvenliği ve mahremiyeti konusunda temel yasal çerçeveyi oluşturmaktadır. Ancak, teknolojinin hızlı gelişimi ve değişen tehdit ortamı, bu düzenlemelerin sürekli olarak gözden geçirilmesini ve iyileştirilmesini gerektirmektedir.

KVKK'nın GDPR ile daha fazla uyumlu hale getirilmesi, uluslararası veri transferleri ve iş birliği açısından önemlidir. GDPR'daki "unutulma hakkı" ve "veri taşınabilirliği" gibi kavramların KVKK'ya daha detaylı bir şekilde entegre edilmesi düşünülebilir. KVKK'nın, GDPR örnek alınarak genişletilmesi, bireysel hakların korunmasına katkıda bulunabilir.

Ayrıca, yapay zeka ve büyük veri gibi yeni teknolojilerin kullanımına ilişkin spesifik düzenlemelerin eklenmesi, kamu kurumlarının bu teknolojileri güvenli ve etik bir şekilde kullanmalarını sağlayabilir (Cath, 2018).

2.15.3.2. Veri İhlallerine Karşı Yasal Yaptırımların Artırılması

Veri ihlallerine karşı caydırıcı ve etkili yasal yaptırımların uygulanması, kamu kurumlarının veri güvenliği ve mahremiyet konularına daha fazla önem vermelerini sağlayacaktır. Söz konusu yasal yaptırımlar;

- **Para cezalarının artırılması:** GDPR'daki gibi, yıllık global cironun belirli bir yüzdesine kadar varan cezalar uygulanabilir.
- **Kişisel sorumluluk:** Veri ihlallerinden sorumlu kamu görevlilerine yönelik kişisel yaptırımlar (örneğin, görevden uzaklaştırma veya cezai sorumluluk) uygulanabilir.
- **İhbar zorunluluğu:** Veri ihlallerinin belirli bir süre içinde (örneğin 72 saat) ilgili otoritelere ve etkilenen kişilere bildirilmesi zorunlu hale getirilebilir.
- **Düzenli denetimler:** Bağımsız denetim kuruluşları tarafından düzenli veri güvenliği denetimlerinin yapılması ve sonuçların kamuoyuyla paylaşılması zorunlu kılınabilir.
- **Şeffaflık gereklilikleri:** Kamu kurumlarının veri işleme faaliyetleri hakkında düzenli raporlar yayınlamaları ve bu raporların kamuoyuna açık olması sağlanabilir.

Bu tür yasal yaptırımların artırılması, kamu kurumlarının veri güvenliği ve mahremiyet konularına daha proaktif bir yaklaşım benimsemelerini teşvik edecektir (Uslan ve Değirmenci, 2023).

2.15.4. Finansal Kaynakların Artırılması

Veri güvenliği ve mahremiyeti için finansal kaynakların artırılması, sürdürülebilir bir siber güvenlik altyapısının temel taşıdır. Veri güvenliği için ayrılan bütçeler, tehditlerin önlenmesinde doğrudan etkili olabilir. Kamu kurumlarının bu alana yeterli yatırım yapmaması, uzun vadede çok daha büyük maliyetlere ve güven kaybına yol açabilir.

2.15.4.1. Kamu Bütçelerinde Veri Güvenliğine Ayrılan Payın Yükseltilmesi

Kamu kurumlarının yıllık bütçelerinde veri güvenliği ve mahremiyeti için ayrılan payın artırılması gerekmektedir. Bu artış; Teknolojik altyapının güçlendirilmesi, Uzman personel istihdamı ve mevcut personelin eğitimi, Güvenlik denetimleri ve penetrasyon testleri, Ar-Ge faaliyetleri ve yenilikçi güvenlik çözümlerinin geliştirilmesi alanlarında yoğunlaştırılabilir (George vd., 2024).

Bütçe artışının yanı sıra, veri güvenliği harcamalarının etkinliğinin düzenli olarak değerlendirilmesi ve raporlanması da önemlidir. Böylelikle, kaynakların en verimli şekilde kullanılmasını sağlayacaktır.

Finlandiya, kamu sektöründe siber güvenlik için bütçesini 2022 yılında %30 oranında artırarak tehditlere karşı daha güçlü bir altyapı oluşturmuştur (Helin ve Himanen, 2023)

2.15.4.2. Güvenlik Teknolojilerine Yatırım

Kamu kurumları, en son güvenlik teknolojilerine yatırım yaparak veri güvenliği ve mahremiyet seviyelerini yükseltebilirler. Bu yatırımlar şunları içerebilir:

- Yapay zeka ve makine öğrenimi tabanlı tehdit tespit sistemleri
- Gelişmiş şifreleme teknolojileri
- Blok zinciri tabanlı veri doğrulama ve izleme sistemleri
- Kuantum-güvenli şifreleme çözümleri
- Biyometrik kimlik doğrulama sistemleri

Bu teknolojilere yapılan yatırımlar, kamu kurumlarının gelecekteki tehditlere karşı hazırlıklı olmalarını sağlayacaktır. Ayrıca, bu yatırımlar yerli teknoloji şirketlerinin gelişmesine ve ülkenin siber güvenlik alanında dışa bağımlılığının azalmasına katkıda bulunabilir

Güvenlik teknolojilerine yapılan yatırımların etkinliğini artırmak için, kamu kurumları arasında bilgi ve deneyim paylaşımı da teşvik edilmelidir. Böylece, kaynakların daha verimli kullanılmasını ve en üstün kabul edilen tekniğin yaygınlaşmasını sağlayacaktır.

Makine öğrenimi ve yapay zeka destekli güvenlik araçları, kamu kurumlarının riskleri önceden tespit etmesine yardımcı olabilir. Japonya, blockchain tabanlı teknolojilere yaptığı yatırımlarla bu alanda öncü bir model oluşturmuştur (Lim vd., 2019).

2.15.5. Kurumlar Arası İş Birlikleri ve İş Birliği Modelleri

Veri güvenliği ve mahremiyetinin sağlanmasında kurumlar arası iş birliği stratejileri, kaynakların etkin kullanımını destekler ve uluslararası iş birliği fırsatları yaratır. Kamu sektörü, güvenlik politikalarını güçlendirmek için hem ulusal hem de uluslararası iş birliklerinden faydalanmalıdır. Veri güvenliği ve mahremiyeti konularında başarılı olmak için, kamu kurumlarının kendi aralarında ve özel sektörle iş birliği yapmaları gerekmektedir. Bu iş birlikleri, bilgi paylaşımını artırır, kaynakların daha etkin kullanılmasını sağlar ve ortak tehditlere karşı daha güçlü bir savunma hattı oluşturur.

2.15.5.1. Kamu-Özel Sektör İş birlikleri

Kamu kurumları ile özel sektör arasında kurulacak iş birlikleri, veri güvenliği ve mahremiyet alanında önemli faydalar sağlayabilir ki bunlar;

- Özel sektörün sahip olduğu ileri teknolojiler ve uzmanlık, kamu kurumlarına aktarılabilir.
- Kamu ve özel sektör, yenilikçi güvenlik çözümleri geliştirmek için ortak projeler yürütebilir.
- Kamu ve özel sektör, siber tehditler hakkında gerçek zamanlı bilgi paylaşımı yapabilir.
- Özel sektör, kamu çalışanlarına yönelik eğitim programları düzenleyebilir.
- Kamu ve özel sektör uzmanlarından oluşan ortak müdahale ekipleri oluşturulabilir.

Bu tür iş birlikleri, kamu kurumlarının en son güvenlik uygulamalarından ve teknolojilerinden faydalanmasını sağlarken, özel sektörün de kamu verilerinin korunmasında aktif rol almasını teşvik eder (Jean-Quartier, 2022).

Kamu-özel sektör iş birlikleri, kamu kurumlarının özel sektörün yenilikçi çözümlerinden faydalanmasını sağlar. ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı (**CISA**), özel sektörle iş birliği yaparak kritik altyapıların güvenliğini artırmaktadır (Roshanaei, 2023).

2.15.5.2. Ulusal ve Uluslararası Güvenlik İnisiyatifleri

Veri güvenliği ve mahremiyet konuları, ulusal sınırları aşan bir nitelik taşıdığından, uluslararası iş birliği büyük önem taşımaktadır. Bu doğrultuda;

Uluslararası siber güvenlik anlaşmaları: Ülkeler arasında veri güvenliği ve mahremiyet standartlarının uyumlaştırılması için anlaşmalar yapılabilir.

Ülkeler arasında düzenli siber güvenlik tatbikatları düzenlenebilir.

- Uluslararası düzeyde tehdit istihbaratı paylaşımı için güvenli platformlar oluşturulabilir.
- Ülkeler arasında veri güvenliği ve mahremiyet konularında ortak araştırma projeleri yürütülebilir.
- Farklı ülkelerden uzmanların bir araya geldiği çalışma grupları oluşturularak, global ölçekte veri güvenliği stratejileri geliştirilebilir.
- Veri güvenliği ve mahremiyet konularında uluslararası standartların geliştirilmesi ve uygulanması için iş birlikleri yapılabilir (Naseeb ve Khan, 2024).

Bu tür uluslararası iş birlikleri, ülkelerin tek başlarına karşı koyamayacakları büyük ölçekli siber tehditlere karşı ortak bir savunma hattı oluşturmalarına yardımcı olur. Ayrıca, farklı ülkelerin deneyimlerinden ve uzmanlıklarından karşılıklı olarak faydalanmalarını sağlar. Ulusal düzeyde ise, aşağıda belirtilen iş birliği modelleri ile kamu kurumları arasında daha sıkı bir iş birliği ve koordinasyon sağlanabilir.

- Tüm kamu kurumlarının veri güvenliği ve mahremiyet uygulamalarını koordine eden ve denetleyen merkezi bir kurum oluşturulabilir.
- Benzer veri türleriyle çalışan kamu kurumları arasında sektörel çalışma grupları kurulabilir.
- Kamu kurumlarının verilerini güvenli bir şekilde depolayabilecekleri ve yönetebilecekleri ortak veri merkezleri oluşturulabilir.
- Kamu kurumlarının bilgi işlem ve güvenlik yöneticilerinin düzenli olarak bir araya gelerek deneyim ve bilgi paylaşımı yapmaları sağlanabilir.
- Birden fazla kamu kurumuna hizmet veren, 7/24 çalışan güvenlik operasyon merkezleri kurulabilir.

Bu tür ulusal iş birliği modelleri, kamu kurumları arasında veri güvenliği ve mahremiyet konularında bir sinerji oluşturarak, kaynakların daha verimli kullanılmasını ve tehditlere karşı daha etkin bir savunma sağlanmasını mümkün kılar (Abisoye ve Akerele, 2021).

Ulusal güvenlik inisiyatifleri kapsamında, **Avrupa Siber Güvenlik Ajansı (ENISA)** tarafından oluşturulan ortak platformlar, ülkeler arasında bilgi paylaşımını desteklemektedir (Köksoy, 2020). Türkiye, bu tür platformlara daha aktif bir şekilde katılım sağlayarak uluslararası standartlara uyumunu güçlendirebilir. ENISA gibi uluslararası inisiyatifler, kamu sektöründe veri güvenliğini sağlamak için önemli bir model sunmaktadır.



3.LİTERATÜR TARAMASI

Kamu sektöründe veri güvenliği ve veri mahremiyeti konusundaki mevcut literatür incelenecek; bu alandaki sorunlar, çözüm önerileri ve önceki araştırmaların bulguları ele alınacaktır. Literatür taraması, araştırmanın teorik çerçevesini oluşturmak ve mevcut bilgi boşluklarını belirlemek amacıyla yapılmıştır.

Literatür taramasında 2017-2025 yılları arasını kapsayan dönemde “veri güvenliği”, “veri mahremiyeti”, “kamu sektörü”, “KVKK” ve “kişisel verilerin korunması” anahtar kelimeleri esas alınarak kapsamlı bir tarama gerçekleştirilmiştir. Bu doğrultuda Yükseköğretim Kurulu Ulusal Tez Merkezi (YÖK Tez), Web of Science (WoS), Scopus ve Google Scholar gibi ulusal ve uluslararası akademik veri tabanları sistematik şekilde incelenmiştir. Söz konusu veri tabanlarında belirlenen anahtar kelimeler farklı kombinasyonlar kullanılarak ilgili literatüre ulaşılmış, elde edilen kaynaklar konu uygunluğu, yöntembilimsel yeterlilik ve çalışmanın kamusal bağlamda ilişkisi açısından değerlendirilmiştir. Literatür taraması sonucunda ayrıca bu alanda yapılan akademik çalışmaların sınırlı olduğunu ortaya koymuştur.

Özgür ve Erciyes (2017) çalışmasında, kamu kurumlarında güvenlik kültürünün oluşturulmasının önemini vurgulamış ve yönetimin desteklediği bir güvenlik kültürünün, veri güvenliği ihlallerini azaltma potansiyeline sahip olduğunu belirtmiştir.

Barkuş ve Koç (2019) çalışmasında, veri ihlallerinin bireyler üzerindeki etkilerini araştırmış ve bu tür ihlallerin toplumsal güveni nasıl sarstığını incelemiştir. Çalışma, veri ihlali yaşanan durumlarda bireylerin devlet kurumlarına karşı duyduğu güvensizliğin arttığını ve bu durumun kamu güvenliği politikalarını zorlaştırdığını göstermektedir. Ayrıca, bireylerin veri mahremiyeti konusundaki farkındalıklarının artırılmasının önemine değinmiştir.

Hizarcı (2019) çalışmasında, Türkiye’de Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) çerçevesinde yapılan yasal düzenlemelerin etkinliğini incelemiştir. Araştırma, bu yasal düzenlemelerin veri ihlallerini önleme konusunda önemli bir adım olduğunu göstermekte, ancak uygulamada karşılaşılan

zorlukların da altını çizmektedir. Özellikle, yasal boşlukların ve düzenleme eksikliklerinin, veri güvenliğini tehdit eden faktörler arasında yer aldığı ifade edilmiştir.

Göçoğlu (2020) çalışmasında, kamu sektöründe veri güvenliği için teknolojik çözümler üzerine bir çalışma gerçekleştirmiştir. Araştırma, bulut bilişim ve yapay zeka gibi modern teknolojilerin, veri güvenliğini artırmada nasıl kullanılabileceğini detaylandırmıştır. Çalışma, kamu kurumlarının bu teknolojilere yatırım yaparak güvenlik altyapılarını güçlendirmeleri gerektiğini savunmaktadır.

Kiraz (2021) çalışmasında, bu ihlallerin kamu kurumları üzerindeki olumsuz etkileri ve kurum imajı üzerindeki sonuçlar tartışılmıştır. Çalışma, veri ihlallerinin yarattığı itibar kaybının, kamu kurumlarının işleyişini olumsuz etkilediğini göstermektedir.

Hatipoğlu ve Tunacan (2021) çalışmasında, Türkiye'deki kamu kurumlarına yönelik siber saldırıları incelemiş ve bu saldırıların güvenlik açıkları ile ilişkisini analiz etmiştir. Araştırma, siber saldırıların çoğunlukla zayıf güvenlik önlemleri ve yetersiz eğitim nedeniyle gerçekleştiğini ortaya koymaktadır. Çalışma, siber saldırılar sonrası kamu kurumlarının maruz kaldığı itibar kaybının, kamu hizmetlerinin etkinliğini olumsuz etkilediğini vurgulamıştır.

Özdemir ve Uluyol (2021), kamu çalışanlarının veri güvenliği konusundaki farkındalık düzeylerini değerlendirmiştir. Araştırma, çalışanların güvenlik protokollerine uyumlarının yetersiz olduğunu ve bu durumun veri ihlallerine zemin hazırladığını ortaya koymuştur. Çalışmada, düzenli eğitim programlarının ve farkındalık artırma kampanyalarının, güvenlik kültürünü güçlendirme potansiyeli taşıdığı vurgulanmaktadır.

Efe (2022) çalışmasında, veri güvenliğinin yalnızca teknik bir gereklilik değil, aynı zamanda bireylerin mahremiyetini korumak için etik bir yükümlülük olduğunu vurgulamıştır. Aynı çalışmada, kamu sektöründeki veri yönetiminin, hem güvenlik hem de mahremiyet açısından kritik öneme sahip olduğu belirtilmiştir.

Özyiğit (2022) çalışmasında, bulut teknolojilerinin veri güvenliğini artırma potansiyelini vurgulamış ve bu teknolojilerin kamu kurumlarında nasıl etkin bir şekilde kullanılabileceğine dair önerilerde bulunmuştur.

Veri mahremiyeti ihlalleri, kamu sektöründe giderek yaygınlaşan bir sorun haline gelmiştir. Abanoz ve Acar (2023) tarafından yapılan bir araştırma, veri ihlallerinin kişisel veri sahipleri üzerindeki psikolojik etkilerini ve toplumda yarattığı güvensizlik algısını incelemiştir. Araştırma, veri ihlallerinin yalnızca bireyler üzerinde değil, aynı zamanda kamu kurumlarının güvenilirliği üzerinde de derin etkileri olduğunu ortaya koymaktadır.

Uslu (2023) çalışmasında, kamu kurumlarında veri güvenliği stratejilerini incelemiş ve mevcut stratejilerin etkinliği üzerinde durmuştur. Çalışma, veri güvenliği yönetim sistemlerinin entegrasyonunun önemini vurgulamış ve stratejik bir yaklaşım benimsemenin, veri güvenliği ihlallerini azaltma potansiyeline sahip olduğunu belirtmiştir.

Yasal düzenlemelerin etkisi, veri güvenliği ve mahremiyeti bağlamında literatürde önemli bir yer tutmaktadır. Uslan ve Değirmenci (2023) çalışmasında, Türkiye'deki Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) kapsamındaki düzenlemelerin etkinliği incelenmiştir. Araştırma, bu yasal düzenlemelerin hem bireylerin haklarını korumada hem de kamu kurumlarının veri yönetiminde sağladığı katkıları değerlendirmiştir.

Çubukcu (2024) tarafından yapılan başka bir çalışmada ise, yasal düzenlemelerin iyileştirilmesi ve veri ihlallerine karşı yaptırımların artırılması gerektiği önerilmiştir. Bu öneriler, kamu sektöründe veri güvenliğinin artırılmasına yönelik somut adımlar atılmasını sağlamayı hedeflemektedir.

Literatür incelendiğinde, kamu sektöründe veri güvenliği ve mahremiyetiyle ilgili çeşitli çözüm önerileri sunulmaktadır. Kahraman ve Özen (2025) çalışmasında, teknolojik altyapının güçlendirilmesi gerektiği belirtilmiş, güncel güvenlik sistemlerinin ve yazılımlarının kullanılmasının önemine vurgu yapılmıştır. Ayrıca, kamu çalışanlarının eğitim ve farkındalık programlarının artırılması gerektiği de ifade edilmiştir.

Kamu sektöründe veri güvenliği ile ilgili sorunlar, çeşitli araştırmalarda ele alınmıştır. Kalıpçı (2025) tarafından gerçekleştirilen bir çalışmada, kamu kurumlarının siber saldırılara karşı yetersiz savunma mekanizmalarına sahip olduğu ortaya konmuştur. Çalışma, Türkiye'deki kamu kurumlarının güvenlik altyapılarının sıkça güncellenmediğini ve bu durumun veri ihlallerine zemin hazırladığını göstermektedir.

Yukarıda incelen alıřmalar, kamu sektrnde veri gvenlięi ve mahremiyeti konusunun ok boyutlu bir alan olduęunu gstermektedir. Kamu sektrnde veri gvenlięi ve mahremiyeti konusundaki mevcut bilgileri derleyerek, arařtırmanın teorik erevesini oluřturmuř ve gelecekteki arařtırmalar iin bir temel saęlamıřtır. Mevcut literatrdeki bořlukların belirlenmesi, arařtırmanın katkı saęlayacaęı alanları netleřtirmekte ve bu konudaki bilgi birikimini artırmayı hedeflemektedir.

Mevcut literatrdeki bilgi eksiklikleri, bu alanda daha fazla arařtırma yapılması gereklilięini ortaya koymaktadır. Gelecek alıřmalar, zellikle kamu alıřanlarının eęitim programlarının etkinlięini ve veri gvenlięi politikalarının uygulanabilirlięini daha derinlemesine incelemelidir. Hem teorik hem de pratik aıdan bu konudaki bilgi birikimini artırmaya katkı saęlayabilir.

4.ARAŞTIRMA METODOLİJİSİ

Bu bölümde; araştırmanın yöntemi, örneklem seçimi, modeli ve hipotezi, veri toplama araçları ile süreci, veri analizi, kullanılan ölçekler ve araştırmanın sınırlılıklarına dair bilgiler sunulmaktadır.

4.1. Araştırma Yöntemi

Bu araştırma, kamu sektöründe çalışan personelin veri güvenliği ve mahremiyeti konusundaki farkındalık ve çözüm önerilerine yönelik tutumlarını değerlendirmeye odaklanmıştır. Araştırma, Türkiye genelinde İçişleri Bakanlığı bünyesindeki teknik hizmetler sınıfındaki personel ve Bilgi İşlem Şefliği/Müdürlüğü çalışanlarından oluşan bir örneklem ile gerçekleştirilmiştir. İki ana ölçek kullanılarak toplanan veriler, IBM Statistics SPSS 20 yazılımı ile analiz edilmiş ve sonuçlar detaylı bir şekilde incelenmiştir. Bu yöntem, araştırmanın güvenilir ve geçerli sonuçlar elde etmesini sağlamış ve kamu sektöründe veri güvenliği ve mahremiyeti alanında önemli bulgular sunmuştur.

4.2. Örneklem Seçimi

Araştırmanın ana kütlesi, Türkiye genelinde Valiliklerin Bilgi İşlem Müdürlüklerinde çalışan teknik hizmetler sınıfındaki personel (teknik personel) ile genel idare hizmetleri sınıfındaki personelden (müdür, şef, memur) oluşan toplam 482 kamu personelinin yer aldığı online resmi bir platfromdur. Türkiye genelinde 81 ilin Valiliği bulunduğu ve her ildeki personele ulaşmak güç olacağından araştırmanın ana kütlesi olarak İçişleri Bakanlığı Bilgi İşlem Grubu isimli Whatsapp grubu tercih edilmiştir. Örneklem yöntemi olarak ise, araştırmacının ulaşılabilir durumda olan katılımcılardan veri toplamasına imkan veren kolayda örneklem tekniği kullanılmıştır (Yağar ve Dökme, 2018).

Araştırmanın örneklem büyüklüğünü hesaplamak için aşağıdaki formül kullanılmıştır. Anakütle büyüklüğü bilindiği ve araştırma betimsel nitelikte anket verisine dayandığı için örneklem büyüklüğü Yamane'nin sadeleştirilmiş formülü ile belirlenmiştir (Yamane, 1973).

Formül: $n = N / (1 + N \cdot e^2)$

n: Gerekli örneklem büyüklüğü.

N: Ana kütle büyüklüğü (482).

e: Hata payı (%5).

Güven düzeyi: $e=0.05$ için zımnem %95 varsayımıyla kullanılır.

$$n = 482 / (1 + 482 \cdot 0.05^2) = 482 / (1 + 482 \cdot 0.0025) = 482 / 2.205 = 218.7 \approx 219$$

Bu örneklem, Türkiye'nin yedi coğrafi bölgesini temsil edecek şekilde Marmara, Ege, Akdeniz, İç Anadolu, Karadeniz, Doğu Anadolu ve Güneydoğu Anadolu bölgelerinde yer alan çeşitli kamu kurumlarında görev yapan personeli içermektedir. Hem kadın hem de erkek çalışanların temsil edildiği bu örneklem, veri güvenliği ve mahremiyeti konusundaki algıların cinsiyetler arasındaki farklılıkları da incelemeye olanak tanımaktadır. Ayrıca, yaş aralıkları açısından da çeşitlilik sağlanmıştır. Örneklem; 21-25, 26-30, 31-40 ve 41 ve üstü yaş gruplarından çalışanları içermektedir. Bu yaş grupları, farklı kariyer aşamalarındaki deneyimleri ve bakış açılarını yansıtmakta, bu da araştırmanın sonuçlarının daha kapsamlı ve zengin bir perspektiften değerlendirilmesine olanak tanımaktadır. Eğitim düzeyi açısından da katılımcıların çeşitliliği sağlanmıştır. Örneklem; lise, ön lisans, lisans ve yüksek lisans mezunu çalışanları içermektedir. Eğitim düzeyleri, katılımcıların veri güvenliği ve mahremiyeti konusundaki bilgi ve deneyimlerini farklılaştırmakta, böylelikle araştırmanın bulgularının daha derinlemesine analiz edilmesine katkı sağlamaktadır.

4.3. Araştırmanın Modeli ve Hipotezi

Bu araştırmanın modeli, kamu sektöründe veri güvenliği ve veri mahremiyeti konusundaki farkındalık ve çözüm önerilerini değerlendirmeyi amaçlayan iki ana ölçek üzerine kurulmuştur. Araştırma modeli, bu iki ölçeğin katılımcılar üzerindeki etkilerini ve bu konulardaki farkındalık düzeylerini analiz etmeyi hedeflemektedir.

Araştırmanın temel hipotezleri şu şekildedir:

H1: İçişleri Bakanlığında çalışan teknik hizmetler sınıfındaki personel ve Bilgi İşlem Şefliği/Müdürlüğünde görev yapan personelin veri güvenliği ve mahremiyeti farkındalık düzeyleri yüksektir.

H2: İçişleri Bakanlığında çalışan teknik hizmetler sınıfındaki personel ve Bilgi İşlem Şefliği/Müdürlüğünde görev yapan personelin veri güvenliği ve mahremiyeti konusundaki çözüm önerilerine yönelik düzeyleri yüksektir.

H3: İçişleri Bakanlığında teknik hizmetler sınıfında ve Bilgi İşlem birimlerinde görev yapan personelin veri güvenliği ve mahremiyet farkındalık düzeyleri cinsiyete göre farklılık göstermektedir.

H4: İçişleri Bakanlığında teknik hizmetler sınıfında ve Bilgi İşlem birimlerinde görev yapan personelin veri güvenliği ve mahremiyet çözüm önerileri düzeyleri cinsiyete göre farklılık göstermektedir.

H5: İçişleri Bakanlığında teknik hizmetler sınıfında ve Bilgi İşlem birimlerinde görev yapan personelin veri güvenliği ve mahremiyet farkındalık düzeyleri yaş aralığına göre farklılık göstermektedir.

H6: İçişleri Bakanlığında teknik hizmetler sınıfında ve Bilgi İşlem birimlerinde görev yapan personelin veri güvenliği ve mahremiyet çözüm önerileri düzeyleri yaş aralığına göre farklılık göstermektedir.

H7: İçişleri Bakanlığında teknik hizmetler sınıfında ve Bilgi İşlem birimlerinde görev yapan personelin veri güvenliği ve mahremiyet farkındalık düzeyleri eğitime göre farklılık göstermektedir.

H8: İçişleri Bakanlığında teknik hizmetler sınıfında ve Bilgi İşlem birimlerinde görev yapan personelin veri güvenliği ve mahremiyet çözüm önerileri düzeyleri eğitime göre farklılık göstermektedir.

H9: Veri güvenliği ve mahremiyeti farkındalığı değişkeni ile veri güvenliği ve mahremiyeti çözüm önerileri değişkeni arasında pozitif bir ilişki bulunmaktadır.

4.4. Veri Toplama Araçları

Veri toplama aracı olarak kullanılan anket, üç bölümden oluşmaktadır. Birinci ve ikinci bölümde, veri güvenliği ve veri mahremiyeti konularında katılımcıların bilgi düzeyi, farkındalık ve uygulamalarını ölçmeyi amaçlayan 20 soru bulunmaktadır. Bu sorular, Likert ölçeği kullanılarak yanıtlanmıştır. Likert ölçeği, katılımcıların belirli ifadelere katılım düzeylerini ölçmek amacıyla kullanılan beşli bir derecelendirme ölçeğidir (1: Hiçbir Zaman, 2: Nadiren, 3: Ara sıra, 4: Sık sık, 5: Her Zaman). Üçüncü bölümde ise, katılımcıların demografik bilgilerini içeren 6 soru yer almaktadır. Bu demografik sorular, katılımcıların yaş, cinsiyet, eğitim durumu, görev, hizmet yılı ve ikamet edilen coğrafi bölge bilgilerini içermektedir.

4.4.1. Veri Toplama Süreci

Anketler, Türkiye genelinde İçişleri Bakanlığında çalışan teknik hizmetler sınıfındaki personel ile Bilgi İşlem Şefliği/Müdürlüğünde görev yapan personele, dijital iletişim kanalları aracılığıyla uygulanmıştır. Veri toplama süreci, katılımcılara e-posta ve WhatsApp platformları üzerinden anket linkinin paylaşılması şeklinde gerçekleştirilmiştir. Bu dijital yöntem, geniş bir coğrafi alana yayılmış olan katılımcılara hızlı ve etkili bir şekilde ulaşmayı sağlamıştır.

İçişleri Bakanlığı Bilgi İşlem Grubu'nun WhatsApp grubuna gönderilen online anketler, katılımcıların kolayca erişebilmesi ve yanıtlaması için tasarlanmıştır. Bu platform, katılımcıların anketi mobil cihazları üzerinden kolayca erişebilmesini sağlamış ve katılım oranını artırmıştır. WhatsApp grubu üzerinden yapılan paylaşımlarda anketin amacı, kapsamı ve katılım koşulları hakkında bilgilendirme yapılmıştır. Ayrıca, anketin gönüllülük esasına dayandığı ve katılımcıların anonim olarak yanıt verebileceği belirtilmiştir.

Veri toplama sürecinde, katılımcıların araştırmanın etik kurallarına uygun olarak bilgilendirilmesi ve gönüllü katılımlarının sağlanması önemsenmiştir. Katılımcılara, anketin amacı ve kullanım alanları hakkında bilgi verilmiş, veri gizliliği ve anonimlik konusunda güvence sağlanmıştır. Katılımcılar, anketi istedikleri zaman bırakma hakkına sahip oldukları konusunda bilgilendirilmiştir.

Veri toplama süreci, belirlenen süre zarfında tamamlanmış olup, kullanılan dijital veri toplama yöntemi, coğrafi yönden geniş bir katılımcı kitlesine ulaşmayı ve veri toplama sürecinin hızlı ve verimli bir şekilde tamamlanmasını sağlamıştır.

4.4.2. Veri Analizi

Toplanan veriler, IBM İstatistik SPSS 20 programı ile analiz edilmiştir. Öncelikle katılımcılara ait demografik değişkenler frekans ve yüzde dağılımlarıyla incelenmiş, ardından veri güvenliği ve mahremiyeti konusundaki sorulara verilen yanıtlar betimleyici istatistiksel yöntemler aracılığıyla değerlendirilmiştir. Ölçeklere verilen yanıtların geçerlilik düzeyi incelendikten sonra Açıklayıcı Faktör Analizi uygulanmış, faktör analizi sonucunda ortaya çıkan alt boyutların güvenirlik değerleri hesaplanmıştır. Daha sonra katılımcıların ölçek ifadelerine verdikleri cevapların normallik dağılımı test edilerek, ilişkisel analizlerde kullanılacak istatistiksel yöntemlerin parametrik veya non-parametrik testler olmasına karar verilmiştir. İlişkisel analizler aşamasında ise; iki kategoriden oluşan değişkenlerde, normal dağılım göstermeyen veriler için parametrik olmayan istatistiksel yöntemlerden Mann Whitney U Testi, normal dağılım gösteren veriler için ise parametrik istatistiksel yöntemlerden Bağımsız Örneklem T Testi kullanılmıştır. Üç veya daha fazla kategorisi bulunan değişkenlerde, normal dağılım göstermeyen durumlarda Kruskal Wallis Testi, normal dağılım gösteren durumlarda Tek Yönlü Anova Testi kullanılmıştır. Üç veya daha fazla kategorili değişkenlerde, istatistiksel olarak anlamlı farklılık tespit edildiğinde, farkın hangi gruplardan kaynaklandığını belirlemek amacıyla uygun Post Hoc testleri gerçekleştirilmiştir. Son aşamada ölçeklerin alt boyutları arasındaki ilişkileri ortaya koymak için Spearman Korelasyon Analizi yapılmıştır. Tüm analizlerde anlamlılık (p) değeri 0,05 olarak kabul edilmiş ve p değerinin 0,05'ten küçük olduğu analiz sonuçları istatistiksel olarak anlamlı, p değerinin 0,05'ten büyük olduğu durumlar ise istatistiksel olarak anlamsız kabul edilmiştir.

4.4.3. Araştırma Ölçekleri

Veri Güvenliği ve Mahremiyeti Farkındalık Ölçeği;

Anketin birinci bölümünde yer alan "Veri Güvenliği ve Mahremiyeti Farkındalık Ölçeği", katılımcıların veri güvenliği ve mahremiyeti konusundaki farkındalık düzeylerini ölçmeyi amaçlamaktadır. Bu ölçek, literatürde veri güvenliği ve mahremiyeti farkındalığı ile politikalarına uyum konusunda yapılan çalışmalara dayandırılarak oluşturulmuştur (Siponen

vd., 2014). Ölçek, veri güvenliği ve mahremiyeti konusundaki bilgi düzeyi, güvenlik politikalarına uyum ve kişisel sorumluluk gibi alt boyutları kapsamaktadır.

Bu bölümdeki sorular, Likert tipi beşli derecelendirme ölçeği kullanılarak yanıtlanmıştır. Bu ölçek, katılımcıların belirli ifadelerle katılım düzeylerini "Hiçbir Zamandan"dan "Her Zaman"a kadar derecelendirmelerini sağlamaktadır.

Veri Güvenliği ve Mahremiyeti Çözüm Önerileri Ölçeği;

Anketin ikinci bölümünde yer alan "Veri Güvenliği ve Mahremiyeti Çözüm Önerileri Ölçeği", katılımcıların veri güvenliği ve mahremiyeti konusundaki çözüm önerilerine yönelik farkındalık ve kabul düzeylerini ölçmeyi hedeflemektedir. Bu ölçek, literatürdeki güvenlik politikaları ve motivasyon teorileri üzerine yapılan çalışmalara dayanarak geliştirilmiştir (Herath ve Rao, 2009). Ölçek, çözüm önerilerine yönelik farkındalık, uygulanabilirlik, etkinlik ve kabul gibi alt boyutları kapsamaktadır.

Bu bölümdeki sorular, veri güvenliği ve mahremiyeti konusundaki mevcut sorunlara yönelik çözüm önerilerini değerlendirmektedir. Katılımcılar, önerilen çözümlere yönelik tutumlarını ve bu çözümleri benimseme düzeylerini Likert tipi beşli derecelendirme ölçeği ile belirtmişlerdir. Verilerin analizi, betimleyici istatistikler kullanılarak gerçekleştirilmiştir.

4.5. Araştırmanın Sınırlılıkları

Her araştırma çalışmasında olduğu gibi, bu çalışmanın da belirli sınırlılıkları bulunmaktadır. Bu sınırlılıklar, araştırmanın bulgularının yorumlanmasında ve genellenmesinde dikkate alınması gereken önemli hususlardır.

Bu araştırmanın örneklemini, Türkiye genelinde İçişleri Bakanlığında çalışan teknik hizmetler sınıfındaki personel ile Bilgi İşlem Şefliği/Müdürlüğünde görev yapan personelden oluşmaktadır. Örneklem büyüklüğü olarak toplam 219 kişi belirlenmiştir. Ancak, bu örneklem tüm Bakanlıkları temsil etmemektedir. Dolayısıyla, elde edilen bulguların genellenebilirliği sınırlıdır. Araştırmanın bulguları, yalnızca bu örneklem grubuna yönelik çıkarımlar yapmaya olanak tanımaktadır ve diğer kamu kurumlarındaki çalışanların veri güvenliği ve mahremiyeti konusundaki tutumlarını tam anlamıyla yansıtmayabilir.

Veri toplama yöntemi olarak anket kullanılmış ve anketler WhatsApp aracılığıyla katılımcılara dağıtılmıştır. Bu yöntem, katılımcıların anketi kendi başlarına doldurmalarını gerektirmiştir. Bu durum, katılımcıların anket sorularını yanlış anlamaları veya eksik cevaplamaları gibi sorunlara yol açabilir. Ayrıca, dijital platformlar üzerinden anket dağıtımı, bazı katılımcıların ankete erişiminde teknik zorluklar yaşamasına neden olmuş olabilir. Bu sınırlılık, verilerin doğruluğunu ve tamlığını etkileyebilir.

Araştırmada kullanılan ölçeklerin güvenirlik ve geçerlilik değerleri, farklı örneklem ve farklı bağlamlarda değişiklik gösterebilir. Ölçeklerin güvenirlik ve geçerliliği, araştırmanın bulgularının tutarlılığına ve güvenilirliğine doğrudan etki edebilir.



5.BULGULAR VE TARTIŞMA

Bu bölümde; toplanan verilerin analizi sonucunda elde edilen bulgular sunulmakta, bu bulgular literatürdeki çalışmalar ve teorik çerçeve ışığında tartışılarak yorumlanmaktadır.

5.1. Tanımlayıcı Bulgular

Bu araştırma kapsamında, Türkiye genelinde İçişleri Bakanlığında çalışan teknik hizmetler sınıfındaki personel ile Bilgi İşlem Şefliği/Müdürlüğünde çalışan toplam 219 katılımcıdan elde edilen veriler, frekans analizi yöntemiyle değerlendirilmiş ve elde edilen bulgular Tablo 5.1.'de sunulmuştur.

Tablo 5.1: Demografik bilgilerin tanımlayıcı bulguları

Demografik Bilgiler	Kategoriler	Sayı (n)	Oran (%)
Cinsiyet	Kadın	76	34,7
	Erkek	143	65,3
	Toplam	219	100,0
Yaş	21-25 Yaş Aralığı	14	6,4
	26-30 Yaş Aralığı	25	11,4
	31-40 Yaş Aralığı	131	59,8
	41 ve Üstü	49	22,4
	Toplam	219	100,0
Eğitim Durumu	Lise	10	4,6
	Önlisans	23	10,5
	Lisans	159	72,6
	Yüksek Lisans	27	12,3
	Toplam	219	100,0

Tablo 5.1: (devam ediyor)

Görev Süresi	0-5 Yıl Arası	30	13,7
	5-10 Yıl Arası	88	40,2
	10-15 Yıl Arası	69	31,5
	15 Yıl ve Üstü	32	14,6
	Toplam	219	100,0
Görev	Teknik Personel	165	75,3
	Memur	44	20,1
	Müdür	7	3,2
	Şef	3	1,4
	Toplam	219	100,0
Coğrafi Bölge	Marmara	34	15,5
	Ege	11	5,0
	Akdeniz	22	10,0
	İç Anadolu	25	11,4
	Doğu Anadolu	58	26,5
	Güneydoğu Anadolu	20	9,1
	Toplam	219	100,0

Tablo 5.1'e göre araştırmaya katılan 219 kişinin cinsiyet dağılımında, erkek katılımcıların sayısı 143, kadın katılımcıların sayısı ise 76 olarak belirlenmiştir. Erkek katılımcılar, toplamın %65,3'ünü oluştururken, kadın katılımcılar %34,7'lik bir oranla temsil edilmektedir. Bu durum, teknik hizmetler ve bilgi işlem alanlarında erkeklerin daha fazla istihdam edildiğini veya bu alanlarda çalışan erkeklerin anketi yanıtlama konusunda kadın katılımcılara kıyasla fazla istekli olabileceğini göstermektedir.

Araştırmaya katılan 219 kişinin yaş dağılımında, 21-25 yaş aralığında 14 kişi (%6,4), 26-30 yaş aralığında 25 kişi (%11,4), 31-40 yaş aralığında 131 kişi (%59,8) ve 41 ve üstü yaş aralığında 49 kişi (%22,4) bulunmaktadır. Bu sonuçlar, katılımcıların büyük çoğunluğunun (%59,8) 31-40 yaş aralığında olduğunu göstermektedir. 41 ve üstü yaş grubunun da %22,4 ile kayda değer bir paya sahip olduğu görülmektedir.

Araştırmaya katılan 219 kişinin görev süresi dağılımında, 0-5 yıl aralığında 30 kişi (%13,7), 5-10 yıl aralığında 88 kişi (%40,2), 10-15 yıl aralığında 69 kişi (%31,5) ve 15 yıl ve üstü görev süresine sahip 32 kişi (%14,6) bulunmaktadır. Bu sonuçlar, katılımcıların çoğunluğunun (%40,2) 5-10 yıl aralığında görev yaptığını göstermektedir. 10-15 yıl aralığında görev yapan katılımcılar %31,5’lik bir oranla ikinci sırada yer almaktadır.

Araştırmaya katılan 219 kişinin görev dağılımında, teknik personel olarak görev yapan 165 kişi (%75,3), memur olarak görev yapan 44 kişi (%20,1), müdür pozisyonunda 7 kişi (%3,2) ve şef pozisyonunda 3 kişi (%1,4) bulunmaktadır. Bu sonuçlar, katılımcıların büyük çoğunluğunun (%75,3) teknik personel olduğunu göstermektedir. Memur olarak görev yapan katılımcılar %20,1 ile ikinci sırada yer alırken, müdür ve şef pozisyonlarında görev yapan katılımcılar sırasıyla %3,2 ve %1,4 oranında temsil edilmektedir.

Araştırmaya katılan 219 kişinin eğitim durumu dağılımında, lise mezunu 10 kişi (%4,6), önlisans mezunu 23 kişi (%10,5), lisans mezunu 159 kişi (%72,6) ve yüksek lisans mezunu 27 kişi (%12,3) bulunmaktadır. Bu sonuçlar, katılımcıların büyük çoğunluğunun (%72,6) lisans mezunu olduğunu göstermektedir. Yüksek lisans mezunları %12,3 ve önlisans mezunları %10,5 oranında temsil edilirken, lise mezunları %4,6 ile en düşük oranı oluşturmaktadır. Bu dağılım, katılımcıların genel olarak yüksek bir eğitim seviyesine sahip olduklarını ve bunun veri güvenliği ve mahremiyeti konularındaki farkındalıklarını artırabileceğini düşündürmektedir.

Araştırmaya katılan 219 kişinin coğrafi bölge dağılımında, Marmara 34 kişi (%15,5), Ege 11 kişi (%5,0), Akdeniz 22 kişi (%10,0), Karadeniz 49 kişi (%22,4), İç Anadolu 25 kişi (%11,4), Doğu Anadolu 58 kişi (%26,5) ve Güneydoğu Anadolu 20 kişi (%9,1) ile temsil edilmektedir. Dağılım incelendiğinde, en yüksek katılımın Doğu Anadolu Bölgesi’nden (%26,5) geldiği, bunu Karadeniz (%22,4) ve Marmara (%15,5) bölgelerinin izlediği görülmektedir.

Veri Güvenliği ve Mahremiyeti Farkındalık Ölçeği (VGMFÖ) ve Veri Güvenliği ve Mahremiyeti Çözüm Önerileri Ölçeğine (VGMÇÖÖ) ilişkin tanımlayıcı bulgular aşağıdaki Tablo 5.2’de gösterilmiştir.

Tablo 5.2: Ölçeklere ait maddelerin tanımlayıcı bulguları

Ölçeklere Ait Maddeler	min	max	$\bar{x}$	ss	n
VGMFÖ					
1.1.Veri güvenliği ve mahremiyeti hakkında bilginiz var mı?	1	5	4,35	,995	219
1.2.Çalıştığınız Kurumda veri güvenliği ve mahremiyeti politikalarını biliyor ve riayet ediyor musunuz?	1	5	4,40	,935	219
1.3.Çalıştığınız kurumda verilerinizin güvenliğinden ve mahremiyetinden endişe duyuyor musunuz?	1	5	2,14	1,068	219
1.4.Çalıştığınız kurumda veri güvenliği ve mahremiyeti ile ilgili sorunların sıklıkla görüldüğünü düşünüyor musunuz?	1	5	2,29	1,209	219
1.5.Çalıştığınız kurumda veri güvenliği ve mahremiyeti ile ilgili hiç eğitim aldınız mı?	1	5	2,90	1,135	219
1.6.Çalıştığınız kurumda veri güvenliği ve mahremiyeti ihlallerinden herhangi birine (phishing,bilgisayar virüsleri, kötü amaçlı yazılımlar vb.) hiç tanık oldunuz mu?	1	5	2,09	1,078	219
1.7.Kurumunuzda veri güvenliği ve mahremiyeti politikaları ve prosedürleri yeterli mi?	1	5	3,79	1,080	219
1.8.Kurumunuzda kullandığınız sistem veri güvenliği ve mahremiyeti açısından güncel mi?	1	5	4,09	,994	219
1.9.Kurumunuz veri mahremiyeti ile ilgili yasal düzenlemelere tam uyum sağlıyor mu?	1	5	4,26	,996	219
1.10.Kurumunuzda veri güvenliği ve mahremiyeti ile ilgili alınan önlemler sizi tatmin ediyor mu?	1	5	3,93	1,075	219
VGMÇÖÖ					
2.1.Kamu sektöründe veri güvenliği ve mahremiyeti sorunlarını çözmenin önemli olduğunu düşünüyor musunuz?	1	5	4,73	,701	219
2.2.Verit güvenliği ve mahremiyeti ile ilgili kapsamlı eğitim ve farkındalık programları oluşturmaının önemini nasıl değerlendiriyorsunuz?	1	5	4,50	,815	219
2.3.Verit güvenliğiyle ilgili yaşanan sorunlar için çözüm önerileri geliştirilmesi konusunda katkıda bulunuyor musunuz?	1	5	3,26	1,180	219
2.4.Verit güvenliği konusunda çalışanların önerileri dikkate alınıyor mu?	1	5	3,48	1,110	219
2.5.Verit güvenliğiyle ilgili sorun yaşandığında kurum içinde açık bir şekilde tartışılıyor mu?	1	5	3,37	1,269	219

Tablo 5.2: (devam ediyor)

2.6.Teknolojik çözümlerle veri güvenliği ve mahremiyeti artırılabilir mi?	1	5	4,38	,883	219
2.7.Güvenlik duvarları ve antivirüs yazılımlar kullanmak veri güvenliği ve mahremiyetini korumak için yeterli midir?	1	5	3,54	,987	219
2.8.Kamu sektöründeki veri güvenliği ve mahremiyeti ile ilgili sorunların çözümüne katkıda bulunmak için özel sektör şirketler ile işbirliği yapılmalı mıdır?	1	5	3,55	1,285	219
2.9.Kurumunuzda veri güvenliği ile ilgili önlemler alındığında bu önlemler tüm çalışanlara etkili bir şekilde duyuruluyor mu?	1	5	3,79	1,117	219
2.10.Kurumunuzda veri güvenliği ve mahremiyeti ile ilgili sorunlarının çözümü için yeterli ödenek ayrılıyor mu?	1	5	3,50	1,139	219

min: Minimum, max: Maksimum, $\bar{x}$: Ortalama, ss: Standart Sapma, n: Sayı

Tablo 5.2’de yer alan bulgulara göre, Veri Güvenliği ve Mahremiyeti Farkındalık Ölçeği (VGMFÖ) için maddelerin tamamı 1 ile 5 arasında puanlanmış, genel ortalama 3,42 olarak hesaplanmıştır. (n=219). Bu değer, yanıtların genel olarak “ara sıra” bandında kümelendiğine işaret etmektedir. Ölçekte en yüksek ortalamaya sahip madde 1.2.’dir ve katılımcıların kurum politikalarını bilme ve riayet etme konusunda güçlü bir eğilime sahip olduğunu göstermektedir. Bunu 1.1. ve 1.9. maddeleri izlemektedir. En düşük ortalamaya sahip madde ise 1.6.’dır ve veri ihlallerine tanıklık etme sıklığının görece düşük algılandığını düşündürmektedir. Benzer şekilde 1.3. ve 1.4. maddelerindeki düşük ortalamalar, endişe düzeyi ve sorunların sıklığı algısının sınırlı olduğunu ortaya koymaktadır. Eğitimle ilgili 1.5. maddesinin ortalaması 2,90 olup, katılımcıların eğitim alma deneyimlerinin orta düzeyin biraz altında kaldığı görülmektedir. Dağılım ölçütleri açısından, standart sapmanın yüksek olduğu maddeler katılımcılar arasında görüş ayrılıklarına işaret ederken, 1.2.’deki daha düşük standart sapma bu konuda daha yüksek bir fikir birliğine işaret etmektedir.

Veri Güvenliği ve Mahremiyeti Çözüm Odaklı Ölçek (VGMÇÖÖ) için ise genel ortalama 3,81’dir (n=219) ve bu sonuç, katılımcıların “sık sık” yöneliminde kümelendiğini göstermektedir. En yüksek ortalamaya sahip madde 2.1.’dir ve kamu sektöründe veri güvenliği ve mahremiyeti sorunlarını çözmenin önemine güçlü bir vurgu yapıldığını göstermektedir. Bunu 2.2. ve 2.6. maddeleri izlemekte; kapsamlı eğitim–farkındalık programları ile teknolojik çözümlerin önemsendiğini göstermektedir. En düşük ortalama 2.3. maddesindedir; bu durum, bireysel düzeyde çözüm önerilerine katkı sağlama davranışının

daha sınırlı kaldığını düşündürmektedir. Kurum içi süreçlere ilişkin maddelerden 2.9. ve 2.5. duyuru ve tartışma pratiklerinin orta düzeyde algılandığını ortaya koymaktadır. 2.8. maddesinde ve 2.5. maddesinde yüksek standart sapma değerleri olduğu yine katılımcılar arasında görüş ayrılıklarına, 2.1. maddesinde ise katılımcılar arasında güçlü bir mutabakat olduğuna işaret etmektedir.

Genel olarak sonuçlar, katılımcıların bilgi, politika uyumu ve konunun stratejik önemine ilişkin yüksek farkındalığa sahip olduklarını; buna karşılık olay tanıklığı ve bireysel çözüm katkısı gibi alanlarda daha düşük düzeyde yanıtlar verdiklerini göstermektedir. Bu bulgular, politika geliştirme ve eğitim programları tasarlamada öncelik alanlarının belirlenmesine katkı sağlayabilir.

5.2. Geçerlilik Analizi

Yeniden yapılandırılan/yeniden geliştirilen ölçek için temel kavramsal boyutları ortaya koymak amacıyla AFA uygulanmıştır; bu yaklaşım, maddelerin hangi latent yapılarla ilişkili olduğunu keşfetmeye ve ölçeğin özelleştirilmiş geçerlilik ve güvenilirlik dinamiklerini belirlemeye olanak tanır.

Açımlayıcı Faktör Analizi (AFA), bir veri setinde gözlemlenen değişkenler arasındaki ilişkileri anlamak ve bu değişkenleri daha az sayıda faktör veya boyut altında gruplamak amacıyla kullanılan istatistiksel bir yöntemdir. Bu analiz, özellikle sosyal bilimler, psikoloji ve eğitim alanlarında yaygın olarak kullanılmaktadır.

5.2.1. Veri Güvenliği ve Mahremiyeti Farkındalık Ölçeği Geçerlilik Analizi Bulguları

Veri güvenliği ve mahremiyeti farkındalık ölçeği (VGMFÖ) için alt boyut sayısı belirtilmeden yapılan AFA analizinde ilk olarak temel bileşen analizi (PCA) ve quartimax teknikleri uygulanarak veri setinin ana bileşen yapısı incelenmiş, ardından bu temel yapıya uygun olarak temel eksen faktörleme (PAF) ve doğrudan eğik döndürme (direct oblimin) teknikleriyle faktörler elde edilmiştir. Temel eksen faktörleme sosyal bilimlerde gözlenen değişkenlerin daha az sayıda altta yatan faktörden etkilendiğini varsaydığı için, doğrudan eğik döndürme yönteminin ise faktörler arasında bir ilişki olduğu varsayımıyla seçilmiştir (Memnun, 2012). Yükler PCA ve direct oblimin teknikleriyle elde edilen boyutlarda daha netleşmiş ve bu teknik ile gerçekliğe daha yakın bir faktör yapısı ortaya konmuştur. Bu

adımlar, ölçeğin yapısal geçerliliğini veri odaklı biçimde keşfetmeyi ve aşırı yüklenen maddeleri ayırt etmeyi hedeflemiştir. Principal Axis Factoring çıkarımı ve Direct Oblimin rotasyonla iki faktörlü bir yapı elde edilmiştir.

KMO (Kaiser-Meyer-Olkin) ölçümü ve Bartlett's Testi ile birlikte yapılan AFA, veri setinin faktör analizi için uygunluğunu test etmiş ve faktör yükleri aracılığıyla ölçek maddelerinin hangi faktörleri temsil ettiğini ortaya koymuştur. **Kaiser-Meyer-Olkin** (KMO) örneklem yeterliliği değeri **0,809** olarak bulunmuştur. Bu değer 0,50'nin üzerinde olduğundan örneklem büyüklüğünün yeterli olduğunu ve 0,80-0,90 arası bir değer Field (2009) tarafından "harika" kategorisinde yer almaktadır. Bartlett's Testi sonucunda $\chi^2(45):1029,955$ ve p-değeri 0,000 ($p<0,05$) olarak hesaplanmıştır. Bu sonuç, veri setinin faktör analizi için uygun olduğunu ve değişkenler arasında anlamlı bir ilişki olduğunu ortaya koymaktadır. AFA sonucunda, 10 maddeden oluşan VGMFÖ'nün 2 alt boyutlu (faktörlü) bir yapıdan oluştuğu bu 2 faktörün toplam varyansın %50,641'ini açıkladığı tespit edilmiştir. Buna göre VGMFÖ'nün geçerli özellik gösterdiği sonucuna varılmıştır. Ayrıca 1.alt boyut varyansının %38,709'unu 2.alt boyut ise %11,932'sini açıklamaktadır. Tablo 5.3'de maddelerin faktörlere göre dağılımı ve faktör yükleri verilmiştir.

Tablo 5.3: VGMFÖ geçerlilik analizi bulguları

Maddeler	1.Alt Boyut Kurumsal Uygulama/Farkındalık	2.Alt Boyut Kurumsal Risk Farkındalığı
B1S1	,567	
B1S2	,827	
B1S3		,673
B1S4		,551
B1S5	,634	
B1S6		,566
B1S7	,615	
B1S8	,641	
B1S9	,787	
B1S10	,777	-0,326
Öz Değer	4,276	1,781
Açıkladığı Varyans	38,709	11,932

Maddeler	1.Alt Boyut Kurumsal Uygulama/Farkındalık	2.Alt Boyut Kurumsal Risk Farkındalığı
Açıklanan Toplam Varyans		50,641

Tablo 5.3’de görüldüğü üzere alt boyutlardan ilki 7 maddeden (B1S1, B1S2, B1S5, B1S7, B1S8, B1S9, B1S10), ikincisi ise 3 maddeden (B1S3, B1S4, B1S6) oluşmaktadır. Faktör yükleri en düşük 0,566 olarak tespit edilmiştir. Dolayısıyla 0,40 ve üzeri faktör yükleri ideal kabul edildiği için (Field, 2009) maddelerin faktörlere önemli katkı yaptıkları değerlendirilmiştir. B1S10’da 2.alt boyutta küçük bir çapraz yükü (-0,326) olsa da ana yüklerle fark büyük olduğundan madde korunmuştur. Alt boyutlar sırasıyla Kurumsal Uygulama/Farkındalık ve Kurumsal Risk Farkındalığı olarak adlandırılmıştır.

5.2.2. Veri Güvenliği Ve Mahremiyeti Çözüm Önerileri Ölçeği Geçerlilik Analizi Bulguları

Veri Güvenliği ve Mahremiyeti Çözüm Önerileri Ölçeği (VGMÇÖ) veri setinin faktör analizi için KMO (Kaiser-Meyer-Olkin) ölçümü ve Bartlett's Testi ile uygunluğunu değerlendirmiştir. Kaiser-Meyer-Olkin (KMO) örneklem yeterliliği değeri 0,809 olarak belirlenmiştir. Bu değer, 0,50’nin üzerinde olduğu için örneklem büyüklüğü yeterlidir.

Bartlett's Testi sonuçlarına göre $\chi^2(45):874,948$ ve p-değeri 0,000 ($p<0,05$) olarak hesaplanmıştır. Bu bulgu, veri setinin faktör analizi için uygun olduğunu ve değişkenler arasında anlamlı bir ilişki bulunduğunu açıkça ortaya koymaktadır. Bu sonuçlar, ölçeğin maddelerinin birbiriyle ilişkilendirilerek, faktör yapısının belirlenmesine olanak tanımakta ve araştırmanın geçerliliğini artırmaktadır.

VGMÇÖÖ için PAF çıkarımı ve direct oblimin rotasyonla iki faktörlü yapı elde edilmiştir. AFA sonucunda, 10 maddeden oluşan VGMÇÖÖ’nün 2 faktörlü bir yapıdan oluştuğu tespit edilmiştir. Ancak B2S8 ikinci alt boyutta faktör yükünün 0,385 olması ve faktör yükünün 0,40’dan küçük olması sebebiyle bu madde çıkarılmıştır. Analiz sonucu elde edilen toplam 9 maddeden oluşan iki alt boyutun toplam varyansın %52,779’unu açıkladığı tespit edilmiştir. Buna göre VGMÇÖÖ’nün geçerli özellik gösterdiği sonucuna varılmıştır. Ayrıca

1.alt boyutun varyansın %48,207'sini 2.alt boyutun ise %14,251'ini açıklamaktadır. Tablo 5.4'de maddelerin faktörlere göre dağılımı ve faktör yükleri verilmiştir.

Tablo 5.4: VGMÇÖÖ geçerlilik analizi bulguları

Maddeler	1.Alt Boyut Kurumsal Çözüm Süreçleri	2.Alt Boyut Stratejik Öncelik
B2S1		,900
B2S2		,797
B2S3	,711	
B2S4	,758	
B2S5	,717	
B2S6		,599
B2S7	,582	
B2S9	,611	
B2S10	,534	
Öz Değer	4,339	1,283
Açıkladığı Varyans	48,207	14,251
Açıklanan Toplam Varyans	52,779	

Tablo 5.4'de görüldüğü üzere alt boyutlardan ilki 6 maddeden (B2S3, B2S4, B2S5, B2S7, B1S9, B2S10), ikincisi ise 3 maddeden (B2S1, B1S2, B2S6) oluşmaktadır. Faktör yükleri en düşük 0,534 olarak tespit edilmiştir. Alt boyutlar sırasıyla Kurumsal Çözüm Süreçleri ve Stratejik Öncelik olarak adlandırılmıştır.

5.3. Güvenirlik Analizi

Cronbach's Alpha, bir ölçeğin iç tutarlılığını ölçmek için kullanılan bir istatistiksel yöntemdir. Bu değerler, George ve Mallery (2003) tarafından önerilen standartlara dayanmaktadır. Ayrıca, Nunnally ve Bernstein (1994) tarafından da benzer sınıflandırmalar yapılmıştır.

Alpha değerleri mükemmel (0,90 ve üzeri) ve çok iyi (0,80 - 0,89) değerleri, ölçeğin yüksek güvenilirliğe sahip olduğunu gösterir. Bu değerler, anketin tutarlı sonuçlar ürettiğini ve

katılımcıların algılarını doğru bir şekilde yansıttığını belirtir. Kabul edilebilir (0,70 - 0,79) ve sınırda (0,60 - 0,69) değerleri ölçeğin yeterli güvenilirlik sunduğunu ifade eder, ancak geliştirme için daha fazla çalışma yapılması faydalı olabilir. Daha düşük değerler ise ölçeğin güvenilirliğinde sorunlar olduğunu gösterir. Bu durumda, ölçek maddelerinin gözden geçirilmesi ve gerekirse yeniden tasarlanması önerilir.

5.3.1. Veri Güvenliği ve Mahremiyeti Farkındalık Ölçeğine dair Güvenirlik Analizi

VGMFÖ'ye uygulanan AFA sonucunda belirlenen alt boyutlara ilişkin güvenirlilik analizi bulguları Tablo 5.5'de sunulmuştur.

Tablo 5.5: VGMFÖ güvenirlilik analizi bulguları

Güvenirlilik Analizi Sonuçları		
Alt Boyutlar	Cronbach's Alpha (α)	Madde Sayısı
Kurumsal Uygulama/Farkındalık	,868	7
Kurumsal Risk Farkındalığı	,649	3

Tablo 5.5'de güvenirlilik düzeyi olan Cronbach's Alpha (α) değerlerine bakıldığında; VGMFÖ'nün 1.alt boyutu olan Kurumsal Uygulama/Farkındalığın güvenirlilik değerinin 0,868 olduğu ve bu değer çok iyi düzeyde ($0.80 < \alpha < 0.90$) olduğu, 2. alt boyutu olan Kurumsal Risk Farkındalığın güvenirlilik değerinin ise 0,649 olduğu ve bu değer sınırda düzeyde ($0.50 < \alpha < 0.60$) olduğu tespit edilmiştir. KUF güvenirlilik değerinin sınırda bir değer çıkması, mevcut madde sayısının (3) az olmasından kaynaklandığından mevcut yapı korunmuştur.

5.3.2. Veri Güvenliği ve Mahremiyeti Çözüm Önerileri Ölçeğine Dair Güvenirlilik Analizi

VGMÇÖÖ'ye uygulanan AFA sonucunda belirlenen alt boyutlara ilişkin güvenirlilik analizi bulguları Tablo 5.6'da sunulmuştur.

Tablo 5.6: VGMÇÖÖ güvenirlik analizi bulguları

Güvenirlik Analizi Sonuçları		
Alt Boyutlar	Cronbach's Alpha (α)	Madde Sayısı
Kurumsal Çözüm Süreçleri	,837	6
Stratejik Öncelik	,817	3

Tablo 5.6’da güvenirlik düzeyi olan Cronbach’s Alpha (α) değerlerine bakıldığında; VGMÇÖÖ’nün 1.alt boyutu olan Kurumsal Çözüm Süreçlerinin güvenirlik değerinin 0,837 olduğu ve 2.alt boyutu olan Stratejik Önceliğin güvenirlik değerinin ise 0,817 olduğu dolayısıyla her iki alt boyutunda güvenirliği çok iyi düzeyde ($0.80 < \alpha < 0.90$) olduğu tespit edilmiştir.

Elde edilen bulgular, bu ölçeklerin ve ölçeklerin alt boyutlarının güvenilir ve geçerli ölçüm araçları olduğu belirlenmiştir. Bu nedenle, her iki ölçeğin de gelecekteki araştırmalarda kullanılabilirliği, veri güvenliği stratejilerinin oluşturulması ve uygulanması açısından büyük önem taşımaktadır.

5.4. Normallik Bulguları

Bir araştırmada yapılacak analizlerin belirlenmesi için, ölçek verilerinin normallik durumu dikkate alınarak analizler gerçekleştirilir. Veri Güvenliği ve Mahremiyeti Farkındalık Ölçeğinin (VGMFÖ) iki alt boyutu olan Kurumsal Uygulama/Farkındalık (KUF) ve Kurumsal Risk Farkındalığının (KRF) ile Veri Güvenliği ve Mahremiyeti Çözüm Önerileri Ölçeğinin (VGMÇÖÖ) iki alt boyutu olan Kurumsal Çözüm Süreçleri (KÇS) ve Stratejik Önceliğin (SÖ) normallik değerleri, Tablo 5.7’de sunulmuştur.

Tablo 5.7: Alt boyutların normallik testi bulguları

Normallik Testi				
Ölçeklerin Alt Boyutları	Kolmogorov-Smirnov p	Shapiro Wilk p	Çarpıklık (Skewness)	Basıklık (Kurtosis)
KUF	,000	,000	-1,115	1,279
KRF	,000	,000	,732	,631
KÇS	,001	,000	-,432	,007
SÖ	,000	,000	-2,801	10,006

p: %95 güven aralığında anlamlılık değeri

Yapılan normallik analizi incelendiğinde; Kolmogorov-Smirnov ve Shapiro-Wilk testlerinin p-değerleri (Anlamlılık) **0.000** olarak bulunmuş ve verilerin normal dağılıma uygun olmadığı görülmüştür ($p < 0,05$). Bununla birlikte, yanıtların dağılımına karar verirken çarpıklık (skewness) ve basıklık (kurtosis) göstergeleri de dikkate alınmalıdır. George ve Mallery (2010)'e göre çarpıklık ve basıklık değerlerinin +2,0 ile -2,0 aralığında kalması durumunda dağılımın normal kabul edilebileceği ifade edilmektedir. Bu ölçüte göre KUF (çarpıklık: 1,115; basıklık: 1,279), KRF (çarpıklık: ,732; basıklık: ,631) ve KÇS (çarpıklık: -,432; basıklık: ,007) alt boyutlarının dağılımı kabul edilebilir sınırlar içindedir. Buna karşılık SÖ alt boyutu belirgin negatif çarpıklık (çarpıklık: -2,801) ve yüksek basıklık (basıklık: 10,006) sergilediğinden normal dağılımdan anlamlı sapma göstermektedir. Bu bulgular ışığında, SÖ alt boyutu normal dağılım varsayımı sağlanmazken, KUF, KRF ve KÇS alt boyutlarda yanıtların normal dağıldığı görülmektedir.

5.5. İlişkisel Bulgular

İlişkisel analizler kapsamında, KUF, KRF ve KÇS alt boyutlarına ilişkin verilen yanıtların normal dağılım gösterdiği belirlenmiş ve bu nedenle parametrik istatistiksel yöntemler kullanılmıştır. SÖ alt boyutuna verilen yanıtların normal dağılım göstermemesi nedeniyle parametrik olmayan yöntemler tercih edilmiştir.

5.5.1. Cinsiyet Değişkenine Göre Farklılık Analizi Bulguları

Cinsiyet değişkeni ile KUF, KRF ve KÇS alt boyutlarına verilen yanıtlar arasındaki ilişkiyi incelemek için yapılan Bağımsız Örneklem T Testi bulguları Tablo 5.8.'de sunulmuştur.

Tablo 5.8: Cinsiyet ile KUF, KRF ve KÇS alt boyutları arasındaki bağımsız örneklem T testi bulguları

Ölçeklerin Alt Boyutları	Cinsiyet	n	$\bar{x}$	ss	p
KUF	Kadın	76	3,9944	,62616	,066
	Erkek	143	3,9421	,83871	
KRF	Kadın	76	1,9605	,84322	,926
	Erkek	143	2,2844	,84842	
KÇS	Kadın	76	3,6096	,82082	,985
	Erkek	143	3,4277	,85249	

n: Sayı, $\bar{x}$: Ortalama, ss: Standart Sapma, p: %95 güven aralığında anlamlılık değeri

Tablo 5.8'e göre; cinsiyet değişkenine göre alt boyut ortalamaları karşılaştırıldığında, KUF, KRF ve KÇS için elde edilen p değerleri sırasıyla (0,066), (0,926) ve (0,985) olup istatistiksel olarak anlamlı bir fark bulunmamıştır ($p>0,05$). Bu sonuç, kadın ve erkek katılımcıların ilgili alt boyutlardaki ortalama puanlarının birbirine yakın seyrettiğini göstermektedir.

Bununla birlikte, ortalama değerler incelendiğinde bazı eğilimler göze çarpmaktadır. KUF alt boyutunda kadınların ortalaması, erkeklere göre çok az daha yüksektir. KRF alt boyutunda erkeklerin ortalaması, kadınlardan yüksektir. KÇS alt boyutunda ise kadınların ortalaması, erkeklere kıyasla bir miktar daha yüksektir. Ancak bu farkların hiçbiri istatistiksel olarak anlamlılık eşiğini geçmemektedir. Dolayısıyla, cinsiyete bağlı belirgin ve

güvenilir bir farklılaşmadan bahsetmek mümkün değildir; gözlenen küçük ortalama farkları örnekleme dayalı dalgalanmalar kapsamında yorumlanmıştır.

Cinsiyet değişkeni ile SÖ alt boyutuna verilen yanıtlar arasındaki ilişkiyi incelemek amacıyla yapılan Mann Whitney U testi bulguları Tablo 5.9’da sunulmuştur.

Tablo 5.9: Cinsiyet ile SÖ alt boyutu arasındaki Mann Whitney U testi bulguları

Ölçeklerin Alt Boyutları	Cinsiyet	n	sıra $\bar{x}$	p
SÖ	Kadın	76	123,70	,014
	Erkek	143	102,72	

n: Sayı, Sıra $\bar{x}$: sıra Ortalaması, p: %95 güven aralığında anlamlılık değeri

Tablo 5.9’a göre; SÖ alt boyutunda cinsiyet grupları Mann Whitney U testiyle karşılaştırıldığında istatistiksel olarak anlamlı bir farklılık gözlenmiştir ($p<0,05$). Kadınların sıra ortalaması 123,70 olup, bu değer erkek grubuna kıyasla daha yüksektir; dolayısıyla kadın katılımcıların SÖ puanlarının görece daha yüksek olduğunu göstermektedir.

5.5.2. Yaş Aralığı Değişkenine Göre Farklılık Analizi Bulguları

Yaş aralığı değişkeni ile KUF, KRF ve KÇS alt boyutlarına verilen yanıtlar arasındaki ilişkiyi incelemek amacıyla yapılan Tek Yönlü Anova Testi bulguları Tablo 5.10’da sunulmuştur.

Tablo 5.10: Yaş aralığı ile KUF, KRF ve KÇS alt boyutları arasındaki Tek Yönlü Anova testi bulguları

Ölçeklerin Alt Boyutları	Yaş Aralığı	n	$\bar{x}$	ss	p	Post Hoc (Games Howell)
KUF	21- 25	14	3,2857	1,04529	,002	
	26- 30	25	3,7771	1,09115		
	31- 40	131	4,0513	,70612		

Tablo 5.10: (devam ediyor)

KUF	41 ve üstü	49	4,0029	,52932	,002	
KRF	21- 25	14	2,3095	,68518	,915	
	26- 30	25	2,1733	,76449		
	31- 40	131	2,1756	,89474		
	41 ve üstü	49	2,1224	,86788		
KÇS	21- 25	14	2,7619	,80254	,000	31-40>21-25,
	26- 30	25	2,4600	1,12555		
	31- 40	131	3,6590	,78279		31-40>41 ve
	41 ve üstü	49	3,2653	,69632		üstü

n: Sayı, $\bar{x}$: Ortalama, ss: Standart Sapma, p: %95 güven aralığında anlamlılık değeri

Tablo 5.10'a göre; yaş aralığı değişkeni ile alt boyutlar karşılaştırıldığında, KÇS'de gruplar arası farklılaşma istatistiksel olarak anlamlıdır. Games-Howell ikili karşılaştırmaları, 31–40 yaş grubunun ortalamasının 21–25 ve 41 ve üstü gruplarından anlamlı düzeyde yüksek olduğunu göstermiştir (31–40 > 21–25 p:0,005; 31–40 > 41 ve üstü p:0,008). Buna karşılık, KUF için klasik tek yönlü ANOVA p=,002 olsa da varyans homojenliği sağlanmadığından uygulanan Welch ANOVA anlamlılık göstermemiştir (p:0,060). KRF alt boyutunda ise yaş grupları arasında istatistiksel olarak anlamlı bir farklılaşma bulunmamıştır (p:0,915). Bu bulgular, çözüm süreçleri/yönetişim algısının özellikle 31–40 yaş bandında daha yüksek olduğunu, buna karşın KUF ve KRF boyutlarında yaşa bağlı belirgin ve tutarlı bir farklılaşma olmadığını göstermektedir.

Tablo 5.11: Yaş aralığı ile SÖ alt boyutu arasındaki Krusal Wallis testi bulguları

Ölçeklerin Alt Boyutları	Yaş Aralığı	n	Sıra $\bar{x}$	p	Post Hoc (Mann-Whitney U)
SÖ	21-25	14	55,39	,001	31-40 >21-25, 41 ve üstü>31-40
	26-30	25	95,08		
	31-40	131	114,42		
	41 ve üstü	49	121,41		

n: Sayı, Sıra $\bar{x}$: sıra Ortalaması, p: %95 güven aralığında anlamlılık değeri

Tablo 5.11'e göre; SÖ alt boyutunda yaş grupları arasında anlamlı bir farklılık vardır ($p<0,05$). Sıra ortalamaları yaşla birlikte artma eğilimi göstermektedir; 21–25 grubunda en düşük düzey, 31–40 yaş aralığı ile 41 ve üstü yaş aralığı gruplarında ise daha yüksek düzeyler gözlenmiştir. Mann Whitney U testi uygulanarak yaş grupları arasında yapılan ikili karşılaştırmalarda 21-25 ile 31-40 yaş aralığındaki gruplarda $p:0,000$ ($p<0,05$) ve 21-25 ile 41 ve üstü yaş aralığındaki gruplarda $p:0,000$ ($p<0,05$) olduğundan grupları arasındaki farklar istatistiksel olarak anlamlıdır. Her iki karşılaştırmada da daha ileri yaş gruplarının SÖ puanları daha yüksektir ve bu bulgular, SÖ alt boyutunun yaşla birlikte yükseldiğine işaret etmektedir.

5.5.3. Eğitim Değişkenine Göre Farklılık Analizi Bulguları

Eğitim değişkeni ile KUF, KRF ve KÇS alt boyutlarına verilen yanıtlar arasındaki ilişkiyi incelemek amacıyla yapılan Tek Yönlü Anova Testi bulguları Tablo 5.12'de sunulmuştur.

Tablo 5.12: Eğitim ile KUF, KRF ve KÇS alt boyutları arasındaki Tek Yönlü Anova testi bulguları

Ölçeklerin Alt Boyutları	Eğitim	n	$\bar{x}$	ss	p	Post Hoc (Games- Howell)
KUF	Lise	10	2,9571	1,51643	,000	Lisans> Önlisans, Yükseklisans> Önlisans
	Önlisans	23	3,5839	,67132		
	Lisans	159	4,0566	,68719		
	Yükseklisans	27	4,0847	,58803		
KRF	Lise	10	2,3000	1,54320	,072	
	Önlisans	23	2,2319	,72777		
	Lisans	159	2,2243	,78801		
	Yükseklisans	27	1,7654	,96881		
KÇS	Lise	10	2,5333	1,54720	,000	
	Önlisans	23	3,2029	,84478		
	Lisans	159	3,5660	,75637		
	Yükseklisans	27	3,4909	,77119		

n: Sayı, $\bar{x}$: Ortalama, ss: Standart Sapma, p: %95 güven aralığında anlamlılık değeri

Tablo 5.12’ e göre; eğitim durumuna göre KUF alt boyutunda gruplar arası fark anlamlıdır ($p<0,05$). Games–Howell ikili karşılaştırmaları lisans ve önlisans grubu ($p:0,019$) ile yüksek lisans ve önlisans gruplarının ($p:0,038$) anlamlı derecede yüksek olduğunu göstermiştir. KRF’ de anlamlı fark bulunmamıştır ($p<0,05$). KÇS’ de genel etki anlamlı olmakla birlikte, Games–Howell çoklu karşılaştırmalarında anlamlı ikili fark saptanmamıştır ($p:0,60$).

Eğitim değişkeni ile SÖ alt boyutuna verilen yanıtlar arasındaki ilişkiyi incelemek amacıyla yapılan Kruskal Wallis Testi bulguları Tablo 5.13’ de sunulmuştur.

Tablo 5.13: Eğitim ile SÖ alt boyutu arasındaki Kruskal Wallis testi bulguları

Ölçeklerin Alt Boyutları	Eğitim	n	Sıra $\bar{x}$	p	Post Hoc (Mann-Whitney U)
SÖ	Lise	10	41,40	,000	Lisans>Lise, Önlisans, Yüksek lisans>Lise, Önlisans
	Önlisans	23	74,00		
	Lisans	159	118,53		
	Yükseklisans	27	115,81		

n: Sayı, Sıra $\bar{x}$: sıra Ortalaması, p: %95 güven aralığında anlamlılık değeri

Tablo 5.13’ e göre; SÖ alt boyutunda eğitim durumuna göre anlamlı fark olduğunu göstermiştir ($p:0,000$). Mann–Whitney ikili karşılaştırmalarında lisans ve yüksek lisans grupları hem lise hem de önlisans gruplarına göre anlamlı derecede daha yüksek puan almıştır. Bonferroni düzeltilmiş Mann–Whitney ikili karşılaştırmalarında lise ve önlisans ($p:0,027$) ile lisans ve yüksek lisans ($p:0,771$) çiftleri arasında anlamlı fark saptanmamıştır ($\alpha_{adj}=0,05/6=0,0083$).

5.6. Alt Boyutlar Arasındaki Korelasyon Bulguları

Ölçeklerin alt boyutları arasında yapılan Spearman Korelasyon analizi bulguları Tablo 5.14’ de sunulmuştur.

Tablo 5.14: Spearman Korelasyon analizi bulguları

Ölçeklerin Alt Boyutları		KUF	KRF	KÇS	SÖ
KUF	r	1,000	-,341	,745	,388
	p		,000	,000	,000
	n	219	219	219	219
KRF	r	-,341	1,000	-,383	-,149
	p	,000		,000	,028
	n	219	219	219	219
KÇS	r	,745	-,383	1,000	,379
	p	,000	,000		,000
	n	219	219	219	219
SÖ	r	,388	-,149	,379	1,000
	p	,000	,028	,000	
	n	219	219	219	219

r: Korelasyon katsayısı, n: Sayı, p: %95 güven aralığında anlamlılık değeri

Tablo 5.14'e göre; alt boyutlar arasında istatistiksel olarak anlamlı ilişkiler bulunmaktadır ($p < 0,05$). En güçlü pozitif ilişki KUF ile KÇS arasında saptanmıştır ($r: 0,745$). Bunun yanı sıra KUF ile SÖ ($r = 0,388$) ve KÇS ile SÖ ($r = 0,379$) arasında da orta düzeyde pozitif korelasyonlar vardır. Diğer taraftan KRF alt boyutu, diğer boyutlarla negatif yönlü ilişkiler göstermektedir: KRF-KÇS ($r = -0,383$), KRF-KUF ($r = -0,341$) ve KRF-SÖ ($r = -0,149$). Bu desen, kurumsal uygulamala/farkındalık ve kurumsal çözüm süreçleri algısı arttıkça (KUF, KÇS) kurumsal risk farkındalığının (KRF) görece azaldığını, stratejik öncelik alt boyutu (SÖ) ise genel olarak pozitif yönlü (SÖ-KUF, SÖ-KÇS), orta ölçekli ilişkiler bulunduğunu göstermektedir.

5.7.Genel Bulguların Değerlendirilmesi

Bu çalışmada yeniden yapılandırılan iki ölçek (VGMFÖ ve VGMÇÖÖ) üzerinde yürütülen geçerlilik, güvenirlik, normallik, ilişkisel ve korelasyon analizleri birlikte değerlendirildiğinde, kamu sektöründe veri güvenliği ve mahremiyeti alanında kurumsal farkındalığın çözüm yönelimleriyle anlamlı biçimde ilişkili olduğu ortaya çıkmıştır.

AFA sonuçları, VGMFÖ’de Kurumsal Uygulama/Farkındalık (KUF) ve Kurumsal Risk Farkındalığı (KRF); VGMÇÖ’de ise Kurumsal Çözüm Süreçleri (KÇS) ve Stratejik Öncelik (SÖ) olmak üzere ikişer faktörlü bir yapıyı göstermiş; her iki ölçekte açıklanan toplam varyans %50’nin üzerine çıkmıştır. Güvenirlilik analizleri KUF ($\alpha=,868$), KÇS ($\alpha=,837$) ve SÖ ($\alpha=,817$) için çok iyi; KRF ($\alpha=,649$) için madde sayısına bağlı sınırdan bir iç tutarlılığa işaret etmektedir.

KUF, KRF ve KÇS alt boyutlarında çarpıklık-basıklık değerleri kabul edilebilir aralıktadır; SÖ alt boyutunda normal dağılımdan belirgin sapma vardır. Bu nedenle KUF, KRF ve KÇS için parametrik; SÖ için parametrik olmayan yöntemler kullanılmıştır.

Cinsiyete göre KUF, KRF ve KÇS’de anlamlı fark yoktur; SÖ’de kadınların sıra ortalaması daha yüksektir. Yaş açısından KÇS’de 31–40 yaş grubu, 21–25 ve 41 ve üstü yaş gruplarından anlamlı biçimde yüksektir; SÖ’de ise sıra ortalamalarında yaşla birlikte artış eğilimi görülmüştür. Eğitim açısından KUF’ta lisans ve yüksek lisans grupları önlisansa göre daha yüksektir. SÖ’de ise lisans ve yüksek lisans grupları, lise ve önlisansa göre daha yüksektir. KRF’de anlamlı grup farkı saptanmamıştır.

En güçlü pozitif ilişki KUF–KÇS arasındadır. KUF–SÖ ($r=,388$) ve KÇS–SÖ ($r=,379$) orta düzeyde pozitifdir. KRF’nin KUF ($r=-,341$), KÇS ($r=-,383$) ve SÖ ($r=-,149$) ile ilişkileri negatif yönlüdür.

Genel olarak, kurumsal uygulama/farkındalık (KUF) ile kurumsal çözüm süreçleri (KÇS) birlikte yükselmekte; stratejik öncelik (SÖ) altboyutu bu iki yapıyla orta düzeyde pozitif ilişki göstermektedir. Kurumsal risk farkındalığı (KRF) ise diğer boyutlarla ters yönlü ilişki sergileyerek farklı bir dinamik ortaya koymaktadır.

5.8. Tartışma

Bulgular, kamu kurumlarında veri güvenliği ve mahremiyeti konusundaki farkındalığın çözüm süreçlerine eşlik eden temel bir bileşen olduğunu göstermektedir. KUF ile KÇS arasındaki yüksek korelasyon, kurumsal uygulamalara ilişkin farkındalık arttıkça çözüm süreçlerinin de daha olumlu algılandığını ve benimsenme eğiliminin güçlendiğini düşündürmektedir. SÖ’nün KUF ve KÇS ile pozitif ilişkisi, stratejik düzeyde

önceliklendirme algısının hem kurumsal farkındalık kapasitesi hem de süreç olgunluğuyla birlikte yükseldiğini göstermektedir.

Demografik desenler, bu genel tabloyu tamamlamaktadır. Cinsiyet açısından yalnızca SÖ alt boyutunda kadınların daha yüksek sıra ortalamasına sahip olması, stratejik önceliklendirme algısında gruplar arası duyarlılık farklarına işaret ederken; KUF, KRF ve KÇS’de fark olmaması, temel farkındalık ve süreç uyumunun cinsiyetten bağımsız ilerlediğini göstermektedir. Yaş değişkeninde 31–40 yaş grubunun KÇS’de daha yüksek değerleri, kurumsal deneyimle birlikte süreçlere katılım ve çözüm yöneliminin kuvvetlenebildiğini göstermektedir. Eğitim düzeyinin KUF ve SÖ’de daha yüksek skorlarla ilişkilendirilmesi, kurumsal uygulamaları anlama ve stratejik çerçeveyi kavrama kapasitesinin eğitimle birlikte arttığını düşündürmektedir.

KRF’nin diğer alt boyutlarla negatif ilişkisi, risk algısının kurumsal uygulama ve çözüm iyimserliğini sınırlayabilen, daha temkinli bir değerlendirme eğilimini yansıtabileceğine işaret etmektedir. Bu sonuç kurumsal risk farkındalığı ile uygulama/süreç odaklı iyimserlik arasında dengeleyici bir ilişki olduğunu düşündürmektedir. Ayrıca SÖ alt boyutunda gözlenen dağılım sapması (negatif çarpıklık ve yüksek basıklık), stratejik önceliklendirme algısında katılımcıların belirli kümelerde yoğunlaştığını, bu boyutun kurumsal bağlam ve deneyimle şekillenen daha heterojen bir yapı taşıdığını ima etmektedir.

Bu çerçevede çalışma, veri güvenliği ve mahremiyeti alanında kurumsal farkındalık, çözüm süreçleri ve stratejik önceliklendirme arasında bütünleşik bir örüntü bulunduğunu; kurumsal risk farkındalığının ise bu örüntüyü farklı bir açıdan etkilediğini ortaya koymaktadır. Bu durum, literatürde yer alan pek çok çalışmanın bulgularıyla örtüşmektedir.

Öncelikle, kamu çalışanlarının farkındalık düzeyinin yüksek olması, güvenlik politikalarına uyumu arttıran temel etkenlerden biridir. Bu çalışmada da benzer biçimde, farkındalığın yüksek olduğu çalışanların çözüm önerilerine katılımın daha güçlü olduğu tespit edilmiştir. Özellikle eğitim düzeyi ile farkındalık arasında kurulan pozitif ilişki, Özdemir ve Uluyol (2021) çalışmasında da benzer şekilde vurgulanmaktadır.

Araştırmada farkındalık düzeyinin yüksek olmasına rağmen bazı güvenlik uygulamalarına yönelik çekincelerin devam ettiği görülmektedir. Bu durum, literatürde “bilişsel farkındalık

ile davranışsal uygulama arasındaki boşluk” olarak tanımlanan olguyla ilişkilendirilebilir (Ndou, 2004; Çakır ve Taşer, 2023). Çalışmamızda katılımcılar, verinin korunmasına ilişkin önlemlerin önemini kabul etmekle birlikte, bazı durumlarda bu önlemlerin uygulamadaki etkinliğini sorgulamaktadır. Bu bulgu, Ordu (2021)’in “farkındalık, davranışı doğrudan belirlemez; davranış, örgütsel kültür ve yönetsel destekle pekiştirilir” savını desteklemektedir.

Araştırmamızda farkındalık düzeyi ile çözüm önerilerine ilişkin tutumlar arasında pozitif yönde anlamlı bir korelasyon bulunmuştur. Bu bulgu, veri güvenliği kültürünün oluşmasında yalnızca teknik önlemlerin değil, bireysel katılımın da belirleyici olduğunu gösteren çalışmaları (Hatipoğlu ve Tunacan, 2021; Kahraman ve Özen, 2025) destekler niteliktedir.

Veri güvenliği ve mahremiyeti konusundaki farkındalığın artması, çalışanların veri güvenliği politikalarına olan uyumunu ve bu politikaların etkinliğini artırmaktadır (Delso-Vicente vd., 2025). Elde edilen bulgular, literatürdeki bu genel eğilimle uyumlu olup, çalışanların veri güvenliği konusundaki bilgi seviyelerinin önerilere yönelik tutumlarını şekillendirdiğini göstermektedir.

Kamu sektöründe veri güvenliği ve mahremiyeti konusundaki farkındalık düzeyinin artırılması, önemli pratik yansımaları beraberinde getirmektedir. Araştırmamız, çalışanların veri güvenliği politikalarına olan uyumlarının artırılmasının, kurumların genel güvenlik duruşunu güçlendireceğini ortaya koymuştur. Farkındalık artırma eğitimleri ve iletişim stratejileri, çalışanların veri güvenliği konusundaki bilgi seviyelerini güncelleyerek, önerilerin daha etkin bir şekilde benimsenmesine olanak sağlayacaktır.

Özellikle, veri güvenliği politikalarının gözden geçirilmesi ve güncellenmesi, çalışanların ihtiyaçlarına ve önerilerine daha uygun hale gelmesi açısından kritik bir rol oynamaktadır. Bu durum, kurum içinde güçlü bir güvenlik kültürü oluşturulmasına katkı sağlar. Çalışanların önerilerini dikkate alarak, uygulama süreçlerinin iyileştirilmesi, veri güvenliği uygulamalarının etkinliğini artırma potansiyeline sahiptir.

Ayrıca, veri güvenliği konusundaki farkındalığın artırılmasında etkili iletişim stratejilerinin büyük önemi bulunmaktadır. İletişim, kurum içindeki bilgi akışını sağlarken, çalışanların veri güvenliği konusundaki algılarını da şekillendiren önemli bir faktördür. Çalışanların

önerilerini ifade edebileceği platformların oluşturulması, veri güvenliği uygulamalarının etkinliğini artırabilir. Kurum içindeki iletişim stratejilerinin güçlendirilmesi, çalışanların veri güvenliği konusundaki bilgilerini artırarak, önerilerin daha etkili bir şekilde uygulanmasına katkıda bulunacaktır.

Veri güvenliği eğitimlerinin yalnızca başlangıç seviyesinde bilgi aktarımının ötesine geçerek, katılımcılara aktif katılım fırsatları sunması büyük önem taşımaktadır. Bu sayede, çalışanlar hem bilgi edinir hem de uygulama becerilerini geliştirme imkanı bulurlar. Eğitimlerin sürekliliği de kritik bir faktördür; çünkü veri güvenliği tehditleri sürekli olarak evrilmektedir. Bu nedenle, eğitim programlarının güncellenmesi ve düzenli aralıklarla tekrarlanması gerekmektedir. Bu, çalışanların güncel bilgilerle donanmasını sağlayarak, veri güvenliği kültürünün sürekliliğini destekler.

Bu çalışma, kamu sektöründe veri güvenliği ve mahremiyeti konusundaki farkındalığın artırılmasının, çözüm önerilerinin etkinliğini artıracak ve güvenli bir çalışma ortamının sağlanmasına katkıda bulunacağını göstermektedir.

6.SONUÇ VE ÖNERİLER

Bu bölümde; araştırmanın genel sonuçları özetlenmekte, kamu kurumlarına yönelik pratik öneriler ile gelecek araştırmalara yönelik akademik öneriler sunulmaktadır.

6.1. Sonuç

Bu çalışma, kamu sektöründe veri güvenliği ve mahremiyetinin yalnızca teknik önlemlerle değil; çalışan farkındalığı, kurumsal süreçlerin olgunluğu ve stratejik önceliklendirme kültürüyle birlikte inşa edildiğini göstermektedir. Genel eğilim nettir: Katılımcılar, konunun stratejik önemini güçlü biçimde kabul etmekte ve çözüm odaklı yaklaşımlara olumlu bakmaktadır. Buna karşın, bireysel katkı, kurum içi tartışma ve duyuru kanalları pratikte orta düzeyde kalmaktadır. Bu da “ne yapılmalı?” sorusunda yüksek bir mutabakat varken, “bunu birlikte nasıl yaparız?” sorusunda kurumsal mekanizmaların daha fazla olgunlaştırılması gerektiğine işaret eder.

Bulgular, kurumsal uygulama ve süreçlere ilişkin farkındalık yükseldikçe çözüm süreçlerine katılımın da güçlendiğini; stratejik önceliklendirme algısının ise bu iki alanla birlikte ilerlediğini göstermektedir. Buna karşılık kurumsal risk farkındalığı, bu iyimserliği dengeleyen bir unsur olarak öne çıkmaktadır: Riskleri yüksek duyarlılıkla gören çalışanlar süreç ve uygulamalara daha temkinli yaklaşabilmektedir. Doğru kurgulandığında bu, kurumlar için bir zayıflık değil; tehdit algısıyla çözüm güvenliğini birlikte ele alan dengeli güvenlik kültürünün temel parçasıdır.

Araştırmada kurulan hipotezler toplu değerlendirildiğinde;

H1: İçişleri Bakanlığında çalışan teknik hizmetler sınıfındaki personel ve Bilgi İşlem Şefliği/Müdürlüğünde görev yapan personelin veri güvenliği ve mahremiyeti farkındalık düzeyleri yüksektir: Kısmen desteklenmiştir. Katılımcılar konuya ve politikalara dair bilgiye sahip; ancak eğitim deneyimi ve olay görgüsü gibi alt alanlarda boşluklar bulunmaktadır. Genel tablo orta–iyi düzeyde bir farkındalığı işaret etmektedir.

H2: İçişleri Bakanlığında çalışan teknik hizmetler sınıfındaki personel ve Bilgi İşlem Şefliği/Müdürlüğünde görev yapan personelin veri güvenliği ve mahremiyeti

konusundaki çözüm önerilerine yönelik düzeyleri yüksektir: Desteklenmiştir. Sorunların çözümüne, eğitim–farkındalık programlarına ve teknolojik çözümlere güçlü bir yönelim vardır; ancak bireysel katkı ve kurum içi tartışma/duyuru pratikleri orta düzeydedir.

H3: İçişleri Bakanlığında teknik hizmetler sınıfında ve Bilgi İşlem birimlerinde görev yapan personelin veri güvenliği ve mahremiyet farkındalık düzeyleri cinsiyete göre farklılık göstermektedir: Desteklenmemiştir. Temel farkındalık boyutlarında cinsiyete bağlı belirgin bir ayrışma gözlemlenmemiştir.

H4: İçişleri Bakanlığında teknik hizmetler sınıfında ve Bilgi İşlem birimlerinde görev yapan personelin veri güvenliği ve mahremiyet çözüm önerileri düzeyleri cinsiyete göre farklılık göstermektedir: Kısmen desteklenmiştir. Kurumsal çözüm süreçlerinde belirgin bir fark yokken, stratejik önceliklendirme boyutunda kadınların eğiliminin daha yüksek olduğu görülmüştür.

H5: İçişleri Bakanlığında teknik hizmetler sınıfında ve Bilgi İşlem birimlerinde görev yapan personelin veri güvenliği ve mahremiyet farkındalık düzeyleri yaş aralığına göre farklılık göstermektedir: Desteklenmemiştir. Temel farkındalık boyutlarında yaşa bağlı tutarlı bir ayrışma saptanmamıştır.

H6: İçişleri Bakanlığında teknik hizmetler sınıfında ve Bilgi İşlem birimlerinde görev yapan personelin veri güvenliği ve mahremiyet çözüm önerileri düzeyleri yaş aralığına göre farklılık göstermektedir: Desteklenmiştir. Çözüm süreçlerine katılım ve stratejik bakış yaşla birlikte güçlenme eğilimi göstermektedir.

H7: İçişleri Bakanlığında teknik hizmetler sınıfında ve Bilgi İşlem birimlerinde görev yapan personelin veri güvenliği ve mahremiyet farkındalık düzeyleri eğitime göre farklılık göstermektedir: Kısmen desteklenmiştir. Kurumsal uygulama farkındalığı boyutunda eğitim seviyesi arttıkça kısmen ayrışma saptanmıştır.

H8: İçişleri Bakanlığında teknik hizmetler sınıfında ve Bilgi İşlem birimlerinde görev yapan personelin veri güvenliği ve mahremiyet çözüm önerileri düzeyleri eğitime göre farklılık göstermektedir: Kısmen desteklenmiştir. Çözüm odaklı stratejik bakış açısında eğitim seviyesi yükseldikçe artma eğilimi gözlemlenmiştir.

H9: Veri güvenliği ve mahremiyeti farkındalığı değişkeni ile veri güvenliği ve mahremiyeti çözüm önerileri değişkeni arasında pozitif bir ilişki bulunmaktadır: Desteklenmiştir. Farkındalık yükseldikçe çözüm süreçlerine yönelim ve stratejik önceliklendirme de artmaktadır.

Elde edilen bulgular, veri güvenliği ve mahremiyeti konusundaki farkındalığın artırılmasının önemini açıkça ortaya koymaktadır. Eğitim programları, çalışanların veri güvenliği konusundaki bilgilerini artırarak, önerilerin daha etkin bir şekilde benimsenmesini sağlama potansiyeline sahiptir. Bu doğrultuda, kamu kurumları için düzenlenecek eğitimlerin içeriği büyük bir öneme sahiptir. Eğitimlerin; güncel tehditler, risk yönetimi ve veri koruma yöntemleri hakkında bilgi vermeye odaklanması, çalışanların bu konudaki algılarını güçlendirecektir.

Bunun yanı sıra, farkındalık artırma faaliyetleri, çalışanların veri güvenliği konusundaki motivasyonlarını artırabilir. Özellikle kurum içindeki iletişim stratejileri, çalışanların önerilerini dikkate almaya yönelik bir kültür geliştirilmesine yardımcı olabilir. Çalışanların önerilerini daha etkin bir şekilde ifade etmeleri için gerekli ortamın sağlanması, veri güvenliği uygulamalarının etkinliğini artıracaktır.

Politika düzeyinde çıkarımlar açık olmakla birlikte kurumsal güvenlik politikaları düzenli aralıklarla güncellenmeli; güncellemeler açık ve anlaşılır biçimde çalışanlara aktarılmalı; uygulama süreçleri çalışan katılımıyla tasarlanmalıdır. Teknolojik yatırımlar, süreç tasarımı ve yetkinlik geliştirmeyle birlikte ele alınmalı; yalnızca teknolojiye değil, bu teknolojiyi etkin kullanacak kültür ve becerilere de yatırım yapılmalıdır. Uygulamalı, vaka temelli eğitimler ve güçlü iletişim–geri bildirim mekanizmaları bir araya geldiğinde, kamu kurumlarının içinde güvenlik kültürü kalıcı biçimde güçlenecek; önerilerin hayata geçme kapasitesi artacak ve kamu hizmetlerinin güvenilirliği somut biçimde yükselecektir. Bu çalışma, “bilmekten” “birlikte yapmaya” geçişi hızlandıracak öncelik alanlarını netleştirmekte ve kamu kurumları için pratik bir yol haritası sunmaktadır.

Kamu sektöründe veri güvenliği ve mahremiyeti konularında etkili iletişim stratejilerinin oluşturulması, çalışanların farkındalık düzeyini artırma noktasında kritik bir rol oynamaktadır. İletişim, kurum içindeki bilgi akışını sağlamakta ve çalışanların önerilerini paylaşımlarına olanak tanımaktadır. Kamu kurumları, çalışanların veri güvenliği

konusundaki algılarını güçlendirmek için düzenli olarak bilgilendirme yapmalı ve çalışanların önerilerini dikkate almalıdır.

Kurum içindeki iletişimin güçlendirilmesi, çalışanların veri güvenliği konusundaki bilgilerini artırmakla kalmayacak, aynı zamanda önerilerin daha etkili bir şekilde uygulanabilir hale gelmesine katkıda bulunacaktır. Çalışanların önerilerini ifade edebileceği platformlar oluşturmak, veri güvenliği uygulamalarının etkinliğini artırabilir. Bu, aynı zamanda kurum içinde bir güvenlik kültürü oluşmasına da katkıda bulunacaktır. Çalışanların önerilerini ifade edebileceği platformlar oluşturmak, veri güvenliği uygulamalarının etkinliğini artırabilir. Bu, aynı zamanda kurum içinde bir güvenlik kültürü oluşmasına da zemin hazırlayacaktır.

Sonuçlar, kamu sektöründeki veri güvenliği stratejilerinin gözden geçirilmesi ve güçlendirilmesi gerektiğini göstermektedir. Veri güvenliği konusundaki farkındalık düzeyinin artırılması, önerilerin daha etkin bir şekilde benimsenmesinde önemli bir rol oynamaktadır. Kamu kurumları, veri güvenliği eğitimlerini düzenli olarak güncelleyerek, çalışanlarının güncel tehditlere karşı bilgi sahibi olmalarını sağlamalıdır. Özellikle, kamu sektörü çalışanlarının veri güvenliği konusundaki eğitimlerinin, yalnızca teorik bilgilerle sınırlı kalmayıp, uygulamalı eğitimleri de içermesi gerektiği vurgulanmaktadır. Uygulamalı eğitimler, çalışanların veri koruma yöntemlerini ve en iyi uygulamaları daha iyi anlamalarına yardımcı olacaktır. Ayrıca bu tür eğitimler, çalışanların gerçek yaşam senaryolarında nasıl hareket edeceklerini öğrenmelerini sağlayarak, kurumların veri güvenliği uygulamalarını güçlendirebilir.

6.2. Öneriler

Bu bölümde, araştırmanın bulgularından hareketle kamu kurumlarının veri güvenliği ve mahremiyet uygulamalarını geliştirmeye yönelik öneriler ile gelecekte yapılacak akademik çalışmalara ilişkin yönlendirici değerlendirmelere yer verilmiştir.

6.2.1. Kamu Kurumlarına Yönelik Öneriler

Eğitim içeriklerinin temel–orta–ileri düzey kademelendirmesiyle yapılandırılması, kurumsal uygulama/farkındalık ve çözüm süreçlerine katılımı güçlendirecektir. Programların vaka

temelli, uygulamalı ve senaryo odaklı bileşenler içermesi; güncel tehditler, risk yönetimi ve veri koruma pratiklerine ilişkin bilişsel bilgiyi davranışsal yeterliklere dönüştürmesi beklenmektedir.

Olay bildirim süreçleri, “öğrenilen dersler” raporlaması ve iyi uygulama havuzlarının standart operasyon prosedürlerine entegre edilmesi önerilmektedir. Düzenli forumlar, geri bildirim döngüleri ve öneri sistemleri aracılığıyla bireysel katkının görünür, izlenebilir ve teşvik edilebilir hale getirilmesi, katılım temelli güvenlik kültürünü güçlendirecektir. Alınan önlemlerin ve politika güncellemelerinin sistematik ve erişilebilir iletişim planlarıyla tüm personele duyurulması, uygulama birliğini artıracaktır.

Bulguların işaret ettiği temkinli tutumlar dikkate alınarak risk iletişimi, somut kontrol önlemleri, performans göstergeleri ve başarı örnekleriyle birlikte kurgulanmalıdır. Böylelikle yüksek risk farkındalığının motivasyon kaybına dönüşmeden, uygulanabilir çözümlere güven üreten bir denge unsuru olarak işlemesi sağlanacaktır.

Kurumsal süreç olgunluğu açısından güçlü performans gösteren yaş/deneyim gruplarının mentorluk, akran eğitimi ve saha koçluğu rollerinde konumlandırılması; deneyim bilgisinin kurumsal öğrenmeye dönüştürülmesi açısından önemlidir. Bu yaklaşım, yatay bilgi paylaşımı ve birimler arası uyumun artırılmasına katkı sunacaktır.

Güvenlik teknolojilerine ilişkin yatırımların, süreç tasarımı, görev–rol tanımları ve yetkinlik geliştirme programlarıyla birlikte ele alınması gerekmektedir. Politika güncellemeleri ile operasyonel iyileştirmelerin eşzamanlı yürütülmesi; ölçülebilir hedefler ve olgunluk göstergeleriyle izlenmesi önerilmektedir.

Stratejik önceliklendirme alanında farklı grupların (özellikle kadın çalışanların) güçlü olduğu yönelimlerin karar süreçlerine sistematik biçimde dahil edilmesi, kurumsal kapasitenin ve güvenlik kültürünün derinleşmesine katkı sağlayacaktır. Kapsayıcı katılım, farklı perspektiflerin risk ve çözüm dengesine yansımaları kolaylaştıracaktır.

Merkez–taşra ve birimler arası farklılıkları gözeterek ihtiyaç analizlerine dayalı yerelleştirilmiş programların geliştirilmesi; uygulama standardının performans metrikleriyle

izlenmesi önerilmektedir. Böylelikle kurumsal ilkeler korunurken yerel bağlamın gereksinimleri karşılanabilecektir.

Farkındalık, süreç olgunluğu ve stratejik öncelik göstergeleri için periyodik ölçüm–raporlama takvimi oluşturulmalı; bulgular, eğitim içerikleri ve süreç tasarımlarına düzenli geri besleme sağlayacak şekilde kullanılmalıdır. Bu mekanizma, güvenlik kültürünün sürekliliğini ve kurumsal öğrenmeyi destekleyecektir.

6.2.2. Gelecek Araştırmalara Yönelik Öneriler

Gelecek araştırmalarda, veri güvenliği ve mahremiyeti konusundaki farkındalık düzeyinin zaman içindeki değişimini incelemek için uzun vadeli çalışmalar yapılabilir. Bu tür araştırmalar, eğitim programlarının etkinliğini değerlendirmek ve sürekli iyileştirme süreçlerini desteklemek açısından önemlidir.

Nitel verilerin yanı sıra, nitel araştırmalar da yapılabilir. Katılımcıların veri güvenliği konusundaki algılarını ve önerilerini daha derinlemesine anlamak için görüşmeler veya odak grup tartışmaları düzenlenebilir. Bu, daha kapsamlı bir anlayış sağlayabilir.

Gelecek çalışmalarda, önerilerin nasıl uygulanabileceğine dair stratejiler geliştirilmesi de önemlidir. Çalışanların önerilerini dikkate alacak sistemler geliştirmek, veri güvenliği uygulamalarının etkinliğini artırabilir.

Eğitim programları, iletişim stratejileri ve politika geliştirme süreçleri, veri güvenliği uygulamalarının güçlendirilmesi açısından kritik öneme sahiptir. Gelecek araştırmalar, bu konuya daha derinlemesine bakarak, kamu sektöründe veri güvenliği ve mahremiyetine yönelik daha etkili stratejilerin geliştirilmesine katkıda bulunabilir.

Farklı kamu kurumları, yerel yönetimler ve değişik görev/pozisyon gruplarını kapsayan karşılaştırmalı çalışmalara ihtiyaç vardır. Kurumsal iklim ve örgüt kültürünün etkilerinin modellere dahil edilmesi, bulguların dış geçerliliğini artıracaktır.

Öz-bildirim temelli verilerin; olay kayıtları, uyum logları ve performans metrikleri gibi operasyonel göstergelerle desteklenmesi, sonuçların güvenilirliğini güçlendirecektir. Böylece algı–davranış boşluğu daha sağlıklı biçimde değerlendirilebilecektir.

Bu çalışma, kurumların veri güvenliği uygulamalarının etkili bir şekilde yürütülmesi için gerekli olan bilgileri ve önerileri sunmakta ve bu alandaki literatüre katkıda bulunmaktadır.

KAYNAKLAR

- Abanoz, M. ve Acar, E. (2023). Yapay Zekâ Ve Ontolojik Güvensizlik: Bireysel Ve Toplumsal Kaygı Dinamikleri Üzerine Bir Değerlendirme. *Laii Sosyal Bilimler Dergisi*, 14(I), 22-51.
- Abisoye, A. ve Akerele, J. I. (2021). A High-Impact Data-Driven Decision-Making Model for Integrating Cutting-Edge Cybersecurity Strategies into Public Policy. *Governance And Organizational Frameworks*.
- Akmeşe, S. (2020). Kamuda Dijital Dönüşümün Siber Güvenlik Ve Dijital Güvence Boyutları Ve İç Denetimin Rolü. *Denetişim* (20), 108-119.
- Akram, V. ve Dağdeviren, O. (2020). Nesnelerin İnterneti için Gerçek Zamanlı Tasarsız Veri Toplama Platformu. *Bilişim Teknolojileri Dergisi*, 13(4), 451-462. <https://doi.org/10.17671/gazibtd.745598>
- Aksoy, E. ve Özkan, F. (2023). Türkiye’de Kamu Yönetimi Eğitiminin Mevcut Durumu ve Sorunlarına Yönelik Bir Çözümleme. *Ekonomi İşletme Siyaset Ve Uluslararası İlişkiler Dergisi*, 9(2), 218-228.
- Alkhalil, Z., Hewage, C., Nawaf, L., ve Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, 563060.
- Al Naim, A. F. ve Ghouri, A. M. (2023). Exploring the Role of Cyber Security Measures (Encryption, Firewalls, and Authentication Protocols) in Preventing Cyber-Attacks On E-commerce Platforms. *International Journal of eBusiness and eGovernment Studies*, 15(1), 44-469.
- Alraja, M. N., Butt, U. J., ve Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers & Security*, 129, 103208.
- Altun, T., Şahin, F. ve Öztaş, N. (2017). Kamu Politikalarının Belirlenmesi ve Uygulanmasında Büyük Veri. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 22(Kayfor 15 Özel Sayısı), 2021-2044.
- Alyass, A., Turcotte, M., ve Meyre, D. (2015). From big data analysis to personalized medicine for all: challenges and opportunities. *BMC medical genomics*, 8, 1-12.
- Aswathy, S. U., ve Tyagi, A. K. (2022). Privacy Breaches through Cyber Vulnerabilities: Critical Issues, Open Challenges, and Possible Countermeasures for the Future. *In Security and Privacy-Preserving Techniques in Wireless Robotics* (pp. 163-210). CRC Press.
- Aydoğdu, Y. (2021). Kamu İdaresinde Kişisel Verilerin Korunması. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 29(1), 263-293. <https://doi.org/10.15337/suhfd.808608>
- Aytekin, A., Erdoğan, Y. ve Kavalcı, K. (2016). Yeni Bir İş Modeli: Muhasebe Alanında Bulut Bilişim. *Uluslararası Yönetim İktisat Ve İşletme Dergisi*, 12(12), 46-62.

- Badur, E. ve Kurt Konca, N. (2022). Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Zararların Tazmini Ve Görevli Mahkeme. *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 13(2), 476-490. <https://doi.org/10.21492/inuhfd.1159230>.
- Bakır, C., Hakkoymaz, V. ve Güçlü, M. (2019). Dağıtık Etiketleme Modeli İle Bilgi Akış Denetimi. *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi*, 6(2), 231-242. <https://doi.org/10.35193/bseufbd.592542>
- Barkuş, F. ve Koç, M. (2019). Dijital Mahremiyet Kavramı Ve İlgili Çalışmalar Üzerine Bir Derleme. *Bilim Eğitim Sanat ve Teknoloji Dergisi*, 3(1), 35-44.
- Bulut, M. (2020). Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler. *Ankara Barosu Dergisi*, 78(3), 99-150. <https://doi.org/10.30915/abd.811902>
- Cath, C. (2018). Governing Artificial Intelligence: Ethical, Legal And Technical Opportunities And Challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2133), 20180080.
- Cooke, P., Heidenreich, M., ve Braczyk, H. J. (2024). Introduction: Regional innovation systems—an evolutionary approach. In *Regional innovation systems* (pp. 1-18). Routledge.
- Çakır, H. ve Taşer, M. (2023). Türkiye’de Yapılan Siber Güvenlik Faaliyetlerinin ve Eğitim Çalışmalarının Değerlendirilmesi. *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım Ve Teknoloji*, 11(2), 347-366. <https://doi.org/10.29109/gujsc.1165131>
- Çakır, H. ve Tuygun, M. (2019). Iso27001 Bilgi Güvenliği Yönetim Sistemi Standardının Kamu Kurumlarına Uygulanabilirliğinin Araştırılması: Ankara İli Örneği. *International Journal of Management Information Systems and Computer Science*, 3(2), 59-78. <https://doi.org/10.33461/uybisbbd.598989>
- Çakır, H. ve Yaşar, H. (2015). Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri. *Duzce University Journal of Science and Technology*, 3(2), 488-507.
- Çelik, D. (2023). Kamu Yönetiminde Dijital Dönüşümde Bir Sorun Alanı: Dijital Kültüre Yönelik Direnç. *Kamu Yönetimi Ve Teknoloji Dergisi*, 5(1), 69-86. <https://doi.org/10.58307/kaytek.1308745>
- Çeliksoy, E. ve Akça, A. (2024). Türkiye’de Kamu Yönetiminde Yaşanan Dijital Dönüşüm Süreci. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 15(2), 445-486. <https://doi.org/10.54558/jiss.1426480>
- Çiçek, M. (2024). Türkiye’de Biyometrik Veri Güvenliği: Kişisel Verilerin Korunması Kanunu Çerçevesinde Etik Bir Değerlendirme. *Kişisel Verileri Koruma Dergisi*, 6(2), 54-76.
- Çubukcu, Z. (2024). Dijital Çağda Kişisel Verilerin Korunmasında Veri Koruma Otoritelerinin Rolü. *Toplum Ekonomi Ve Yönetim Dergisi*, 5(3), 454-469.

- Davenport, T. H. (2018). From analytics to artificial intelligence. *Journal of Business Analytics*, 1(2), 73-80.
- Dayıoğlu, E. (2016). Kamu İdarelerinde Bilgi Sistemi Güvenlik Risklerinin Yönetimi. *Denetim* (4), 71-81.
- Delso-Vicente, AT, Diaz-Marcos, L., Aguado-Tevar, O., ve de Blanes-Sebastián, MG(2025) Çalışanların Bilgi Güvenliği Politikalarına Uyumunu Etkileyen Faktörler: Siber Güvenlikte Davranışsal Ve Teknolojik Yönlere İlişkin Sistemik Bir Literatür İncelemesi. *Future Business Journal* , 11 (1), 28.
- Demir, N. ve Büyükalın Filiz, S. (2018). Kamu Çalışanlarının Bilgi ve İletişim Teknolojilerini Kullanım Düzeylerinin İncelenmesi Sayıştay Başkanlığı Örneği. *Sayıştay Dergisi* (108)149-174.
- Doluküp, İ. ve Hakbilen, G. (2021). Kurumsal kalite sisteminin kullanılabilirliğinin değerlendirilmesi. *Sağlıkta performans ve kalite dergisi*, 18(1), 89-108.
- Dülger, M. V. (2016). Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 3(2), 101-168.
- Efe, A. (2022). Yapay Zekâ Ortamındaki Dijital Kamu Yönetiminin Yol Haritası. *Kamu Yönetimi Ve Teknoloji Dergisi*, 4(1), 99-130.
- Egemen, E. E. (2023). Kişisel Verilerin İşlenmesinde “Doğru ve Gerektiğinde Güncel Olma” İlkesi ve Kişisel Verileri Koruma Kurulunun 2023/78 Sayılı Kararı. *Trabzon Üniversitesi Hukuk Fakültesi Dergisi*, 1(1), 105-133.
- Eichensehr, K. E. (2020). The Law And Politics Of Cyberattack Attribution. *UCLA L. Rev.*, 67, 520.
- Eltimur, D. (2022). İnsan Haklarının Korunması Bağlamında Yapây Zeka Uygulamaları. *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi*, 12(2), 559-594. <https://doi.org/10.54704/akdhfd.1155778>
- Ener, .D. ve Demircan, Y. (2008). Küreselleşme Sürecinde Değişen Devlet Anlayışından Kamu Hizmetlerinin Dönüşümüne: Sağlık Hizmetlerinde Piyasa Mekanizmaları. *Süleyman Demirel Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi*, 13(1), 57- 82.
- Enocson, J. ve Söderholm, L. (2018). Prevention of Cyber Security Incidents within the Public Sector: A qualitative case study of two public organizations and their way towards a sustainable cyber climate(Master’s Thesis), Linköping University.
- Eriçok, R. E. (2023). Dünyada ve Türkiye’de Kamu-Özel İşbirliği Uygulamaları: Rakamsal Verilerle Bir Analiz. *İktisat Politikası Araştırmaları Dergisi*, 10(2), 629-661. <https://doi.org/10.26650/JEPR1310789>

- Ertekin, İ. (2022). Kamu Yönetimi Ve Halkla İlişkiler Yönüyle Kişisel Verilerin Korunması Kanunu (KVKK). *Ombudsman Akademik*, 8(16), 39-67.
- Eyüpgiller, S. (2023). Türk Vergi Sisteminde Dijital Dönüşümde Önemli Bir Dönem: 2017-2021. *Social Review of Technology and Change*, 1(1), 68-100.
- Flowerday, S. V. ve Tuyikeze, T. (2016). Information Security Policy Development And Implementation: The What, How And Who. *Computers & Security*, 61, 169-183.
- Field, A. (2009). Discovering statistics using SPSS: Book plus code for E version of text (Vol. 896). London, UK: *SAGE Publications Limited*.
- Fiore, M. (2025). Advanced Modeling Techniques And Methodologies For Reliable And Secure Blockchain Platforms Design (Master's Thesis), *Politecnico di Bari*.
- F. Shaar ve A. Efe, "Ddos Attacks And Impacts On Various Cloud Computing Components", *IJISS*, vol. 7, no. 1, pp. 26-48, 2018.
- George, A. S., Baskar, T., ve Srikanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, 2(1), 51-75.
- George, D. ve Mallery, P. (2003). SPSS for Windows step by step: A simple guide and reference. 11.0 update Fourth edition. *Boston: Allyn & Bacon*.
- George, D. ve Mallery, M. (2010). SPSS For Windows Step Bysstep: A Simple Guide And Reference. *Baston: Allyn & Bacon*.
- Göçoğlu, V. (2020). Kamu Hizmetlerinin Sunumunda Dijital Dönüşüm: Nesnelerin İnterneti Üzerine Bir İnceleme. *MANAS Sosyal Araştırmalar Dergisi*, 9(1), 615-628. <https://doi.org/10.33206/mjss.538784>
- Güdek, B. (2023). Kamu Sektöründe Etik Yönetime İlişkin Politikaların Uygulanması: KVKK ve Veri Etiği. *Politik Ekonomik Kuram*, 7(2), 237-251. <https://doi.org/10.30586/pek.1325605>
- Hatipoğlu, C. ve Tunacan, T. (2021). Türkiye’de Siber Saldırı ve Tespit Yöntemleri: Bir Literatür Taraması. *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi*, 8(1), 430-445. <https://doi.org/10.35193/bseufbd.838732>
- Helin, A. ve Himanen, P. (2023). Joining NATO: Effects on Finland's Cyber Security (Master's Thesis), *Laurea University of Applied Sciences & Jamk University of Applied Sciences*.
- Herath, T. ve Rao, H. R. (2009). Protection Motivation And Deterrence: A Framework For Security Policy Compliance İn Organisations. *European Journal Of Information Systems*, 18(2), 106-125.
- Hilbert, M. (2013). Big Data For Development: From Information-To Knowledge Societies. *Available at SSRN 2205145*.

- Hizarcı, E. (2019). 6698 Sayılı Kişisel Verilerin Korunması Kanununun Ab Veri Koruma Hukuku ışığında Değerlendirilmesi (Master's thesis), Marmara Üniversitesi, Turkey.
- Hoofnagle, C. J., Van Der Sloot, B., ve Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What It Is And What It Ortalamas. *Information & Communications Technology Law*, 28(1), 65-98.
- İren, E. ve Can, Ö. (2017). Bilgi Sistemlerinde Güncel Güvenlik Problemleri Ve Önerilen Çözümler. *TÜBAV Bilim Dergisi*, 10(2), 27-42.
- Jean-Quartier, C., Rey Mazón, M., Lovrić, M., ve Stryeck, S. (2022). Collaborative Data Use Between Private And Public Stakeholders—a regional case study. *Data*, 7(2), 20.
- Kahraman, A. ve Özen, Ü. (2025). Yerel Yönetimlerin Dijital Dönüşümü Sürecinde Bilişim Teknolojileri Ve Dijital Yeterliliklerin Değerlendirilmesi. *Ekev Akademi Dergisi*, (101), 404-427.
- Kalipçi, N. E. (2025). Kişisel Ve Kurumsal Bilgi Güvenliğinde Güncel Teknolojiler ve Yapay Zekâ Destekli Çözümler. *Turan-Sam*, 17(65), 468-477.
- Karasoy, H. ve Gezici, H. S. (2023). Bombalardan Baytlara: Siber Güvenliğin Ulusal Güvenlikteki Rolü ve Yapay Zekânın Siber Güvenlikteki Önemi. *Uluslararası Yönetim Akademisi Dergisi*, 6(1), 173-188.
<https://doi.org/10.33712/mana.1254015>
- Kavak, A. ve 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>
- Kiraz, O. Z. (2021). Siber Güvenlik Bağlamında Yeni Tehdit Algılamalarının Türkiye'nin Güvenlik Politikalarına Etkileri. *Journal of Management Theory and Practices Research*, 2(2), 69-88.
- Köksoy, Fulya. "Avrupa Birliği'nin Siber Güvenlik Politikası: Kurumsalcılık Mı Tutarlılık mı?". *Güvenlik Stratejileri Dergisi* 16, sy. 35 (Ekim 2020): 635-74.
<https://doi.org/10.17752/guvenlikstrjtj.807014>
- Kuipers, S. ve Schonheit, M. (2022). Data Breaches And Effective Crisis Communication: A Comparative Analysis Of Corporate Reputational Crises. *Corporate Reputation Review*, 25(3), 176-197.
- Labadie, C. ve Legner, C. (2023). Building Data Management Capabilities To Address Data Protection Regulations: Learnings from EU-GDPR. *Journal of Information Technology*, 38(1), 16-44.
- Laurinaitis, M., Štītis, D., ve Verenius, E. (2021). Implementation Of The Personal Data Minimization Principle In Financial Institutions: *Lithuania's case*. *Journal of*

Money Laundering Control, 24(4), 664-680.

Lim, C., Wang, Y., Ren, J., ve Lo, S. W. (2019). A Review Of Fast-Growing Blockchain Hubs In Asia. *The Journal of the British Blockchain Association*.

Loukaka, A. ve Rahman, S. S. (2020). Security Professionals Must Reinforce Detect Attacks To Avoid Unauthorized Data Exposure. *Information Technology in Industry*, 8(1).

Memnun, D. S. (2012). Sosyal Bilimler İçin Veri Analizi El Kitabı-Kitap Tanıtım Ve Değerlendirme. *Dicle Üniversitesi Ziya Gökalp Eğitim Fakültesi Dergisi* (18), 292-297.

Minnaar, A. ve Herbig, F. J. (2021). Cyberattacks And The Cybercrime Threat Of Ransomware To Hospitals And Healthcare Services During The COVID-19 Pandemic. *Acta Criminologica: African Journal of Criminology & Victimology*, 34(3), 155-185.

Mishra, A. (2022). Modern Cybersecurity Strategies for Enterprises: Protect and Secure Your Enterprise Networks, Digital Business Assets, and Endpoint Security with Tested and Proven Methods (English Edition). *BPB Publications*.

M. Yılmaz ve S. Ballı, “Veri Şifreleme Algoritmalarının Kullanımı İçin Akıllı Bir Seçim Sistemi Geliştirilmesi”, *Ubgmd*, c. 2, sy. 2, ss. 18–28, 2016, doi:10.18640/ubgmd.303580.

Naseeb, S. ve Khan, W. N. (2024). Mitigating Cybercrime through International Law: The Role of Global Cybersecurity Agreements. *Mayo Journal of Communication World*, 1(1), 31-40.

Natgunanathan, I., Mehmood, A., Xiang, Y., Beliaikov, G., ve Yearwood, J. (2016). Protection of privacy in biometric data. *IEEE access*, 4, 880-892

Ndou, V. (2004). E-Government For Developing Countries: Opportunities And Challenges. *Electron. J. Inf. Syst. Dev. Ctries.*, 18(1), 1-24.

Nissenbaum, H. (2004). Privacy As Contextual Integrity. *Wash. L. Rev.*, 79, 119.

Nunnally, J.C. ve Bernstein, I.H. (1994) The Assessment of Reliability. *Psychometric Theory*, 3, 248-292.

Ordu, A. (2021). Yükseköğretim Kurumlarında Örgütsel Farkındalık: Örgütsel Farkındalık Ölçeği'nin Türkçeye Uyarlanması. *MSGSÜ Sosyal Bilimler*, 1(23), 588-688.

Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., ve Beloev, I. (2024). A Comprehensive Survey: Evaluating The Efficiency Of Artificial Intelligence And Machine Learning Techniques On Cyber Security Solutions. *Ieee Access*, 12, 12229-12256.

Ökmen, P. Ve Çağatay, D. (2016). Kamu Hizmeti- Yerel Hizmet İlişkisi ve Açılımları Üzerine Notlar. *Yerel Politikalar* (6).

- Özdemir, A. ve Uluyol, Ç. (2021). Kamu Kurum Ve Kuruluşlarında Bilgi Güvenliği Farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi*, 25(3), 649-666.
<https://doi.org/10.20296/tsadergisi.815635>
- Özer Deniz, M. (2021). İşçilerin Özel Nitelikli Kişisel Verilerinin Korunması Ve Bundan Doğan Sorumluluk. *Türkiye Adalet Akademisi Dergisi* (45), 355-378.
- Özgür, E. ve Erciyes, E. (2017). Kamu Yönetiminde Yaşanan Dönüşümlerin İç Güvenlik Sektörüne Yansımaları. *Güvenlik Bilimleri Dergisi*, 6(1), 79-109.
<https://doi.org/10.28956/gbd.320011>
- Özkaya, Ö. ve Toprak, İ. (2022). Türkiye’de Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi. *MANAS Sosyal Araştırmalar Dergisi*, 11(3), 1291-1305.
<https://doi.org/10.33206/mjss.1098009>
- Özköse, H. (2020). Büyük Veri Kavramı ile İlgili Akademik Yayınların Metin Madenciliği Yöntemi ile Analizi. *Veri Bilimi*, 3(1), 11-20.
- Özyiğit, H. (2022). Kurumsal Risk Yönetimi ve Bulut Bilişim Sistemi. *Muhasebe ve Finansman Dergisi* (93), 31-52. <https://doi.org/10.25095/mufad.1012896>
- Paşaoğlu, C., Güler, H., ve Jafari, M. (2019). Ağ Tabanlı Veri Sızıntısı Tespiti Ve Önlenmesi Üzerine Bir İnceleme. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 3(2), 79-92.
- Polater, S. (2019). Kişisel Verilerin Reklam Amaçlı İşlenmesinde Hukuka Uygunluk Sebepleri. *Kişisel Verileri Koruma Dergisi*, 1(1), 1-20.
- Rai, H. M., Shukla, K. K., Tightiz, L., ve Padmanaban, S. (2024). Enhancing Data Security And Privacy In Energy Applications: Integrating Iot And Blockchain Technologies. *Heliyon*, 10(19).
- Rama, P. ve Keevy, M. (2023). Public Cybersecurity Awareness Good Practices On Government-Led Websites. *International Journal of Research in Business and Social Science* (2147-4478), 12(7), 94-104.
- Rosenbloom, D. H., Kravchuk, R. S., ve Clerkin, R. M. (2022). Public Administration: Understanding Management, Politics, And Law In The Public Sector. *Routledge*.
- Roshanaei, M. (2023). Cybersecurity Preparedness of Critical Infrastructure—A National Review. *Journal of Critical Infrastructure Policy*• Volume, 4(1).
- Sawiz, S. A. M. (2024). Yeni Dijital Teknolojilerin Denetim Süreçlerine Etkisi: Blockchain ve Yapay Zekânın Rolü (Yüksek Lisans Tezi), Selçuk Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı Muhasebe Finansman Bilim Dalı.
- Schneier, B. (2015). Secrets And Lies: Digital Security In A Networked World. John Wiley & Sons.
- Shahrullah, R. S., Park, J., ve Irwansyah, I. (2024). Examining personal data protection law

- of Indonesia and South Korea: The privacy rights fulfilment. *Hasanuddin Law Review*, 10(1), 1-20.
- Siponen, M., Mahmood, M. A., ve Pahlila, S. (2014). Employees' Adherence To Information Security Policies: An Exploratory Field Study. *Information & Management*, 51(2), 217-224.
- Solmaz, S. B. (2023). Siber Güvenlik Tarihindeki Dönüm Noktaları: Tehditlerin Evrimi Ve Savunma Stratejileri. *Orta Doğu Ve Orta Asya-Kafkaslar Araştırma Ve Uygulama Merkezi Dergisi*, 3(1), 1-9.
- Solove, D. J. (2004). The Digital Person: Technology And Privacy In The Information Age (Vol. 1). *NyU Press*.
- Supangkat, S. H., Firmansyah, H. S., Rizkia, I., ve Kinanda, R. (2025). Challenges in Implementing Cross-Border Digital Identity Systems for Global Public Infrastructure: A Comprehensive Analysis. *IEEE Access*.
- Stangl, A. L., Earnshaw, V. A., Logie, C. H., Van Brakel, W., C. Simbayi, L., Barré, I., ve Dovidio, J. F. (2019). The Health Stigma And Discrimination Framework: A Global, Crosscutting Framework To Inform Research, Intervention Development, And Policy On Health-Related Stigmas. *BMC medicine*, 17(1), 31.
- Stewart, H. ve Jürjens, J. (2017). Information Security Management And The Human Aspect In Organizations. *Information & Computer Security*, 25(5), 494-534.
- Swanzy, P. N., Abukari, A. M., ve Ansong, E. D. (2024). Data Security Framework For Protecting Data In Transit And Data At Rest In The Cloud. *Current Journal Of Applied Science And Technology*, 43(6), 61-77.
- Şıracı, S. (2023). Yüz Tanıma Teknolojilerinin Kişisel Verilerin Korunması Hukuku Açısından İncelenmesi. *Kişisel Verileri Koruma Dergisi*, 5(1), 23-46.
- Şişkin, D. Ş. ve 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>
- Tamer, H. Y. ve Övgün, B. (2023). Dijitalleşme Süreci Çerçevesinde Kamuda Stratejik Yönetim, *ODTÜ Gelişme Dergisi*, 509-538.
- Toros, F. (2025). Kişisel Veri Yönetimi Politikalarının İnsan Kaynakları Departmanı Üzerindeki Etkileri: Nitel Bir Analiz. *Sosyal Mucit. Academic Review*, 6 (1), 76-97. <https://doi.org/10.54733/smar.1540596>
- Tudosı, A. D., Graur, A., Balan, D. G., ve Potorac, A. D. (2023). Research on Security Weakness Using Penetration Testing in a Distributed Firewall. *Sensors*, 23(5), 2683.
- Tüminçin, F., Aytekin, A., ve Ayaz, A. (2019). Veri madenciliğinde karar ağacı algoritması, ADAB 5th International Social Research and Behavioral Sciences Symposium.

- Ural Uslan, Y. ve Değirmenci, S. (2023). Avrupa Birliği Genel Veri Koruma Tüzüğü Işığında Türkiye’de Kişisel Verileri Koruma Kurumu. *Optimum Ekonomi Ve Yönetim Bilimleri Dergisi*, 10(1), 23-38.
<https://doi.org/10.17541/optimum.1106817>
- URL-1 https://www.researchgate.net/figure/Distribution-of-the-10-most-attacked-sectors-by-attack-types-own-edition-based-on_fig2_384307297 (20.11.2024).
- URL-2 <https://gdpr-info.eu> (26.12.2024).
- URL-3 https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG (29.12.2024).
- URL-4 <https://www.pdpc.gov.sg/> (03.01.2025).
- URL-5 <https://laws-lois.justice.gc.ca/> (06.01.2025).
- URL-6 <https://www.legislation.gov.au/C2004A03712/latest/text> (05.01.2025).
- URL -7 <https://www.ncbi.nlm.nih.gov/books/NBK500019/> (07.01.2025).
- URL-8 (2016) <https://www.cybermagonline.com/anonymous-turkiyeye-yapilan-siber-saldirlarin-sorumlulugunu-kabul-etti> (12.02.2025).
- URL-9 (2020) <https://www.aa.com.tr/tr/bilim-teknoloji/salginin-etkisiyle-siber-saldirlarin-hedefi-saglik-sektoru-oldu/> 1852818 (13.02.2025).
- URL-10 (2018) <https://www.dgrnet.com.tr/2024/08/turkiyenin-maruz-kaldigi-simdiye-kadarki-en-buyuk-5-siber-saldiri/> (14.02.2025).
- URL-11 (2022) <https://siberbulten.com/siber-saldirlar-2/sisli-belediyesi-fidye-yazilim-saldirisina-ugradi/> (16.02.2025).
- Uslu, H. (2023). Dijital dönüşüm ve kamu hizmetleri yönetiminde yenilikçi yaklaşımlar ve zorluklar. *Uluslararası Politik Araştırmalar Dergisi*, 9(3), 15-31.
- Uysal, Y., Malkoç Yılmaz, K. (2025). Türkiye’de Kamu Yönetimin Dijital Kültür Üzerine Etkileri. *Kamu Yönetimi Ve Teknoloji Dergisi*, 7(1), 74-102.
<https://doi.org/10.58307/kaytek.1523213>
- Waind, E. (2020). Trust, Security And Public Interest: Striking The Balance A Narrative Review Of Previous Literature On Public Attitudes Towards The Sharing, Linking And Use Of Administrative Data For Research. *International Journal Of Population Data Science*, 5(3), 1368.
- Wallace, M. ve Webber, L. (2017). The Disaster Recovery Handbook: A Step-By-Step Plan To Ensure Business Continuity And Protect Vital Operations, Facilities, And Assets Amacom.
- Walters, R., Trakman, L., ve Zeller, B. (2019). Data Protection Law. *Springer Nature*.

- Wicaksono, F. D. N., Purbaratri, W., Alam, M. F. P., ve Safitri, A. N. I. (2024). IoT Security Attacks on the Public Sector: Systematic Literature Review. *Bit-Tech*, 7(1), 194-201.
- Winship, C. ve Mare, R. D. (1984). Regression Models With Ordinal Variables. *American Sociological Review*, 512-525.
- Van Rest, J., Boonstra, D., Everts, M., van Rijn, M., ve van Paassen, R. (2012, October). Designing Privacy-By-Design. In Annual Privacy Forum (pp. 55-72). *Berlin, Heidelberg: Springer Berlin Heidelberg*.
- Voigt, P. ve Von dem Bussche, A. (2017). The Eu General Data Protection Regulation (gdpr). *A practical guide, 1st ed., Cham: Springer International Publishing*, 10(3152676), 10-5555.
- Voss, W. G. ve Bouthinon-Dumas, H. (2021). EU General Data Protection Regulation Sanctions In Theory And In Practice. *Santa Clara High Tech. LJ*, 37, 1.
- Yağar, F. ve Dökme, S. (2018). Niteliksel Araştırmaların Planlanması: Araştırma Soruları, Örneklem Seçimi, Geçerlik ve Güvenirlilik. *Gazi Sağlık Bilimleri Dergisi*, 3(3),1-9.
- Yamane, T. (1973) Statistics: An Introductory Analysis. *3rd Edition, Harper and Row, New York*.
- Yoganandham, G. (2024). Digital Transformation Of Welfare Services In Tamil Nadu: Economic Implications, Fraud Risks, And Privacy Challenges In The Integration Of Aadhaar And Pan Card Systems-A Comprehensive Assessment. *Degrés*, 9(12).
- Yosif, U. (2021). Kişisel Verilerin İşlenmesi Şartları ve 6698 Sayılı Kişisel Verilerin Korunması Kanununun Ruhu Olarak Genel İlkeler. *Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi*, 4(1), 1-22.
- Yücedağ, N. (2019). Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler. *Kişisel Verileri Koruma Dergisi*, 1(1), 47-63.
- Zehir, C., Bilgetürk, M. (2023). Büyük Veri Analitiği Yeteneği Ve Firma Performansı İlişkisi: Firma Büyüklüğünün Düzenleyici Rolü. *Yıldız Sosyal Bilimler Enstitüsü Dergisi*, 6(2), 62-73. <https://doi.org/10.14744/ysbed.2022.00019>

EKLER

Bu bölümde, araştırma kapsamında kullanılan veri toplama aracı olan anket formu ile çalışmanın etik uygunluğunu gösteren resmî belgeye yer verilmiştir.

EK 1: Anket formu

“Kamu sektöründe veri güvenliği ve mahremiyeti ile ilgili sorunlar ve çözüm önerileri” adlı yüksek lisans tezi anketi

Bu çalışma, “Kamu Sektöründe Veri Güvenliği ve Mahremiyeti ile İlgili Sorunlar ve Çözüm Önerileri” adlı tez çalışması için veri toplama amacı ile yapılmaktadır. Çalışma verileri herhangi bir kişi, kurum veya kuruluş ile paylaşılmadan gizlilik ilkeleri esasıyla değerlendirilecektir. Lütfen size en uygun olan yanıtı objektif bir şekilde işaretleyiniz. Feyza SÜMER Bartın Üniversitesi, Yönetim Bilişim Sistemleri Yüksek Lisans Öğrencisi Prof. Dr. Alper AYTEKİN (Bartın Üniversitesi, Yönetim Bilişim Sistemleri Bölümü)	Her zaman	Sık sık	Ara sıra	Nadiren	Hiçbir zaman
Bölüm 1: Aşağıda veri güvenliği ve veri mahremiyeti ile ilgili birtakım sorular yer almaktadır. Bu soruları cevaplarken yan tarafta bulunan seçeneklerden size en uygun olan seçenek ve/veya seçenekleri işaretleyiniz. 1-Hiçbir zaman 2-Nadiren 3-Ara sıra 4-Sık sık 5-Her zaman					
1.1. Veri güvenliği ve mahremiyeti kavramları hakkında bilginiz var mı?					
1.2. Çalıştığınız kurumda veri güvenliği ve mahremiyeti politikalarını biliyor ve riayet ediyor musunuz?					
1.3. Çalıştığınız kurumda verilerinizin güvenliğinden ve mahremiyetinden endişe duyuyor musunuz?					
1.4. Çalıştığınız kurumda veri güvenliği ve mahremiyeti ile ilgili sorunların sıklıkla görüldüğünü düşünüyorsunuz?					
1.5. Çalıştığınız kurumda veri güvenliği ve mahremiyeti ile ilgili hiç eğitim aldınız mı?					
1.6. Çalıştığınız kurumda veri güvenliği ve mahremiyeti ihlallerinden herhangi birine (phishing, bilgisayar virüsleri, kötü amaçlı yazılımlar vb.) hiç tanık oldunuz mu?					
1.7. Kurumunuzda veri güvenliği ve mahremiyeti politikaları ve prosedürleri yeterli mi?					
1.8. Kurumunuzda kullandığınız sistem veri güvenliği ve mahremiyeti açısından güncel mi?					
1.9. Kurumunuz veri mahremiyeti ile ilgili yasal düzenlemelere tam uyum sağlıyor mu?					
1.10. Kurumunuzda veri güvenliği ve mahremiyeti ile ilgili alınan önlemler sizi tatmin ediyor mu?					
Bölüm 2: Aşağıda veri güvenliği ve veri mahremiyeti ile ilgili çözüm önerileri yer almaktadır. Bu soruları cevaplarken yan tarafta bulunan seçeneklerden size en uygun olan seçenek ve/veya seçenekleri işaretleyiniz. 1-Hiçbir zaman 2-Nadiren 3-Ara sıra 4-Sık sık 5-Her zaman					
2.1. Kamu sektöründe veri güvenliği ve mahremiyeti sorunlarını çözmenin önemli olduğunu düşünüyor musunuz?					
2.2. Veri güvenliği ve mahremiyeti ile ilgili kapsamlı eğitim ve farkındalık programları oluşturma öneminin nasıl değerlendiriyorsunuz?					

2.3. Veri güvenliğiyle ilgili yaşanan sorunlar için çözüm önerileri geliştirilmesi konusunda katkıda bulunuyor musunuz?					
2.4. Veri güvenliği konusunda çalışanların önerileri dikkate alınıyor mu?					
2.5. Veri güvenliğiyle ilgili sorun yaşandığında kurum içinde açık bir şekilde tartışılıyor mu?					
2.6. Teknolojik çözümlerle veri güvenliği ve mahremiyeti artırılabilir mi?					
2.7. Güvenlik duvarları ve antivirüs yazılımlar kullanmak veri güvenliği ve mahremiyetini korumak için yeterli midir?					
2.8. Kamu sektöründeki veri güvenliği ve mahremiyeti ile ilgili sorunların çözümüne katkıda bulunmak için özel sektör şirketler ile işbirliği yapılmalı mıdır?					
2.9. Kurumunuzda veri güvenliği ile ilgili önlemler alındığında bu önlemler tüm çalışanlara etkili bir şekilde duyuruluyor mu?					
2.10. Kurumunuzda veri güvenliği ve mahremiyeti ile ilgili sorunlarının çözümü için yeterli ödenek ayrılıyor mu?					

Bölüm 3: Katılımcılara ait demografik bilgiler.				
Cinsiyet:	☐ Bay	☐ Bayan		
Yaşınız:	☐ 21-25	☐ 26-30	☐ 31-40	☐ 41 ve üstü
Kurumunuzdaki görev süreniz	☐ 0-5 yıl	☐ 5-10 yıl	☐ 10-15 yıl	☐ 15 yıl ve üstü
Göreviniz:	☐ Memur ☐ Teknik Personel ☐ Müdür ☐ Hizmetli ☐ Diğer (Belirtiniz:)			
Eğitim Durumunuz:	☐ Lise ☐ Önlisans ☐ Lisans ☐ Yüksek lisans			
Yaşadığınız coğrafi bölge:	☐ Marmara ☐ İç Anadolu ☐ Ege ☐ Karadeniz ☐ Akdeniz ☐ Doğu Anadolu ☐ Güneydoğu Anadolu			

EK 2: Etik Kurulu onay belgesi



T.C.
BARTIN ÜNİVERSİTESİ REKTÖRLÜĞÜ
Sosyal ve Beşeri Bilimler Etik Kurulu
Onay Belgesi

TOPLANTI SAYISI
11

KARAR SAYISI
1

TOPLANTI TARİHİ
18.06.2025

Protokol No:	2025-SBB-0644
Araştırmanın Başlığı:	Kamu Sektöründe Veri Güvenliği ve Veri Mahremiyeti ile İlgili Sorunlar ve Çözüm Önerileri
Proje Yürütücüsü:	Feyza SÜMER
Başvuru Formunun Geliş Tarihi:	28.05.2025

Başvuru dosyasında etik sorun oluşturabilecek sorular/maddeler, süreçler ya da unsurlar bulunmadığından 18.06.2025 tarihli ve 11 numaralı toplantıda 2025-SBB-0644 numaralı başvuruya araştırma için ETİK KURUL ONAY belgesinin verilmesine karar verilmiştir.

Prof. Dr. Ayla ÇETİN DİNDAR
Başkan

Doç. Dr. Hilal UYSAL
Başkan yardımcısı

Doç. Dr. Mehmet
ALTUNMERAL
Üye

Doç. Dr. Sevda KAMAN
Üye

Dr. Öğr. Üyesi Nergiz TEKE
Üye

Dr. Öğr. Üyesi Sevim
Handan YILMAZ
Üye

Dr. Öğr. Üyesi Sevinç
AKKAYA TAHTA
Üye

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Feyza SÜMER

Doğum Yeri ve Tarihi :

Eğitim Durumu

Lisans Öğrenimi : Yönetim Bilişim Sistemleri / Bartın Üniversitesi

Yüksek Lisans Öğrenimi : YBS Anabilim Dalı / Bartın Üniversitesi

Bildiği Yabancı Diller : İngilizce

Bilimsel Faaliyet/Yayınlar : The effect of metaverse Technologies on education and human-computer interaction: A systematic analysis of the literature

Aldığı Ödüller :

İş Deneyimi

Stajlar :

Projeler ve Kurs Belgeleri :

Çalıştığı Kurumlar : Erzincan Valiliği / İçişleri Bakanlığı (Şef)

İletişim

E-Posta Adresi :

Tarih : 04/11/2025 (Tez Savunma Tarihi)

