

T.C.
İSTANBUL KENT ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
İŞLETME YÖNETİMİ BİLİM DALI



İSTANBUL KENT
ÜNİVERSİTESİ

KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK KURUMSAL
FARKINDALIK İLE ÇALIŞANLARIN GÜVEN DÜZEYİ
ARASINDAKİ İLİŞKİ: BİR ARAŞTIRMA

YÜKSEK LİSANS TEZİ

MURAT BAYBALI

İSTANBUL – 2025

T.C.
İSTANBUL KENT ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
İŞLETME YÖNETİMİ BİLİM DALI



İSTANBUL KENT
ÜNİVERSİTESİ

KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK KURUMSAL
FARKINDALIK İLE ÇALIŞANLARIN GÜVEN DÜZEYİ
ARASINDAKİ İLİŞKİ: BİR ARAŞTIRMA

YÜKSEK LİSANS TEZİ

MURAT BAYBALI

Tez Danışmanı: Doç. Dr. Bülent DEMİR

İSTANBUL – 2025

KABUL VE ONAY

Murat BAYBALI tarafından hazırlanan “Kişisel Verilerin Korunmasına Yönelik Kurumsal Farkındalık İle Çalışanların Güven Düzeyi Arasındaki İlişki: Bir Araştırma” adlı tez çalışmasının savunma tarihi 16.09.2025 tarihinde yapılmış olup aşağıda verilen jüri tarafından oy birliği ile İstanbul Kent Üniversitesi Lisansüstü Eğitim Enstitüsü İşletme Anabilim Dalı İşletme Yönetimi Bilim Dalı Yüksek Lisans olarak kabul edilmiştir.

Jüri Üyeleri

İmza

Danışman

Doç. Dr. Bülent DEMİR

.....

Üye

Doç. Dr. Murat SAĞBAŞ

.....

Üye

Dr. Öğr. Üyesi Serkan AKGÜN

.....

İstanbul Kent Üniversitesi Lisansüstü Eğitim Enstitüsü Yönetim Kurulu’nun tarih ve sayılı kararıyla onaylanmıştır.

.....

Doç. Dr. Bülent DEMİR

Lisansüstü Eğitim Enstitüsü Müdürü

BEYAN

Bu tezin yazılmasında bilimsel ahlak kurallarına uyulduğunu, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, tezin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir tez çalışması olarak sunulmadığını beyan ederim.

Murat BAYBALI

16.09.2025



ÖN SÖZ

Bu tezin yazılması aşamasında, çalışmamı sahiplenerek titizlikle takip eden danışmanım Doç. Dr. Bülent DEMİR'in değerli katkı ve emekleri için içten teşekkürlerimi ve saygılarımı sunarım. Doç. Dr. Bülent DEMİR bütün süreç boyunca her anlamda yanımda olmuş, desteğini ve katkılarını esirgememiştir. Savunma sınavı sırasında jüri üyeleri çalışmamın son haline gelmesine değerli katkılar yapmışlardır. Bu vesileyle tüm hocalarıma ve tezimin son okumasında yardımlarını esirgemeyen yakınlarıma teşekkürlerimi borç bilirim. Son olarak bu günlere ulaşmamda emeklerini hiçbir zaman ödeyemeyeceğim anneme ve aileme şükranlarımı sunarım.

Murat BAYBALI

16.09.2025

İÇİNDEKİLER

KISALTMALAR.....	i
TABLO LİSTESİ	ii
ÖZET	iii
ABSTRACT	iv
GİRİŞ.....	1
BÖLÜM 1: KİŞİSEL VERİLERİN KORUNMASI VE KURUMSAL FARKINDALIK.	3
2.1. Kişisel Veriler ve Korunması	4
2.1.1. Kişisel Veri Kavramı	4
2.1.2. Özel Nitelikli Kişisel Veriler	5
2.1.3. Kişisel Verilerin İşlenmesi Süreçleri	5
2.1.4. Kişisel Verilerin Korunmasının Önemi	7
2.1.5. Kişisel Veri İhlali ve Sonuçları	8
2.2. Kişisel Verilerin Korunmasına İlişkin Hukuki Düzenlemeler	9
2.2.1. Türkiye’de Kişisel Verilerin Korunması Kanunu (KVKK)	9
2.2.2. Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)	10
2.2.3. Kişisel Verilerin Korunmasında Kurumların Yükümlülükleri ve Çalışanların Sorumlulukları	11
2.3. Kurumsal Farkındalık	12
2.3.1. Kurumsal Farkındalık Kavramı	12
2.3.2. Kişisel Verilerin Korunmasında Kurumsal Farkındalığın Rolü	14
2.3.3. Farkındalık Oluşturmaya Yönelik Kurumsal Uygulamalar.....	14
2.3.4. Bilgilendirme, Eğitim ve İç Denetim	15
BÖLÜM 2: GÜVEN KAVRAMI VE KİŞİSEL VERİLER BAĞLAMINDA LİTERATÜR İNCELEMESİ	16
3.1. Güven Kavramı.....	16
3.1.1. Güvenin Tanımı ve Boyutları	18
3.1.2. Örgütsel Güvenin Temelleri	19
3.1.3. Çalışanların Kuruma Olan Güveni	19
3.1.4. Güvenin Kurum Kültürü Üzerindeki Etkisi.....	20
3.2. Kişisel Veri Güvenliği ile Çalışan Güveni Arasındaki İlişki	22
3.2.1. Gizlilik Algısının Güvene Etkisi	23
3.2.2. Şeffaflık, Denetim ve Güven	24
3.2.3. Kurumsal Etik ve Güven İlişkisi	25

3.2.4. Bilgi Güvenliği İhlalleri ve Psikolojik Etkiler.....	25
3.3. Kişisel Verilerin Korunması Kanunu (KVKK) ve Güven.....	26
3.3.1. KVKK'nın Çalışanlar Açısından Önemi	27
3.3.2. Yasal Düzenlemelerin Güven Algısına Katkısı.....	27
3.3.3. KVKK İhlalleri ve Kurumsal Güven Kayıpları.....	27
BÖLÜM 3: ARAŞTIRMA METODOLOJİSİ	29
3.1. Araştırmanın Amacı ve Önemi	29
3.2. Araştırmanın Sınırlılıkları.....	29
3.3. Araştırmada Kullanılan Ölçekler	30
3.4. Araştırmanın Örneklemi	31
3.5. Araştırmanın Modeli.....	32
3.6. Veri Toplama Yöntemleri.....	32
3.7. Konuyla İlgili Yapılmış Çalışmalar.....	33
3.8. Araştırmanın Hipotezleri	34
3.9. Demografik Bulgular.....	34
3.10. Tanımlayıcı İstatistikler.....	35
3.11. Regresyon Analizi Sonuçları	37
3.12. Hipotez Testleri	39
SONUÇ VE ÖNERİLER	45
KAYNAKÇA	49
ÖZGEÇMİŞ	56

KISALTMALAR

DPA:	Veri işleme sözleşmesi
DPIA:	Veri koruma etki değerlendirmesi
DPO:	Veri Koruma Görevlisi
GDPR:	Genel Veri Koruma Yönetmeliği
KVKK:	Kişisel Verileri Koruma Kurumu
VERBİS:	Veri Sorumluları Sicili



TABLO LİSTESİ

Tablo 1: Katılımcıların Demografik Özellikleri.....	34
Tablo 2: Ölçek Maddelerine İlişkin Tanımlayıcı İstatistikler.....	35
Tablo 3: Kişisel Verilerin Korunmasına Yönelik Kurumsal Farkındalık ve Çalışanların Güven Düzeyi Arasındaki Korelasyon.....	37
Tablo 4: Regresyon Model Özeti.....	37
Tablo 5: Regresyon Modeline İlişkin ANOVA Sonuçları.....	38
Tablo 6: Regresyon Katsayıları.....	38
Tablo 7: Cinsiyete Göre KVK Farkındalık ve Güven Düzeyi Puanları.....	39
Tablo 8: Yaş Gruplarına Göre KVK Farkındalık ve Güven Düzeyi Puanları.....	40
Tablo 9: Yaş Gruplarına Göre ANOVA Sonuçları.....	40
Tablo 10: Yaş Gruplarına Göre Tukey HSD Post-Hoc Testi Sonuçları (KVK Farkındalık).....	40
Tablo 11: Eğitim Durumuna Göre KVK Farkındalık ve Güven Düzeyi Puanları.....	41
Tablo 12: Eğitim Durumuna Göre ANOVA Sonuçları.....	41
Tablo 13: Eğitim Durumuna Göre Tukey HSD Post-Hoc Testi Sonuçları (KVK Farkındalık).....	42
Tablo 14: Kurumda Çalışma Süresine Göre KVK Farkındalık ve Güven Düzeyi Puanları.....	42
Tablo 15: Kurumda Çalışma Süresine Göre ANOVA Sonuçları.....	42
Tablo 16: Kurumda Çalışma Süresine Göre Tukey HSD Post-Hoc Testi Sonuçları (KVK Farkındalık).....	43
Tablo 17: KVK Eğitimi Alma Durumuna Göre KVK Farkındalık ve Güven Düzeyi Puanları.....	43

ÖZET

İstanbul Kent Üniversitesi Lisansüstü Eğitim Enstitüsü
Kişisel Verilerin Korunmasına Yönelik Kurumsal Farkındalık İle Çalışanların
Güven Düzeyi Arasındaki İlişki: Bir Araştırma

Murat BAYBALI

Yüksek Lisans Tezi

İşletme Anabilim Dalı / İşletme Yönetimi Bilim Dalı

Danışman: Doç. Dr. Bülent DEMİR

2025 – 67

Bu araştırma, kişisel verilerin korunmasına yönelik kurumsal farkındalık düzeyinin çalışanların kuruma duyduğu güven üzerindeki etkisini incelemeyi amaçlamaktadır. Araştırmanın örneklemini, İstanbul'da faaliyet gösteren bir kamu kurumunda çalışan 250 personel oluşturmaktadır. Veri toplama aracı olarak, kişisel verilerin korunmasına yönelik kurumsal farkındalık ve çalışanların güven düzeyini ölçen anketler kullanılmıştır. Araştırma sonucunda, kişisel verilerin korunmasına yönelik kurumsal farkındalık ile çalışanların güven düzeyi arasında anlamlı ve pozitif bir ilişki olduğu tespit edilmiştir ($r = 0,62$, $p < 0,01$). Regresyon analizi, kurumsal farkındalığın çalışanların güven düzeyindeki varyansın %38'ini açıkladığını göstermiştir ($R^2 = 0,38$). Ayrıca, yaş, eğitim düzeyi, kurumda çalışma süresi ve kişisel verilerin korunması eğitimi alma durumu gibi demografik değişkenlerin hem kurumsal farkındalık hem de güven düzeyi üzerinde anlamlı etkisi olduğu belirlenmiştir. Bu bulgular, kurumların kişisel verilerin korunmasına yönelik farkındalık düzeylerini artırmalarının, çalışanların güven düzeyini olumlu yönde etkilediğini ortaya koymaktadır. Kurumların veri koruma politikalarını güçlendirmeleri ve çalışanlarına yönelik düzenli eğitim programları düzenlemeleri, çalışanların güven düzeyini artırmada etkili olabilir.

Anahtar Kelimeler: Kişisel Verilerin Korunması, Kurumsal Farkındalık, Çalışan Güveni, Veri Koruma, KVKK

ABSTRACT

Istanbul Kent University Postgraduate Education Institute

The Relationship Between Corporate Awareness and Employee Trust Level

Regarding the Protection of Personal Data: A Study

Murat BAYBALI

Master Thesis

Business Administration Division / Business Management Discipline

Supervisor: Associate Bülent DEMİR

2025 – 67

This research aims to examine the effect of corporate awareness level regarding the protection of personal data on employees' trust in the organization. The sample of the research consists of 250 personnel working in a public institution operating in Istanbul. Surveys measuring corporate awareness regarding the protection of personal data and employees' trust level were used as data collection tools. As a result of the research, a significant and positive relationship was found between corporate awareness regarding the protection of personal data and employees' trust level ($r = 0.62$, $p < 0.01$). Regression analysis showed that corporate awareness explained 38% of the variance in employees' trust level ($R^2 = 0.38$). In addition, it was determined that demographic variables such as age, education level, working time in the institution, and receiving training on the protection of personal data had a significant effect on both corporate awareness and trust level. These findings reveal that increasing the awareness level of institutions regarding the protection of personal data positively affects employees' trust level. Strengthening data protection policies and organizing regular training programs for employees can be effective in increasing employees' trust level.

Keywords: Protection Of Personal Data, Corporate Awareness, Employee Trust, Data Protection, Kvkk.

GİRİŞ

Dijital dönüşümün hızla ilerlediği günümüz iş dünyasında, kişisel verilerin korunması hem yasal bir zorunluluk hem de kurumsal itibar açısından kritik öneme sahip bir konuya haline gelmiştir. Özellikle son yıllarda yaşanan veri ihlalleri ve siber güvenlik tehditleri, kurumların veri güvenliği politikalarını gözden geçirmelerini ve bu konuda daha proaktif adımlar atmalarını gerektirmektedir. Bu bağlamda, kurumların kişisel verilerin korunmasına yönelik farkındalık düzeyleri ile çalışanların kurumlara duydukları güven arasındaki ilişki, incelenmesi gereken önemli bir araştırma alanı olarak karşımıza çıkmaktadır.

Kişisel verilerin korunması, yalnızca teknik önlemlerle sağlanabilecek bir güvenlik meselesi değil, aynı zamanda kurumsal kültürün ve çalışan davranışlarının şekillendirdiği kapsamlı bir süreçtir. Kurumların bu konudaki farkındalıkları ve uyguladıkları politikalar, çalışanların kuruma olan güvenini doğrudan etkilemektedir. Çalışanlar, kişisel verilerinin güvende olduğuna inandıklarında, kurumlarına karşı daha yüksek düzeyde güven ve bağlılık geliştirmektedirler.

Bu araştırma, kişisel verilerin korunmasına yönelik kurumsal farkındalık ile çalışanların güven düzeyi arasındaki ilişkiyi incelemeyi amaçlamaktadır. Çalışma kapsamında, kurumların veri koruma politikaları, bu politikaların çalışanlara aktarılma biçimleri ve çalışanların bu politikalara yönelik algıları detaylı olarak ele alınacaktır. Ayrıca, kurumsal farkındalığın çalışan güveni üzerindeki etkisi, farklı sektörler ve kurum büyüklükleri açısından karşılaştırmalı olarak analiz edilecektir.

Türkiye'de 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve uluslararası alanda geçerli olan Genel Veri Koruma Yönetmeliği (GDPR) gibi düzenlemeler, kurumların veri koruma konusundaki sorumluluklarını artırmıştır. Bu yasal çerçeve, kurumların kişisel verilerin işlenmesi, saklanması ve korunması konusunda daha şeffaf ve hesap verebilir olmalarını gerektirmektedir. Dolayısıyla, kurumların bu yasal gerekliliklere uyum sağlama düzeyleri, çalışanların güven algısını şekillendiren önemli faktörlerden biridir.

Bu araştırmanın sonuçları, kurumların kişisel verilerin korunmasına yönelik farkındalık düzeylerini artırmak ve çalışan güvenini güçlendirmek için geliştirebilecekleri

stratejilere ışık tutacaktır. Ayrıca, veri koruma politikalarının etkinliğini artırmak ve kurumsal güven kültürünü geliştirmek isteyen yöneticiler için pratik öneriler sunacaktır.



BÖLÜM 1: KİŞİSEL VERİLERİN KORUNMASI VE KURUMSAL FARKINDALIK

Kişisel verilerin korunması ve kurumsal farkındalık, günümüz dijital ekosisteminde giderek daha kritik hale gelen temel bir sorundur; çünkü bireylerin kimlikleri, özel hayatları ve davranışsal verileri, bir kuruma ait bilgi sistemlerinde işlenirken güvenlik açıkları, ihlaller veya yetkisiz paylaşım yoluyla zarar görebilir ve bu durum hem bireylerin mahremiyet haklarına zarar verir hem de kurumun itibarını, yasal uyumunu ve operasyonel güvenliğini olumsuz yönde etkiler (Ağıralan ve Yiğit, 2015). Bu nedenle kurumsal düzeyde güçlü bir veri koruma kültürü oluşturmak için önce üst yönetimin güvenli veri işleme politikalarını benimsemesi, tüm çalışanların sürekli eğitimlerle bilinçlendirilmesi, kişisel verilerin hangi amaçlarla, hangi hukuki zemine dayanarak ve hangi sürelerle işlendiğinin açıkça tanımlanması, veri envanterinin ve risk değerlendirme süreçlerinin düzenli olarak güncellenmesi, teknik ve organizasyonel tedbirlerin (erişim kontrolleri, şifreleme, veri minimizasyonu, anonimleştirme, kayıt ve bildirim mekanizmaları gibi) sürekli uygulanması ve ayrıca tedarik zincirindeki üçüncü taraflarla veri paylaşımının güvenlidir, uyumlu ve sözleşme ile güvence altına alınmış olması gerekir; bu çerçevede farkındalık, yalnızca bir uyum gereci olarak kalmamalı, aynı zamanda günlük iş akışlarının her aşamasında bir karar desteği ve davranış standartı olarak benimsenmelidir (Yılmaz, Gönen ve Ulus, 2016).

Çalışanlar için farkındalık eğitimleri, veri sınıflandırması, güvenli geliştirme yaşam döngüsü, güvenlik olaylarına müdahale planı ve etik ilkelere dayalı bir yaklaşımın entegrasyonunu kapsamalıdır. Kuruluşlar, yasa koyucuların belirlediği veri koruma mevzuatına uygunluğu sağlamanın yanı sıra kurum içi iletişim ve hesap verebilirlik mekanizmalarını güçlendirerek, kullanıcı taleplerine hızlı ve şeffaf yanıt verebilme, ihlal durumlarında etkili bildirim süreçlerini işletme ve sürekli iyileştirme için geribildirim döngülerini kurma sorumluluğunu taşırlar. Bu unsurlar bir araya geldiğinde, yalnızca yasal bir zorunluluk olarak kalmayan, aynı zamanda güvene dayalı müşteri ve çalışan ilişkileri inşa eden, inovasyonu destekleyen ve rekabet avantajı sağlayan bütünsel bir veri güvenliği kültürünün oluşmasına zemin hazırlar (Olca ve Can, 2014).

2.1. Kişisel Veriler ve Korunması

Kişisel verilerin korunması, bireylerin mahremiyetinin güvenli bir şekilde sağlanması için kurumsal süreçlerin, teknik tedbirlerin ve yasal uyumun bütüncül bir şekilde entegre edilmesini gerektiren bir sorumluluktur. Bu kapsamda veri envanteri, amaçla sınırlama, veri minimizasyonu, uygun saklama süreleri, güçlü erişim kontrolleri, şifreleme ve anonimleştirme gibi tedbirler sürekli uygulanır (Kılınç, 2012). Çalışan farkındalığı ve eğitimlerle desteklenen bir kurumsal kültür oluşturulur, veri sahiplerinin hakları gözetilir, ihlal durumlarında hızlı bildirim ve etkili müdahale mekanizmaları devreye alınır, tedarik zincirinde de güvenliğini sözleşmelerle güvence altına almak suretiyle hem yasal uyum sağlanır hem de müşteri ve çalışan güveni ile rekabet avantajı güçlendirilir (Dülger, 2016).

2.1.1. Kişisel Veri Kavramı

Kişisel Veri kavramı, belirli veya belirlenebilir bir kişinin kimliğini doğrudan veya dolaylı olarak tanımlayan her türlü bilgiyi kapsayan geniş bir terimdir; bu kapsama örnek olarak ad, soyadı, kimlik numarası, adres, iletişim bilgileri, doğum tarihi, fotoğraf, ses kaydı, konum verileri, sağlık bilgileri, finansal bilgiler, sosyal medya aktiviteleri ve çevrimiçi davranış izleri gibi veri türleri girer (Altundiş, 2016).

IP adresleri, çerezlerle ilişkilendirilen kullanıcı davranışları ve cihaz kimlikleri gibi dolaylı veriler de belirli bir kişiyle ilişkilendirilebildiğinde kişisel veri olarak kabul edilir. Kişisel veriler, topluca veya tekil halde işlendiğinde bir kişinin mahremiyetini, güvenliğini ve temel haklarını etkileyebileceği için, çoğu ülkede belirli yasal çerçeveler ve yükümlülükler kapsamında korunur. Bu koruma, veri minimizasyonu, amaçla sınırlama, güvenli işleme, saklama sürelerinin belirlenmesi ve bireylerin haklarına saygı gösterilmesi gibi prensiplerle sağlanır. Kişisel veri kavramını doğru uygulamak için organizasyonlar, hangi verilerin kişisel olduğunu, nasıl işlendiğini, hangi amaçlarla toplandığını ve hangi paydaşlarla paylaşıldığını açıkça tanımlamalı, uygun güvenlik tedbirlerini uygulamalı ve ilgili mevzuata uyum süreçlerini sürdürmelidir. İstersen bu kavramı bir kurum bağlamında kısa bir özet veya belirli bir mevzuata uygun açıklamalarla daha da ayrıntılandırabilirim (İzgi, 2014).

2.1.2. Özel Nitelikli Kişisel Veriler

Özel nitelikli kişisel veriler, bir kişinin ırk veya etnik kökeni, siyasi görüşleri, dini veya felsefi inançları, sendika üyeliği gibi geçmişe bağlı veya kimlik açısından hassas bilgileri ile sağlık, biyometrik veriler, genetik veriler ve cinsel yaşam veya yönelim gibi yüksek düzeyde koruma gerektiren verileri kapsar; bu tür verilerin işlenmesi, kişinin temel hak ve özgürlüklerini ciddi şekilde etkileyebileceği için yalnızca açık rıza, mevzuatta öngörülen sıkı istisnalar veya diğer yasal gerekçelerle mümkündür (Gürsel, 2016).

Amaçla sınırlama ve veri minimizasyonu ilkeleriyle sadece belirlenen ve yasal olarak uygun görülen amaçlar için işlenir; yüksek güvenlik tedbirleri (şifreleme, anonimleştirme, erişim sınırlamaları, güvenli depolama) uygulanır, saklama süreleri net olarak belirlenir ve süre sonunda güvenli imha veya anonimleştirme yapılır. Veri sahibinin hakları (rızanın geri alınması, erişim, düzeltme, silme, işlenmesini kısıtlama, taşınabilirlik) açıkça korunur ve ihlal durumlarında bildirim mekanizmaları ile hesap verebilirlik sağlanır. Üçüncü taraflarla paylaşım sözleşmelerle güvence altına alınır ve gerektirdiğinde tedarik zinciri yönetimi güvenli şekilde yürütülür. İstersen bu konuyu bir kurum için politika özeti, risk taslağı veya farkındalık içerikleri şeklinde daha da derinleştirebilirim (Tezcan, 2013).

2.1.3. Kişisel Verilerin İşlenmesi Süreçleri

Bir kurumun kişisel verileri güvenli ve yasal bir şekilde işlemesini sağlayan süreçler, genellikle şu aşamalı zinciri kapsar: veri envanteri ve sınıflandırma, amaçla sınırlama ve veri minimizasyonu, toplama ve kayıttan yürütme, saklama sürelerinin belirlenmesi ve güvenli imha, erişim yönetimi ve güvenlik önlemleri, veri paylaşımı ve tedarikçi yönetimi, birey haklarının yönetimi, ihlal yönetimi ve bildirim mekanizmaları, uyum izleme ve sürekli iyileştirme (İleri, 2016). Aşağıda bu aşamalar yer almaktadır;

- **Veri Envanteri ve Sınıflandırma:** Hangi verilerin işlendiğini, kimlerin erişebildiğini, hangi amaçlarla işlendiğini ve hangi yasal dayanakların kullanıldığını belirleyen kapsamlı bir envanter oluşturulur; veriler hassas/özel nitelikli olup olmadıklarına göre sınıflandırılır (Kartal, 2012).

- **Amaçla Sınırlama ve Veri Minimizasyonu:** Veriler sadece belirli, meşru ve açıkça ifade edilmiş amaçlar için toplanır; ihtiyaçtan fazlası toplanmaz (Kılınç, 2012). Gereksiz veri işleme faaliyetleri engellenir.
- **Toplama ve Kayıt:** Verinin nasıl toplandığı (kullanıcıdan, otomatik sistemlerden, ortaklaşa veri akışlarından) ve hangi haklar bağlamında işlendiği kayıt altına alınır; açık rıza, yasal dayanak veya istisnalar net olarak belgelenir (Tekin, 2014).
- **Güvenli Saklama ve İmha:** Verilerin saklama süreleri belirlenir; süre dolduğunda güvenli imha veya anonimleştirme süreçleri işletilir. Yedekleme ve felaket kurtarma planları buna göre tasarlanır (Küçüköğlu, Polat ve Güdek, 2013).
- **Erişim Yönetimi ve Teknik-Organizasyonel Tedbirler:** Erişim kontrolleri, kimlik doğrulama, yetkilendirme süreçleri, veri şifreleme, anonimleştirme ve veri minimizasyonu gibi tedbirler uygulanır; güvenlik olaylarına müdahale planları hazırır.
- **Veri Paylaşımı ve Tedarikçi Yönetimi:** Üçüncü taraflarla veri paylaşımı, sözleşme güvence şartları, veri işlemlerini sınırlayıcı hükümler ve denetim mekanizmaları ile yönetilir; tedarik zinciri güvenliği için risk değerlendirmeleri yapılır (İbrahim, 2009).
- **Birey Haklarının Yönetimi:** Verilere erişim, düzeltme, silme (yeniden işleme için saklama sınırları dahil), işlenmesini kısıtlama, veri taşınabilirliği ve itiraz hakları için prosedürler belirlenir; talepler için belirli süreler içinde yanıt verilir.
- **İhlal Yönetimi ve Bildirim:** Veri ihlallerinde hızlı tespit, sınıflandırma, gereğini yerine getirme (ihbar, etkili iletişim, düzeltici adımlar) ve gerektiğinde yetkili otoritelere bildirim süreçleri kurulur (Akıllı, Çam, Kılınç ve Kızılboğa, 2013).
- **Uyum İzleme ve İç Denetim:** Politikaların, prosedürlerin ve mevzuat uyumunun düzenli olarak izlenmesi, iç denetimler, risk değerlendirmeleri ve düzeltici faaliyetlerin uygulanması.

- **Sürekli İyileştirme:** Öğrenilen dersler, yeni riskler ve teknolojik gelişmelere göre süreçler güncellenir; farkındalık eğitimleri ve politika çapaları düzenli olarak yapılır.

2.1.4. Kişisel Verilerin Korunmasının Önemi

Kişisel verilerin korunmasının önemi pek çok açıdan belirginleşir ve hem bireyler hem de kurumlar için kritik avantajlar sağlar:

- **Bireylerin Mahremiyetini ve Temel Haklarını Korur:** Kişisel veriler kişisel hayatın mahremiyetini doğrudan etkiler; korunması, kimlik hırsızlığı, kötüye kullanım ve kötü niyetli gözetim gibi riskleri azaltır, bireylerin özgürce hareket edebilmesini ve kendini güvende hissetmesini sağlar (Yüksel, 2009).
- **Güven ve İtibarı Güçlendirir:** Veri güvenliğine yatırım yapan kurumlar, müşteriler, çalışanlar ve ortaklar nezdinde güven kazanır; bu da müşteri sadakatini artırır, çalışan bağlılığını güçlendirir ve iş ortaklıklarını kolaylaştırır.
- **Yasal Uyumu Sağlar ve Cezai Riskleri Azaltır:** Birçok ülkede kişisel veri koruma mevzuatları vardır ve ihlaller ciddi para cezalarına, operasyonel kesintilere ve yasal süreçlere yol açabilir (Olca ve Can, 2014). Uyum, yasal gereklilikleri yerine getirmenin ötesinde, operasyonel güvenliği de artırır.
- **Rekabet Avantajı ve İnovasyonu Destekler:** Verinin Güvenli ve etik kullanımı, yeni hizmetler ve iş modellerinin geliştirilmesini kolaylaştırır (Işık ve Keskin, 2013). Veriye güvenli ve sorumlu erişim, veri temelli inovasyon için güvenli bir temel oluşturur.
- **İyileştirilmiş Karar Alma ve Risk Yönetimi Sağlar:** Veri koruma süreçleri, risklerin daha iyi görünür hale gelmesini sağlar. Veri envanteri, sınıflandırma ve denetimler, güvenlik açıklarını erken tespit etme ve giderme imkânı sunar (Karakuş, 2009).
- **Sivil Toplum ve Demokratik Süreçlere Destek Verir:** Şeffaflık, hesap verebilirlik ve kullanıcı taleplerine hızlı yanıt verme mekanizmaları, vatandaşların haklarını korur ve kamu güvenini güçlendirir.

- **Tedarik Zinciri Güvenliğini Artırır:** Üçüncü taraflarla veri paylaşımında güvenlik ve uyum şartlarının netleşmesi, tedarik zinciri boyunca verilerin korunmasını sağlar ve operasyonel sürekliliği destekler.

Kişisel verilerin korunması yalnızca bir yükümlülük değil, güvenli, sürdürülebilir ve müşteri odaklı bir dijital ekonomi için temel bir yapı taşıdır. İstersen bu konuyu belirli bir bağlama (ör. kurum politikası özeti, risk değerlendirme taslağı veya farkındalık eğitimi içeriği) göre daha özelleştirebiliriz.

2.1.5. Kişisel Veri İhlali ve Sonuçları

Kişisel veri ihlali, bir şirketin, kurumun veya üçüncü bir tarafın, bireylerin kimlik bilgileri, iletişim adresleri, finansal verileri, sağlık kayıtları veya çevrimiçi davranışlarına ilişkin hassas bilgileri yetkisiz erişim, ifşa, değiştirme veya yok etme gibi güvenlik açıkları sonucunda korumasız bir şekilde ortaya çıkmasıdır. Bu tür ihlaller sadece teknik güvenlik eksikliklerinden kaynaklanabileceği gibi, çalışan hataları, altyapı zafiyetleri, tedarik zinciri güvenliği, yetersiz farkındalık ve eğitimsizlik, yanlış yapılandırmalar, zayıf parola politikaları veya güvenlik güncellemelerinin gecikmesi gibi çeşitli faktörlerin birleşiminden de ortaya çıkabilir (Atasoy, 2016).

İhlal gerçekleştiğinde, bireyler için doğrudan ve dolaylı zararlar söz konusu olabilir: kimlik hırsızlığına karşı savunmasızlık artar, mali kayıplar ortaya çıkabilir, güvenilirlik ve güvenilirlik zarar görebilir, kişisel hayatın mahremiyeti ihlal edilerek sosyal ve profesyonel itibar zayıflayabilir. Bazı durumlarda psikolojik stres, kaygı ve güvensizlik duyguları tetiklenir. Kurumlar için ise ihlaller düzenleyici yaptırımlar, cezai süreçler, yüksek net zararlar ve yüzleşmek zorunda kalınan itibar kaybı anlamına gelir. Müşteri güveninin azalması, müşteri kaybı, piyasa değeri üzerinde olumsuz etkiler ve işlem maliyetlerinde artış gibi sonuçlar doğurabilir (Eşitli, 2012). Yasal gereklilikler kapsamında ihlal haber verilmeli, uygun bildirim süreçleri işletilmeli ve etkilenen bireylere destek sağlanmalıdır (Kılınç, 2012).

2.2. Kişisel Verilerin Korunmasına İlişkin Hukuki Düzenlemeler

Kişisel verilerin korunması; bireylerin temel hak ve özgürlüklerini güvence altına almak amacıyla, hukuka uygunluk, dürüstlük ve şeffaflık ilkeleri çerçevesinde yürütülen bir süreçtir. Bu kapsamda, kimlik bilgileri, sağlık verileri, mali durum, iletişim bilgileri ve davranış verileri gibi her türlü kişisel verinin işlenmesi, saklanması, paylaşılması ve aktarılması; başta 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) olmak üzere Anayasa, ilgili Türk mevzuatı ve gerektiğinde GDPR gibi uluslararası düzenlemelere uygun olarak gerçekleştirilir (Kılınç, 2012).

Veri işleme faaliyetleri, veri sahibinin açık rızası, sözleşmesel gereklilik, yasal yükümlülük, hayati çıkarlar, kamu yararı ve meşru menfaat gibi hukuki sebeplerden birine dayanır (Gürsel, 2016). Bu süreçte, veri sahibinin erişim, düzeltme, silme, işleme kısıtlaması, verinin taşınabilirliği ve itiraz hakları güvence altına alınır. Ayrıca, veri güvenliğini sağlamak için teknik ve idari tedbirlerin alınması zorunludur.

Verilerin hangi amaçla ve ne kadar süreyle işleneceği açıkça belirlenir; veri sorumluları VERBİS gibi kayıt sistemlerine bildirim yapar (Eşitli, 2012). Özel nitelikli kişisel veriler ve çocuklara ait veriler için daha sıkı güvenlik önlemleri uygulanır. Uluslararası veri aktarımlarında yeterli koruma sağlanması için uygun transfer mekanizmaları ve ek tedbirler devreye alınır.

KVKK, ikincil mevzuat ve yönetmelikler ile desteklenir; Kişisel Verileri Koruma Kurumu, denetim ve yaptırım yetkileriyle düzenlemelerin uygulanmasını sağlar. Bu çerçevede, veri sorumlularının veri envanteri oluşturmasını, rıza yönetimini netleştirmesini, güvenli veri işleme ve imha süreçlerini kurmasını, hak taleplerine hızlı ve etkin yanıt verebilmesini ve kurum içinde sürdürülebilir bir uyum kültürü geliştirmesini hedefler. Temel ilkeler; adil, amaçla sınırlı, veri minimizasyonuna dayalı, aydınlatma yükümlülüğü ve denetime açık bir veri işleme yaklaşımıdır (Gürsel ve Dügmeçi, 2018).

2.2.1. Türkiye’de Kişisel Verilerin Korunması Kanunu (KVKK)

Türkiye’de Kişisel Verilerin Korunması Kanunu (6698 sayılı KVKK), gerçek kişilerin kişisel verilerinin işlenmesini kapsayan ve verinin elde edilmesinden silinmesine kadar tüm

aşamaları düzenleyen temel bir mevzuattır (Oğuz, 2018). Kanun, hukuka uygunluk, dürüstlük, amaçla sınırlılık, veri minimizasyonu, doğru ve güncel tutma, saklama süresinin sınırlılığı, güvenliğin sağlanması ve verilerin aktarımına ilişkin prensipleri esas alır.

KVKK; veri sahibinin açık rızası, sözleşmesel gereklilik, hukuki yükümlülük, hayati çıkarlar, kamu yararı veya meşru menfaat gibi hukuki sebeplerle veri işlenmesine izin verir (Braun, 2017). Özel nitelikli kişisel veriler ve çocuklara ait veriler için daha sıkı güvenlik önlemleri ve sınırlamalar öngörür.

Kanun, kamu otoritelerine veri koruma alanında denetim ve yaptırım yetkisi tanır; veri sorumlularının VERBİS'e kaydolmasını, ihlal durumlarında bildirim ve raporlama yükümlülüklerini yerine getirmesini zorunlu kılar. Veri sahiplerinin erişim, düzeltme, silme, işleme kısıtlaması, veri taşınabilirliği ve itiraz gibi hakları güvence altına alınır.

Ulusal ve uluslararası veri transferlerinde yeterli koruma sağlanması zorunludur. KVKK, idari para cezaları ve diğer yaptırımlar ile desteklenir ve kamu-özel sektör ayrımı yapmaksızın kişisel veri işleyen tüm gerçek ve tüzel kişilere uygulanır (Kartal, 2018). Teknik ve idari tedbirlerin alınması, Kurum'un denetim, bildirim ve uyum görevleri ile desteklenir.

KVKK; hukuki güvenlik, adil işlem, gereklilik ve orantılılık gibi kavramları temel alır, çağdaş veri koruma standartlarıyla uyumlu bir çerçeve sunar. Uluslararası veri aktarımı, veri taşınabilirliği, ihlallerin bildirilmesi ve veri güvenliği konularında ayrıntılı hükümler içerir. Türkiye'nin veri koruma alanındaki kurumsal ve yasal altyapısını oluşturan KVKK, bireylerin temel hak ve özgürlüklerini güvence altına almak amacıyla sürekli güncellenen ve pratik uyumluluğu hedefleyen kapsamlı bir mevzuat bütünlüğünü temsil eder (Akıncı ve Raporu, 2017).

2.2.2. Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), AB vatandaşlarının kişisel verilerinin korunması ile bu verilerin serbestçe dolaşımı arasındaki dengeyi kurmayı amaçlayan, veri işleme süreçlerinde hesap verebilirlik ilkesini merkezine alan kapsamlı bir düzenlemedir (Akıncı ve Raporu, 2017). Hukuka uygunluk, dürüstlük, şeffaflık, veri

minimizasyonu, amaçla sınırlı işleme, doğru ve güncel tutma, saklama süresinin sınırlılığı, bütünlük ve güvenlik gibi temel ilkeleri benimser. Kişisel verilerin işlenmesini, veri sahibinin açık rızası, sözleşmesel gereklilik, yasal yükümlülük, hayati çıkarlar, kamu yararı veya meşru menfaat gibi hukuki sebeplere dayandırır. Özel nitelikli kişisel veriler için daha sıkı güvenlik önlemleri öngörür ve bazı durumlarda açık rızayı zorunlu kılar. Veri sahiplerine; erişim, düzeltme, silme (unutulma hakkı), işleme kısıtlaması, veri taşınabilirliği, itiraz ve otomatik karar vermeye karşı çıkma gibi kapsamlı haklar tanır.

Veri güvenliği için teknik ve organizasyonel tedbirlerin alınmasını zorunlu kılar; yeterli koruma bulunmayan veri aktarımlarında uygun güvenlik tedbirleri veya yeterlilik kararları aranır. Denetim ve yaptırımlar konusunda Avrupa Veri Koruma Kurulu ile ulusal veri koruma otoritelerine (DPA) geniş yetkiler verir (Başalp, 2015). Uyum sürecinde Veri Koruma Etki Değerlendirmesi (DPIA) gibi risk analizi araçlarını ve yüksek güvenlik standartlarını teşvik eder. İhlallerin bildirilmesini zorunlu kılar ve şeffaflığı artırır. Modern dijital ekonominin veri odaklı ihtiyaçlarını karşılamaya yönelik geniş kapsamlı hükümler içerir; işletmelere hem yükümlülükler hem de esneklik sağlar. GDPR, bireylerin haklarını güçlendiren, küresel veri akışlarını düzenleyen ve günlük işlemlerde sürdürülebilir bir uyum kültürü oluşturmayı hedefleyen, Türkiye’de KVKK ile uyum hedeflerinin önemli bir parçası olan, sürekli gelişen bir veri koruma vizyonunu yansıtır.

2.2.3. Kişisel Verilerin Korunmasında Kurumların Yükümlülükleri ve Çalışanların Sorumlulukları

Kurumlar, kişisel verilerin korunmasıyla ilgili mevzuata uyumu sağlamak için bir veri koruma politikası oluşturmalı, bu politika kapsamında veri sorumlusu olarak sorumlulukları belirlemeli ve çalışanlarının bu politikalara uygun hareket etmesini temin etmek üzere gerekli idari ve teknik tedbirleri almalı; verilerin işlenmesi amacıyla uygulanacak hukuki sebepleri ve işleme süreçlerini açıkça tanımlamalı, veri envanteri ve kayıt tutma süreçlerini kurmalı, risk bazlı veri güvenliği önlemlerini (erişim kontrolleri, yetkilerin rol bazlı atanması, şifreleme gibi) uygulamalı ve güvenlik ihlallerine karşı bildirim yükümlülüklerini netleştirmelidirler (Manav, 2015).

Çalışanların kişisel veriye erişim talep ve hallerinde yetkilendirme süreçlerini sürdürmeli, farkındalık eğitimleriyle çalışanları bilinçlendirmeli, olay yönetimi ve ihlal

bildirim mekanizmalarını işler halde tutmalı, bu ihlallerin doğurabileceği hukuki ve idari yaptırımlara karşı proaktif bir yaklaşım benimsemeli ve gerektiğinde veri sahiplerine hızlı ve şeffaf bilgilendirme yapmalıdırlar. Çalışanlar ise kendilerine verilen görevler kapsamında sadece yetkili oldukları verileri işleyecek şekilde hareket etmeli, veri minimizasyonu ilkesine uygun davranmalı, kişisel verileri korumak için gerekli güvenlik önlemlerini uygulamalı, güvenlik politikalarına riayet etmeli, güvenlik açıklarını bildirme sorumluluğunu üstlenmeli ve verilerin yanlış kullanımını veya yetkisiz erişimini önlemek için gerekli tedbirleri almakla yükümlüdürler (Karataş Durmuş, 2017).

Veri sahiplerinin haklarını kullanma süreçlerinde doğru, zamanında ve eksiksiz bilgi sağlama konusunda titiz davranmalı, rıza süreçlerini ve veri işleme amaçlarını açıkça iletmelidirler. Bu kapsamda kurumlar, denetimlere açık bir uyum kültürü oluşturarak, çalışanların iş akışlarına entegre edilmiş güvenli veri işleme pratiklerini sürdürmeli ve gerektiğinde üçüncü taraflarla yapılan sözleşmelerde uygun veri koruma şartlarını ve yükümlülükleri netleştirmelidirler (Dülger, 2018).

2.3. Kurumsal Farkındalık

Kurumsal farkındalık, bir organizasyonun misyonu, vizyonu, değerleri ve stratejik hedefleri konusunda çalışanlarının, müşterilerin ve paydaşların ortak bir anlayışa sahip olması durumudur (Karatay, 2017). Bu farkındalık, iletişimin açık ve tutarlı olmasını, karar süreçlerinde etik ilkelere sadık kalınmasını ve tüm seviyelerde hesap verebilirliğin güçlendirilmesini sağlar. Kurumsal farkındalık, çalışanların günlük iş akışlarında şirketin amaçlarına odaklanmalarını kolaylaştırır, kurumsal kültürü güçlendirir ve değişim yönetimini kolaylaştırır. Güçlü kurumsal farkındalık, güven, bağlılık ve sürdürülebilir başarı için temel bir zemin oluşturur (Kavut, 2010).

2.3.1. Kurumsal Farkındalık Kavramı

Kurumsal farkındalık, bir organizasyonun misyonu, vizyonu, değerleri, stratejik hedefleri ve kültürü hakkında çalışanların, müşterilerin ve paydaşların ortak ve net bir anlayışa sahip olması durumudur (Deneçli, 2015). Bununla birlikte, bu farkındalık organizasyonun tüm düzeylerinde tutarlı davranış ve kararlar üretilmesini sağlar.

Bileşenler:

- **Misyon ve Vizyon Farkındalığı:** Şirketin varoluş amacı ve gelecekte ulaşmak istediği hedefler konusunda ortak anlayış (Sarıtış ve Kaya, 2017).
- **Değerler ve Kültür Farkındalığı:** Hangi etik ilkelerin ve davranış normlarının benimsendiği konusunda farkındalık.
- **Stratejik Hedefler Farkındalığı:** Kısa ve uzun vadeli hedeflerin ne olduğunun bilinmesi ve bunlara yönelik yönlendirme (Turhan, Özen ve Albayrak, 2018).
- **İletişim Farkındalığı:** Açık, tutarlı ve iki yönlü iletişim kanallarının etkin kullanımı.
- **Hesap Verebilirlik Farkındalığı:** Roller, sorumluluklar ve hesap sorulabilirlik zincirinin net olması.
- **Değişim ve Adaptasyon Farkındalığı:** Değişim süreçlerinin farkında olmak ve bu süreçlere uyum sağlamak.

Amaç ve faydalar:

- Karar alma süreçlerinde tutarlılık ve etiklik artışı.
- Çalışanlar arasında güven ve bağlılığın güçlenmesi.
- Çalışanların günlük işlerinde şirkete odaklanmaları ve performansın artması.
- Değişim yönetiminin kolaylaşması ve organizasyonel uyumun sağlanması.
- Marka güveni ve paydaş güveninin güçlenmesi.

Uygulama yolları:

- Net vizyon, misyon ve değerlerin yazılı ve kolay erişilebilir olması.
- Yöneticiler ve liderler tarafından örnek davranış göstermek.
- Şeffaf iletişim kanalları ve açık geri bildirim mekanizmaları.
- Entegrasyonun sağlandığı eğitimler ve oryantasyon programları.
- Performans değerlendirme sistemlerinde kurumsal farkındalık hedeflerinin yer alması.
- Değişim yönetimi süreçlerinde paydaş katılımı ve iletişimi.

Kurumsal farkındalık, organizasyonun tüm üyelerinin ortak bir dil ve amaç etrafında buluşmasını sağlayan, güvene dayalı bir çalışma ortamı ve sürdürülebilir başarı için temel bir yapı oluşturur (Onbulak, 2017).

2.3.2. Kişisel Verilerin Korunmasında Kurumsal Farkındalığın Rolü

Kişisel verilerin korunmasında kurumsal farkındalık, sadece teknik çözümlerle sınırlı kalmayan, tüm çalışanların veriye ilişkin riskleri anlaması ve uygun davranışları günlük iş akışlarına entegre etmesiyle mümkün olan proaktif bir kültürü teşvik eder. Bu farkındalık, veri sahipliği ve erişim yetkileri gibi sorumlulukların netleşmesini, veri envanteri ve sınıflandırma süreçlerinin uygulanabilirliğini artırır. Politika ve prosedürlerin basitleştirilmiş, anlaşılır bir dille paylaşılmasını sağlar. Düzenli farkındalık eğitimleri, simülasyonlar ve hızlı düzeltim mekanizmaları ile hatalar azaltılır, uyum maliyetleri düşer ve güven ile itibar güçlenir (Ağıralan ve Yiğit, 2015).

2.3.3. Farkındalık Oluşturmaya Yönelik Kurumsal Uygulamalar

Kurumsal farkındalık, bir organizasyonun en üst düzeyinden en alt düzeyine kadar yayılmasını gerektiren bütüncül bir süreçtir (Deneçli, 2015). Üst yönetimin kararlı destek ve örnek davranışları, farkındalık programlarının güvenilirliğini artırır. Stratejik hedefler, çalışanların günlük işlerine nasıl yansımaları gerektiğini açıkça belirler; vizyon ve değerler, iletişim planlarına ve performans ölçütlerine entegre edilir. Böylece farkındalık, sadece eğitimlerle sınırlı kalmaz, her karar ve davranışta hissedilir hale gelir.

Şeffaf, iki yönlü iletişim, farkındalık oluşturma'nın temel taşlarından biridir. Basit, erişilebilir ve sürekli güncellenen bilgilendirme materyalleri (kılavuzlar, kısa videolar, dijital posterler) kullanılır (Boztepe, 2013). Yönlü geri bildirim mekanizmaları (anketler, kısa anketler, sohbet botları) çalışanların sorularını ve endişelerini hızlı biçimde iletmelerini sağlar. İletişimde başarı, anlaşılır dil kullanımı ve paydaş katılımını teşvik eden çoklu kanalların (e-posta, intranet, toplantılar, iş süreçleri içi bildirimler) uyumlu birleşiminde yatar. Düzenli, hedef odaklı eğitim programları tasarlanır. Yeni çalışanlar için oryantasyonun bir parçası olarak kurulur ve mevcut çalışanlar için periyodik güncellemelerle sürdürülür. Eğitimler, gerçek senaryolar ve kısa simülasyonlar içerir; öğrenilenler pratikte nasıl uygulanacağına dönüştürülür. Mikro-öğrenme modülleri ve kolay ulaşılabilir kaynaklar, yoğun iş temposunda bile sürekli farkındalık sağlar. Öğrenmenin ölçülebilir olması için kısa pekiştirme testleri ve sertifikasyonlar kullanılabilir (Cihangir, 2016).

2.3.4. Bilgilendirme, Eğitim ve İç Denetim

Kurumsal farkındalığı güçlendirmek için etkili bilgilendirme, hedefe odaklı eğitim ve zayıf noktaları tespit eden iç denetim üçgeni kritik bir rol oynar (Sarı, 2013). Net ve erişilebilir bilgilendirme materyalleriyle çalışanlar güncel politikalar, prosedürler ve güvenlik gereklilikleri hakkında sürekli bilgilendirilir. Ardından, pratiğe dönüştürülebilir eğitimler (örnek olaylar, simülasyonlar, mikro-öğrenme modülleri) ile öğrenme kalıcı hale getirilir ve beceriler doğrulanır. İç denetim ise bu süreçlerin etkililiğini bağımsız olarak değerlendirir. Uyum seviyeleri, kontrol kuvvetleri, hatalı davranışların kök nedenleri ve iyileştirme önerileri belirlenir. Böyle bir enstitüde bilgilendirme ve eğitim, iç denetim bulguları ile sürekli iyileştirme için girdi sağlar; bir arada çalıştıklarında güven, güvenlik kültürü ve sürdürülebilir uyum güçlenir (Ergin, Selimoğlu ve Tolkun, 2016).

BÖLÜM 2: GÜVEN KAVRAMI VE KİŞİSEL VERİLER BAĞLAMINDA LİTERATÜR İNCELEMESİ

Güven kavramı, kişisel veriler bağlamında yalnızca bireylerin mahremiyetine saygı göstermekle sınırlı olmayan; organizasyonel güven, tüketici güveni ve veriye dayalı örgütsel karar alma süreçlerinin etkileşimini kapsayan çok disiplinli bir araştırma alanı olarak öne çıkar (Aksoy ve Sever, 2012). Araştırmalar, güvenin farklı boyutlarını bireysel güven, kurumsal güven, güvenilirlik algısı ve güvenlik algısı birbirinden ayırarak incelemekte; sosyal sermaye perspektifinden güvenin ticari performans, müşteri sadakatine ve kurumsal itibara etkilerini ele almaktadır. Veri ihlallerinin maliyetleri ile güven kaybının uzun vadeli finansal sonuçları arasındaki karmaşık ilişkiler de literatürde önemli bir yer tutar (Afşar, 2013).

Güven ile Kişisel Verilerin Korunması (KVK) uyumu arasında karşılıklı ve güçlendirici bir ilişki bulunduğu, rıza yönetimi, kullanıcı deneyimi ve güvenli tasarım ilkelerinin (privacy-by-design ve security-by-design) entegrasyonu yoluyla güvenin artırılacağı konusunda geniş bir görüş birliği mevcuttur (Ağıralan ve Yiğit, 2015). Bununla birlikte, güvenin kültürel ve bölgesel farklılıklardan etkilendiği, teknolojik gelişmelere paralel olarak sürekli değiştiği; ancak şeffaflık, hesap verebilirlik, adil davranış ve sahici kullanıcı odaklılık ilkelerinin bu değişimin merkezinde yer aldığı literatür tarafından vurgulanmaktadır.

3.1. Güven Kavramı

Güvenlik kavramı, yalnızca fiziksel bir alanın sınırlarını korumakla sınırlı kalmayan, aynı zamanda bireylerin, toplulukların ve kurumların bilgi, değerler ve yaşam biçimlerine yönelik tehditlere karşı direnç geliştirme sürecidir ki bu süreç, teknolojik, sosyal, etik ve ekonomik boyutları birbirine bağımlı biçimde içeren çok katmanlı bir yapıyı ifade eder ve bu çok katmanlı yapı içerisinde güvenliğin sağlanması için risklerin proaktif olarak tespit edilmesi, etkili savunma mekanizmalarının kurulması ve gerektiğinde hızlı adaptasyonla tehditlere yanıt verilmesi gerekliliğini ortaya koyar (Boztepe, 2013). Güvenliğin yalnızca bir olayın ertelenmesi ya da zarar miktarının azaltılması ile sınırlı kalmayıp, aynı zamanda güven unsurlarını güçlendirmek için güvenilirlik, hesap verebilirlik ve şeffaflık gibi temel

değerlerin toplumsal normlar haline gelmesini hedefleyen bir etik çerçeveye bağlı olduğunu da vurgular.

Bir toplumun güvenliğini düşünürken, güvenlik kavramının sadece dış tehditlere karşı korunma olarak anlaşılmaması gerektiğini, iç dinamikler bağlamında da güvenin inşa edilmesi gerektiğini söylemek mümkündür; zira güvenliğin güven kaynağı olan sosyal güvenlik ağlarının, adaletin sağlanmasına yönelik kurumsal mekanizmaların ve güvenlik kültürünün bir arada varlık göstermesiyle güçlenmesi, bireylerin riskleri paylaşma ve toplumsal dayanışmayı güçlendirme kapasitesini artırır. Bu çerçevede risk yönetimi, güvenlik politikalarının belirli hedeflere yönlendirilmesiyle mümkün olurken, bu hedeflerin açık, kapsayıcı ve ortak paydada mutabık kalınabilir olması da karar alım süreçlerinde katılımcı yaklaşımı zorunlu kılar ve böylece güvenlik politikalarının toplumsal meşruiyetinin pekişmesini sağlar (Özler ve Yıldırım, 2015).

Teknolojik güvenlik pratikleri bağlamında ele alındığında, güvenliğin dinamik ve sürekli evrilen bir kavram olduğu görülür; çünkü dijitalleşme, iletişim teknolojilerinin evrimleşmesi ve veri akışının küresel düzeyde artmasıyla tehditler de aynı hızla çeşitlenmiş ve karmaşıklaşmıştır. Bu nedenle güvenliğin tek bir savunma mekanizmasıyla korunamayacağı, çok katmanlı savunma sistemlerinin tasarlanması gerektiği, bunun da öncelikle tehdit modellemelerinin derinlemesine analizini, güvenlik mimarilerinin esnekliğini ve olay müdahale süreçlerinin hızlı, koordineli ve hatasız bir şekilde işlemesini gerektirdiğini belirtmek gerekir. Aynı zamanda kullanıcı davranışlarının güvenlik kültürünün merkezinde yer aldığı ve farkındalık eğitiminin, güvenlik duvarlarının, erişim kontrolünün ve güvenli kodlama uygulamalarının başarılı bir biçimde hayata geçirilmesinde kritik bir rol oynadığını da göz ardı etmemek gerekir (Ezirgan Rar, 2014).

Güvenliğin etik boyutu ise, güç eşitsizliklerinin varlığını ve bu eşitsizliklerin güvenlik kararlarına etki etme potansiyelini hesaba katar; çünkü güvenlik politikalarının uygulanması sırasında kimlerin hangi kaynaklara hangi koşullarda erişebileceğinin belirlenmesi, mahremiyet haklarıyla ilgili kaygılar ve adil muamele ilkesiyle dengelenmelidir. Böylece güvenlik uygulamaları, sadece tehditleri bertaraf etmeyi amaçlayan teknik çözümlerin ötesine geçerek, insan haklarına saygılı, ölçülü ve hesap verebilir bir yaklaşımı benimsemiş olur; bu bağlamda güvenlik mimarileri, şeffaf denetim mekanizmaları, rızaya dayalı veri paylaşımı ve suistimalin önüne geçmeyi hedefleyen kontrollerle desteklenmelidir; bunun

sonucunda güvenlik, baskı ve korkunun değil, güven ve özgürlüklerin güçlendirilmesiyle kurumsal ve toplumsal güvenliğin sürdürülebilir bir temele oturmasını sağlar (Okmeydan, 2017).

Güvenlik kavramı, riskleri proaktif bir şekilde analiz eden, çok katmanlı savunma ve uyumlu politika yapısını gerektiren, teknolojik yeniliklere uyum sağlayan, etik ve sosyal sorumluluk çerçevesinde hareket eden ve bireylerin ise güvenli bir çevrede özgürce ve güvenle yaşayabilmesini hedefleyen geniş ve dinamik bir disiplin olarak karşımıza çıkar. Bu nedenle güvenliğin temelinde, güvenin inşa edilmesi, güvenliğin sürekliliğinin sağlanması ve güvenlik kültürünün toplumun her katmanında benimsenmesi gibi eksiksiz bir yaklaşım yatmaktadır (Turgutoğlu, 2017).

3.1.1. Güvenin Tanımı ve Boyutları

Güven, belirsizlik ve risk altında bile bir durumun öngörülebilir, istikrarlı ve destekleyici olduğuna dair inanç ve umut hissidir; bu his, duygusal deneyimler ile bilişsel değerlendirmelerin etkileşimiyle şekillenirken, güvenin kaynağı olan sosyal ilişkilerden kurumsal mekanizmalara kadar geniş bir yelpazede ortaya çıkar ve güvenin oluşumu, güvenilirlik, yetkinlik, iyilik ve şeffaflık gibi temel boyutların zaman içinde etik ve tutarlı bir şekilde ortaya konmasıyla güçlendirilir. Bu bağlamda güven, yalnızca bir tehditle karşı karşıya kalındığında harekete geçilecek bir savunma mekanizması olmayıp, karşılıklı sorumluluk ve hesap verebilirlik temelinde inşa edilen bir güvenlik mirasının taşıyıcısıdır (Kaygın ve Atay, 2014).

Güvenin sürdürülebilirliği, açık iletişim, rızaya dayalı iş birlikleri ve adil muamele ilkelerinin günlük uygulamalarda hayata geçirilmesiyle mümkün olur. Güvenin dinamik doğası gereği, kültürel farklılıklar ve bağlamsal koşullar güvenin ifade biçimini değiştirirken, bireylerin ve kurumların güvenlik politikalarını şeffaflık ve katılımcı süreçlerle tasarlaması, riskleri paylaşma ve yükleri ortaklaştırma kapasitesini artırır; bu da toplumsal dayanışmayı güçlendirir ve güven ortamının kalıcı bir değer olarak toplumun her katmanında benimsenmesini sağlar (Şahin ve Arabacı, 2017).

3.1.2. Örgütsel Güvenin Temelleri

Örgütsel güven, çalışanlar, yöneticiler ve paydaşlar arasında bir kurumu yöneten değerler, süreçler ve davranışlar üzerinden kurulan inanç ve güven ortamını ifade eder. Bu güven, kuruluşun vaatlerini yerine getirme kapasitesine, karar süreçlerinin adilliğine ve iletişimin şeffaflığına olan inançla şekillenirken, güvenin temel taşları olan güvenilirlik, yetkinlik, iyilik/oranlanmış ilgi ve şeffaflık ile hesap verebilirlik gibi boyutların tutarlı ve etik bir şekilde sergilenmesiyle pekiştirilir; bu bağlamda güvenin inşa süreci, açık ve etkili iletişim, öngörülebilirlik, tutarlı uygulama ve yetkin liderlik yoluyla ilerlerken, katılımcı yönetim, geri bildirim mekanizmaları ve çalışana yatırım yapan öğrenme kültürü ile zenginleşir; ayrıca güvenin sürdürülebilirliği, adil karar süreçleri, ayrımcılığın azaltılması ve yetenek gelişimine verilen önemin sürekliliğiyle doğrudan ilişkilidir (Tokgöz ve Seymen, 2013).

İçerideki güven, yalnızca bireylerin performansına değil, potansiyelin ortaya konulmasına da katkıda bulunur ve psikolojik güvenlik alanını güçlendirerek çalışanların risk almasına, yenilikçi çözümler üretmesine ve hatalardan öğrenmesine olanak tanır. Dış etkiler söz konusu olduğunda da örgütsel güven, kriz anlarında hızlı ve koordineli tepkileri mümkün kılan bir dayanıklılık sağlar; bu dayanıklılık, iç ve dış denetimler, hesap verebilir raporlama ve rızaya dayalı veri paylaşımı gibi kontrol mekanizmalarıyla desteklendiğinde, güvenin kurumun kültürü haline gelmesini ve zamanla çalışan bağlılığı, iş memnuniyeti ve organizasyonel performans üzerinde olumlu bir zincirleme etkisi yaratır (Aktuğ, 2016).

3.1.3. Çalışanların Kuruma Olan Güveni

Çalışanların kuruma olan güveni, bir organizasyonun vaatlerini yerine getirme kapasitesine olan inançtan, karar süreçlerinin adilliğine ve iletişimin şeffaflığına kadar uzanan geniş bir güven zemininin bireylerin zihinlerinde ne kadar sağlam ve istikrarlı bir şekilde kurulduğuna bağlı olarak şekillenen, çok katmanlı bir duygusal ve bilişsel algı olarak karşımıza çıkar. Güven, çalışanların sorunları ve belirsizlikleriyle başa çıkarken kuruma olan sadakatlerini, işlerine olan bağlılıklarını ve uzun vadeli katılım niyetlerini güçlendirdiği gibi, aynı zamanda yenilikçilik ve girişimcilik ruhunun sürdürülmesi için gerekli olan psikolojik güvenlik ortamını da destekler ve bu sayede hatalardan öğrenme, risk alma ve yaratıcı çözümler üretme süreçlerini cesaretlendirir; çünkü güvenin temel göstergeleri olan

güvenilirlik (taahhütlerin tutarlılığı ve sözlerin yerine getirilmesi), yetkinlik (gerekli beceri ve kaynaklara erişim ile sorun çözme kapasitesi), iyilik ve karşılıklı ilgi (kurumun çalışanların çıkarlarını gözeterek yaklaşımı ve yardımsever davranışlar sergilemesi), şeffaflık ve adalet (yapılan davranışların ve kararların açık, dürüst ve etik değerlere uygun olması) ile hesap verebilirlik (karar süreçlerinin izlenebilirliği ve hataların sahiplenilmesi), çalışanların güven düzeyini doğrudan etkileyen ve kurum kültürünün zeminini oluşturan yapısal unsurlar olarak öne çıkar (Keçeci, Süer, Atakan, Dural ve Çalışkan, 2017).

Unsurlar bir araya geldiğinde, çalışanlar kendilerini güvenli bir ortamda, fikirlerini çekinmeden ifade edebildikleri, hatalarını saklamadan paylaşabildikleri ve kariyer gelişimlerine dair bilinçli bir yönlendirme aldıkları bir çalışma yaşamı kabulleriyle özdeşleşir ve böylece kuruma olan güven, sadece mevcut iş tatminini artırmakla kalmaz, aynı zamanda yeteneklerin elde tutulmasını, yetkin liderlik tarafından ilham verici bir hedef olarak gösterilmesini ve örgüt içi dayanışmanın güçlenmesini sağlayarak organizasyonun rekabetçi konumunu da güçlendirir. Çalışanların kuruma olan güveni, bireysel motivasyonlardan organizasyonel performansa uzanan geniş bir etki alanına sahip olup, güvenin sürekliliğini güvenli iletişim kanalları, adil performans değerlendirme süreçleri ve etik uyumun sürekliliği ile pekiştiren bir güven kültürünün kurulması ve korunmasıyla en sağlam temeller üzerinde inşa edilir (Afşar, 2013).

3.1.4. Güvenin Kurum Kültürü Üzerindeki Etkisi

Güven, bir kurumun kültürel dokusunu oluşturan temel dinamiklerden biridir ve çalışanların davranışlarını, iletişim tarzını, karar alma süreçlerini ve yeniliğe olan yaklaşımını köklü biçimde şekillendirir. Özellikle güvenin çeşitli boyutlarının (güvenilirlik, yetkinlik, iyilik/karşılıklı ilgi, şeffaflık ve hesap verebilirlik) kurumsal pratiklere entegre edildiği ortamlarda, kültür daha kapsayıcı, dayanışmacı ve adaptif bir nitelik kazanır (Kahveci ve Demirtaş, 2014).

Güvenin Kültürel Boyutları

Güvenli iletişim kültürü: Açık iletişim kanalları, hatalardan ders çıkarma, geri bildirimde değer verme ve psikolojik güvenliğin tesis edilmesiyle çalışanlar fikirlerini özgürce paylaşır; bu durum inovasyon ve problem çözmede katalizör görevi görür (Dursun, 2013).

Adalet ve eşitlik ilkesi: Karar süreçlerinde adaletli davranış, fırsat eşitliği ve performansa dayalı değerlendirme kültürü, güç ve statü hatlarının aşılmasına yardımcı olur; bu da güvene dayalı bir işyeri atmosferi yaratır.

Şeffaflık ve hesap verebilirlik: Yöneticiler ve çalışanlar arasında hesap verebilirlik mekanizmalarının görünür olması, kararların neden ve nasıl alındığının açıkça paylaşılması, güven ortamını pekiştirir ve politikaların meşruiyetini artırır (Boztepe, 2013).

İnsan odaklı yaklaşım: Çalışanların ihtiyaçları, gelişimi ve refahı önceliklendiğinde, çalışanlar kendilerini değerli ve güvenli hisseder; bu da örgütsel bağlılığı ve dayanışmayı güçlendirir.

Kültürel uyum ve çeşitlilik: Farklı geçmişlerden gelen bireylerin güvenli ve kapsayıcı bir ortamda kendilerini ifade edebilmesi, kurum kültürünün esnekliğini ve yeniliğe açıklığını artırır (Amaç, Burak ve Duran, 2017).

Güvenin Kültürel Sonuçları

Özyönetim ve özerklik: Güvenin güçlü olduğu kültürlerde çalışanlar kendi alanlarında karar alma gücüne sahip olur, bu da hızlı tepki verebilme ve yaratıcı çözümler üretme kapasitesini yükseltir.

Bilgi paylaşımı ve öğrenme kültürü: Bilginin saklanmaması ve paylaşılması, kurum içi öğrenmeyi hızlandırır; hatalardan ders çıkarma pratiği norm haline gelir.

Liderlik davranışlarının rolü: Güven odaklı kültürlerde liderlik, örnek teşkil eden davranışlar, sözünde durma ve hesap verebilirlik üzerinden şekillenir; bu da güvenin kurumsal hafızaya ve normlara dönüştürülmesini sağlar.

Psikolojik güvenlik ve risk alma: Çalışanlar, hatalardan korkmadan risk alabilir; bu durum inovasyon ve süreç iyileştirmelerini destekler.

Kriz dayanıklılığı: Güven temelli kültürler, kriz anlarında koordineli iletişim ve hızlı karar alma kapasitesini artırır; güvenin kurumsal hafızası kriz sonrası toparlanmayı hızlandırır (Ağırkan ve Kağan, 2017).

Ölçüm ve Geliştirme Yaklaşımları

Güven haritası ve iklim anketleri: Çalışanların güven düzeylerini, hangi alanlarda güvenin zayıf olduğunu ve hangi davranışların güveni güçlendirdiğini belirlemek için düzenli ölçümler.

Geri bildirim döngüleri: Anket sonuçlarına dayalı aksiyon planlarının geliştirilmesi ve ilerlemenin geri bildirimlerle izlenmesi.

Şeffaf iletişim uygulamaları: Karar süreçlerini ve performans göstergelerini paylaşmak için düzenli bilgilendirme toplantıları, açıklayıcı raporlar ve açık kapı politikaları (Yaşar, 2016).

Liderlik geliştirme: Liderlerin güven odaklı davranışları benimsemesi için eğitimler, mentorluk ve örnek gösterim programları.

Çeşitlilik ve kapsayıcılık girişimleri: Farklılıkların güven inşasında yapıcı bir güç olduğunun farkındalığını artıran programlar ve politikalar (Yavuzaslan, 2017).

Güven, kurum kültürünün omurgasını oluşturan vazgeçilmez bir değerdir. Güvenli ve kapsayıcı bir kültür, çalışanların kendilerini güvenli, değerli ve katkıda bulunan bireyler olarak görmelerini sağlar; bu da bağlılık, performans ve yeniliğin sürdürülebilir bir şekilde artmasına yol açar. Böyle bir kültürde liderlik davranışları, karar süreçleri ve iletişim pratikleri tutarlı ve etik ilkelere dayalı olduğunda, güven uzun vadeli rekabet avantajı ve kurumsal dayanıklılığın temelini oluşturur (Çamdereli ve Şener, 2016).

3.2. Kişisel Veri Güvenliği ile Çalışan Güveni Arasındaki İlişki

Çalışan güveni ile kişisel veri güvenliği arasındaki ilişki, organizasyonun veriyi nasıl topladığı, sakladığı, işlediği ve paylaşmaya karar verdiği konusundaki tutumların çalışanların zihinlerinde yarattığı inançlar üzerinden şekillenen, çok katmanlı ve dinamik bir bağlıdır; bu bağda güven, yalnızca teknik güvenlik önlemlerinin yeterliliğiyle değil, aynı zamanda etik ilkelere bağlılık, şeffaf iletişim ve adil uygulamaların günlük iş akışlarına entegrasyonu ile beslenir. Başlangıçta, çalışanlar hangi verilerin toplandığı, bu verilerin hangi amaçlarla kullanıldığı, ne kadar süre saklandığı ve üçüncü taraflarla nasıl paylaşıldığı konusunda netlik gördüklerinde, veriyle ilgili süreçlere güven duyarlar ve bu güven, genel olarak kuruma olan güveni güçlendirir (Manav, 2015).

Organizasyonun kültürüne yansyarak, çalışanların kendilerini değerli hissedip katkıda bulunmaya gönüllü olmalarını sağlar. Veri güvenliği ihlallerinin veya şeffaf olmayan uygulamaların varlığı, çalışanlarda büyük ölçüde güven kaybına yol açabilir; bu tür olaylar, yalnızca bireysel gizlilik kaygılarını artırmakla kalmaz, aynı zamanda yönetim mekanizmalarının ve risk iletişiminin zayıf olduğuna dair inancı pekiştirir ve bu da çalışanların kuruma olan bağlılığını zayıflatır (Henkoğlu ve Uçak, 2015). Böyle bir bağlamda, güvenin temel taşları olan güvenilirlik, yetkinlik, iyilik/karşılıklı ilgi, şeffaflık ve

hesap verebilirlik hem teknik olarak uygulanabilir politikalarla hem de organizasyonel kültürün günlük pratikleriyle bir araya gelerek güvenin karşılıklı olarak güçlenmesini sağlar. Özellikle şeffaflık ve rıza, çalışanların kendi verilerinin nasıl işlendiğini anlamalarını ve bu işlemler üzerinde söz sahibi olmalarını mümkün kılar; bu durum, psikolojik güvenliği artırır ve çalışanların hatalarını saklamadan paylaşması, riskleri üstlenmesi ve yenilikçi çözümler geliştirme konusunda daha istekli olmaları için zemin hazırlar. Bununla birlikte, veri minimizasyonu ilkesi, en az ayrıcalık yaklaşımı ve net amaç belirleme gibi uygulamalar, güveni korurken aynı zamanda verimliliği ve operasyonel esnekliği de destekler; çalışanlar, yalnızca gerek duydukları verilerin işlendiğini ve bunun hangi bağlamlarda kullanıldığını gördükleri sürece kendilerini güvende hissederler (Akıncı ve Raporu, 2017).

Veri koruma görevlileri veya benzeri hesap verebilirlik mekanizmalarının varlığı, sorumlulukların netleşmesini ve olay anında hızlı ve tutarlı iletişimin kurulmasını sağlar; kriz anlarında güvenin yeniden tesis edilmesi için iletişimin açık ve tutarlı olması hayati önem taşır (Dülger, 2015). Bu bağlamda ölçüm ve geribildirim mekanizmaları, güvenin sürekliliğini sağlamak için kritik araçlardır: düzenli olarak yürütülen güvenlik farkındalık eğitimleri, gizlilik memnuniyeti anketleri, güvenlik ihlallerinin şeffaf bir şekilde raporlanması ve bu raporlar üzerine somut iyileştirme adımlarının atılması, çalışanların güven duygusunu pekiştirir ve güvenin kurumsal hafızaya dönüştürülmesini kolaylaştırır. Teknolojik çözümler ile etik ve yasal uyum arasındaki dengeyi sağlamak da büyük önem taşır; uçtan uca şifreleme, güvenli iletişim kanalları, erişim kontrollerinin sıkılaştırılması ve veriye dayalı karar süreçlerinde açık bilgilendirme mekanizmalarının bulunması, yalnızca güvenliği artırmakla kalmaz aynı zamanda çalışanların kendilerini değerli hissedip güvenli bir çalışma ortamında üretkenliklerini korumalarını sağlar.

3.2.1. Gizlilik Algısının Güvene Etkisi

Gizlilik algısının güvene etkisi, çalışanların kendilerine ait verilerin nasıl toplandığı, işlendiği ve korunduğu konusundaki hissiyatına bağlı olarak şekillenen bir dizi duygusal ve bilişsel tepkiyi içerir; yüksek gizlilik algısı, veri minimizasyonu, amaçla sınırlama ve açık bilgilendirme gibi ilkelerin uygulanmasıyla çalışanlarda kuruma güveni güçlendirir, psikolojik güvenliği destekler ve örgütsel bağlılığı artırır. Bu algı, gizlilik konusunda net ve anlaşılır iletişim, kullanıcı dostu gizlilik arayüzleri ve şeffaf denetimler ile pekiştirilir; çalışanlar kendi verileri üzerinde kontrole sahip olduklarını gördüklerinde endişelerini

azaltır, riskleri daha rahat paylaşır ve hatalardan öğrenmeye açık olur (Malakmadze, Ünver ve Arıkan, 2017).

Veri ihlalleri, belirsiz amaçlar veya saklama süreleri konusunda yetersiz bilgi, güven kaybına yol açar ve motivasyon, iş tatmini ile performans üzerinde olumsuz etkiler doğurabilir. Bu nedenle, gizlilik algısını olumlu yönde etkileyen uygulamalar arasında veri minimizasyonu, açık amaç belirleme, erişim kontrollerinin netliği, güvenli veri işleme yöntemleri ve düzenli, anlaşılır iletişim ile denetim süreçlerinin çalışması yer alır; böyle bir ortamda çalışanlar hem kendilerini değerli hem de güvenli hissederler, bu da kuruma olan bağlılığı ve örgütsel performansı olumlu yönde etkiler (Ağıralan ve Yiğit, 2015).

3.2.2. Şeffaflık, Denetim ve Güven

Şeffaflık, denetim ve güven üçgeni, kurumsal yönetim ve veri güvenliği bağlamında birbirini güçlendiren temel öğeler olarak öne çıkar. Şeffaflık, karar süreçlerinin, politikaların ve verinin nasıl kullanıldığına dair açık iletişimi ifade ederken; denetim ise bu süreçlerin bağımsız veya iç denetim mekanizmalarıyla uyumlu ve etkili bir şekilde işletildiğini doğrular. Bu iki unsur bir araya geldiğinde çalışanlar, paydaşlar ve müşteriler nezdinde güvenin inşa edilmesini ve sürdürülmesini sağlar; aynı zamanda risklerin belirsizlikler halinde kalmasını engeller ve hesap verebilirlik kültürünü güçlendirir.

Şeffaflık, kararların nasıl alındığını, hangi verilerin toplandığını ve bu verilerin hangi amaçlarla kullanıldığını çalışanlara ve paydaşlara net biçimde iletmeyi gerektirir; bu bağlamda açık iletişim kanalları, anlaşılır politikalar ve kolay erişilebilir raporlama araçları hayati öneme sahiptir. Denetim ise bu politikaların uygulanışını bağımsız veya iç denetim süreçleriyle teyit eder, kontrollerin etkinliğini ve mevzuata uyumu ölçer, zayıf noktaları ortaya koyar ve iyileştirme için somut öneriler sunar. Şeffaflık ile denetim arasındaki sinerji, güvenin temel taşlarını güçlendirir (Gürol ve Tüysüzoğlu, 2017).

Çalışanlar davranışların adalet ve hesap verebilirlik ilkelerine uygun olduğunu görür, paydaşlar süreçlerin güvenilirliğini algılar ve kurum kültürü, hatalardan öğrenme, sürekli iyileştirme ve etik uyum odaklı bir yaklaşımı benimser. Bu etkileşim, yalnızca kriz anlarında güveni korumakla kalmaz, günlük operasyonlarda da risk iletişimini ve karar alma süreçlerini daha öngörülebilir hale getirir. Ancak aşırı açıklık riskleri de beraberinde

getirebilir; bu nedenle şeffaflık ile gizlilik arasındaki dengeyi kurmak, hangi bilgilerin paylaşılacağını, ne zaman paylaşılacağını ve kimin erişebileceğini belirleyen net çerçeveler oluşturmaktır. Böyle bir denge içinde, açık iletişim, uygun güvenlik kontrolleri ve düzenli denetim raporlarının paylaşılması, güveni güçlendirir ve kurumsal güvenilirliği yükseltir (Tore ve Tanyeri, 2016).

3.2.3. Kurumsal Etik ve Güven İlişkisi

Kurumsal etki ve güven arasındaki ilişki, organizasyonun itibarını, çalışan davranışlarını ve dış paydaşlarla olan iletişimini kapsayan geniş bir dinamiği meydana getirir. Güven yüksek olduğunda, çalışanlar karar süreçlerine katkıda bulunmaya, riskleri açıkça paylaşmaya ve hatalardan ders çıkarmaya daha istekli olur; bu da psikolojik güvenliğini güçlendirir ve inovasyonu destekler (Cengiz ve Aksoy, 2017). Aynı zamanda kurumsal etki, güvenli ve etik bir çalışma ortamı inşa ederek yetenek çekmesini, çalışan bağlılığını artırır ve yetenekli adayların kuruma çekilmesini kolaylaştırır. Dış paydaşlar nezdinde güven, tutarlı davranışlar, şeffaf iletişim ve söz verilen taahhütlerin yerine getirilmesiyle oluşur; bu da müşteri sadakatini artırır, iş ortaklıklarını güçlendirir ve uzun vadeli rekabet avantajı sağlar. Güçlü bir güven kültürü kurumsal etkiyi pekiştirir; güven, kurumsal etkiyi sağlamlaştıran sürdürülebilir bir değerdir.

3.2.4. Bilgi Güvenliği İhlalleri ve Psikolojik Etkiler

Bilgi güvenliği ihlalleri, bireylerin kişisel verilerinin yetkisiz erişime açılması veya verilerin yanlış şekilde kullanılması gibi olayları içerir ve bu tür ihlaller çalışanlar üzerinde derin psikolojik etkilere yol açabilir. Hem stoklanan güvenlik duygusunun zedelenmesi hem de iş kaygısı artışı, güven kaybına ve stres düzeyinde belirgin yükselmeye neden olur. İhlal sonrası belirsizlik ve hesap verebilirlik eksikliği hissi, çalışanlarda psikolojik güvende bir zayıflama yaratabilir; bu durum, hataların saklanması, riskli kararların ertelenmesi ve iletişimde çekingenlik gibi davranışları tetikleyebilir. Etkili bir müdahale ve güvenli iletişim süreci bu olumsuz etkileri azaltabilir: şeffaf bildirim, hızlı ve uygun zarar azaltma adımları, adaletli sorumluluk dağılımı ve destekleyici örgüt kültürü, çalışanların güven duygusunu yeniden inşa eder ve psikolojik güvenliğini korur (Avcı ve Karataş, 2017).

İhlal riskine karşı proaktif eğitimler, net olay müdahale planları ve simülasyonlar, çalışanların olaylara karşı dayanıklılığını artırır; bu tür önlemler, ihlallerin telafisi sırasında bile çalışanların kontrol duygusunu güçlendirir ve motivasyon kaybını minimize eder. Bilgi güvenliği ihlallerinin psikolojik etkileri karmaşık bir etkileşimle ortaya çıkar: korku ve güvensizlik duyguları ile bilinçli güven yönetimi stratejileri arasında bir denge kurulduğunda, organizasyonlar hem çalışan refahını korur hem de güvenliğin kurumsal performans üzerindeki olumsuz etkilerini azaltır (Baltacı, 2017).

3.3. Kişisel Verilerin Korunması Kanunu (KVKK) ve Güven

KVKK, Türkiye’de kişisel verilerin işlenmesinde temel hak ve özgürlüklerin korunmasını amaçlayan bir çerçeve yasa olarak, veri sahibinin haklarını güvence altına alır ve veri sorumlularının sorumluluklarını netleştirir. Bu bağlamda güven, hem bireylerin kendilerine ait verilerin nasıl toplandığı, saklandığı ve kullanıldığı konusunda netlik görmesiyle hem de bu süreçlerin mevzuata uygun olarak yürütülmesiyle örülür. KVKK’ya uygunluk, sadece teknik güvenlik önlemlerinin yeterliliğiyle değil, şeffaf iletişim, rıza süreçlerinin doğru yönetimi, veri minimizasyonu ve amaç sınırlamasının uygulanmasıyla da pekiştirilir. Şeffaflık ve hesap verebilirlik, veri sahiplerinin haklarını kullanma ve denetim mekanizmalarına güven duyma ihtiyacını karşılar; bu da organizasyon içindeki güven kültürünü güçlendirir ve çalışanlar ile müşteriler arasında güvene dayalı sürdürülebilir ilişkiler kurulmasına olanak verir (Dülger, 2016).

KVKK uyum süreci kapsamında düzenli risk değerlendirmeleri, veri etkimi değerlendirmesi (DPIA), veri koruma görevlisi (DPO) ataması ve olası ihlal durumlarında hızlı, net ve adil iletişim, güvenin korunmasına ve kriz yönetiminin etkinliğine önemli katkılar sağlar. KVKK ile güven arasındaki ilişki, yasal yükümlülüklerin ötesinde etik davranışlar, kullanıcı haklarının korunması ve kurumsal itibarın güçlendirilmesiyle kurulup sürdürülür; bu da hem bireysel güvenliği hem de kurumsal güvenilirliği artırır (Vuraloğlu, 2017).

3.3.1. KVKK'nın Çalışanlar Açısından Önemi

KVKK'nın çalışanlar açısından önemi, kişisel verilerin korunmasıyla güvenli bir çalışma ortamı ve sağlıklı iş ilişkileri kurmayı amaçlar. Çalışanlar, hangi verilerin toplandığı, kimlerle paylaşıldığı ve hangi amaçlarla kullanıldığı konusunda netlik ister; bu sayede mahremiyetleri korunur ve hakları güvence altına alınır. KVKK'ya uyum, verinin minimuma indirgenmesi, gerektiğinde saklama sürelerinin sınırlı olması ve rıza Temelli işleme gibi ilkelerin uygulanmasıyla güveni pekiştirir. Rol tabanlı erişim kontrolleri ve en az yetki ilkesinin benimsenmesi, hatalı veya yetkisiz erişimleri minimize eder; ihlal durumlarında hızlı bildirim ve şeffaf iletişim, çalışanlarda psikolojik güvenliği korur ve organizasyonun itibarını güçlendirir. Eğitimler ve farkındalık çalışmaları ise çalışanların veri koruma kültürünü benimsemelerini sağlar, olaylara karşı dayanıklılığı artırır ve yasal riskleri azaltır. KVKK, çalışan haklarını korurken, kurumsal güvenlik ve güven ilişkisini güçlendirir; bu da motivasyonu, bağlılığı ve genel performansı olumlu yönde etkiler (Eren, 2017).

3.3.2. Yasal Düzenlemelerin Güven Algısına Katkısı

Yasal düzenlemeler, güven algısını güçlendirmek için temel bir çerçeve sunar. Bu düzenlemeler, kişisel verilerin korunması, güvenlik standartları, hesap verebilirlik ve etik davranışlar gibi alanlarda net kurallar koyar; bu da bireylere ve paydaşlara karşı sorumluluk duygusunu pekiştirir. Yasal yükümlülükler, örgütleri riskleri azaltmaya, süreçleri şeffaf hale getirmeye ve hatalı uygulamaları düzeltmeye teşvik eder. Bu sayede çalışanlar ve müşteriler, olmakta olanı okuyabilir ve güvenin temel taşlarını oluşturan adil ve tutarlı uygulamaları görür. Düzenlemeler ayrıca denetim mekanizmaları ve yaptırım süreçleri aracılığıyla hesap verebilirliği artırır; bu da güveni sadece sözde kalmayan, ölçülebilir ve sürdürülebilir bir değer haline getirir. Sonuç olarak, sağlam ve uygulanabilir yasal çerçeveler, güveniğin inşa edilmesi ve sürdürülmesi için güvenilir bir temel sağlar; bireyler daha bağımsız hareket edebilir, paylaşım ve iş birliği daha güvenli bir zeminde gerçekleşir (Eroğlu, 2014).

3.3.3. KVKK İhlalleri ve Kurumsal Güven Kayıpları

KVKK ihlalleri, bireylerin kişisel verilerinin izinsiz erişime açık hale gelmesi veya yanlış kullanılması sonucunda ortaya çıkar ve hem yasal hem de itibar açısından kurumsal

güveni önemli ölçüde zedeler (Eşitli, 2012). Böyle ihlaller, çalışanlar arasında psikolojik güvensizliği tetikleyerek hataların saklanması, iletişimde çekingenlik ve görevlerden kaçınma gibi davranışları artırabilir; bu da operasyonel verimliliği düşürür ve inovasyonu baskılar. Dış paydaşlar nezdinde güven kaybı, müşteri sadakatini zayıflatır, iş ortaklığı fırsatlarını azaltır ve uzun vadeli rekabet avantajını tehdit eder. Hızlı ve şeffaf ihlal yönetimi, sorumluluk paylaşımı ve etkili zarar azaltma adımları sayesinde güven kırıklarını onarma potansiyeline sahiptir. KVKK ihlallerine karşı proaktif önlemler, veri envanteri ve risk değerlendirmesi ile veri koruma görevlisi ataması gibi uygulamalar, güven kaybını minimize eder ve kriz durumlarında iletişimi düzenli ve güven verici kılar. KVKK ihlallerinin etkileri karmaşık bir güven kaybı döngüsüne yol açabilir; ancak etkili uyum yönetimi, şeffaf iletişim ve hızlı müdahale ile bu kayıplar telafi edilerek kurumsal güven yeniden tesis edilir (Dülger, 2016).

BÖLÜM 3: ARAŞTIRMA METODOLOJİSİ

3.1. Araştırmanın Amacı ve Önemi

Kişisel verilerin korunması, günümüz bilgi toplumunda hem bireyler hem de kurumlar açısından giderek daha kritik bir konu haline gelmiştir. Özellikle dijitalleşmenin hız kazanmasıyla birlikte, kurumların çalışanlarına ve paydaşlarına ait kişisel verileri toplama, işleme ve saklama süreçleri daha karmaşık ve hassas bir hale gelmiştir (Smith, Dinev ve Xu, 2011). Bu süreçte, kişisel verilerin korunmasına yönelik kurumsal farkındalık, sadece yasal bir zorunluluk olmanın ötesinde, kurumların etik sorumluluğu ve sürdürülebilirliği açısından da büyük önem taşımaktadır (Bélanger ve Crossler, 2011).

Araştırmanın temel amacı, kurumlarda kişisel verilerin korunmasına yönelik kurumsal farkındalık düzeyinin çalışanların kuruma duyduğu güven üzerindeki etkisini incelemektir. Kurumsal farkındalık, çalışanların kişisel verilerinin güvenli bir şekilde işlendiğine ve saklandığına dair inançlarını güçlendirmekte, bu da çalışanların kuruma olan güvenini ve bağlılığını artırmaktadır (Dinev ve Hart, 2006). Özellikle Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ve Türkiye’de 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) gibi yasal düzenlemeler, kurumların bu alandaki sorumluluklarını daha da artırmıştır.

Çalışanların güven düzeyi, kurumun şeffaflığı, etik değerleri ve veri koruma uygulamaları ile doğrudan ilişkilidir. Kurumların kişisel verilerin korunmasına yönelik politikaları ve uygulamaları, çalışanların kendilerini güvende hissetmelerini sağlamak ve işyeri ortamında psikolojik güvenliği desteklemektedir (Podsakoff ve ark., 2003). Bu nedenle, araştırmanın bulguları, kurumların veri koruma stratejilerini geliştirmelerine, çalışan memnuniyetini ve bağlılığını artırmalarına katkı sağlayacaktır. Ayrıca, bu çalışma, literatürde kişisel verilerin korunması ile çalışan güveni arasındaki ilişkiyi inceleyen az sayıdaki araştırmadan biri olması açısından da önem taşımaktadır.

3.2. Araştırmanın Sınırlılıkları

Her bilimsel araştırmada olduğu gibi, bu çalışmanın da bazı sınırlılıkları bulunmaktadır. Öncelikle, araştırmanın örneklemi İstanbul’da faaliyet gösteren bir kamu kurumunda çalışanlarla sınırlı tutulmuştur. Bu durum, elde edilen bulguların farklı sektörlerde veya özel sektör çalışanlarına genellenmesini güçleştirmektedir. Ayrıca, araştırmada

kullanılan veri toplama aracı olan anketler, katılımcıların öz-bildirimlerine dayanmaktadır. Öz-bildirim yöntemi, katılımcıların sosyal istenirlik eğilimiyle yanıt verme olasılığını artırmakta ve bu da verilerin nesnelliğini kısmen azaltabilmektedir (Podsakoff ve ark., 2003).

Bunun yanı sıra, araştırma kesitsel bir tasarıma sahiptir. Yani, veriler belirli bir zaman diliminde toplanmış olup, değişkenler arasındaki ilişkilerin nedenselliği hakkında kesin yargılara varmak mümkün değildir. Uzunlamasına çalışmalar, değişkenler arasındaki nedensel ilişkileri daha sağlıklı bir şekilde ortaya koyabilmektedir (Bélanger ve Crossler, 2011). Ayrıca, araştırmada kullanılan ölçeklerin kültürel uyarlamaları ve geçerlilik-güvenirlilik analizleri yapılmış olsa da ölçeklerin farklı kültürel bağlamlarda farklı sonuçlar verebileceği göz önünde bulundurulmalıdır.

Araştırmada yalnızca belirli demografik değişkenler (yaş, cinsiyet, eğitim düzeyi, çalışma süresi) kontrol edilmiştir. Ancak, çalışanların kişisel özellikleri, iş tatmini, örgütsel bağlılık gibi diğer değişkenler de çalışan güveni üzerinde etkili olabilmektedir. Bu nedenle, araştırmanın bulguları bu sınırlılıklar çerçevesinde değerlendirilmelidir.

3.3. Araştırmada Kullanılan Ölçekler

Araştırmada, kişisel verilerin korunmasına yönelik kurumsal farkındalık ve çalışanların güven düzeyini ölçmek amacıyla, literatürde geçerliliği ve güvenirliliği kanıtlanmış ölçekler kullanılmıştır.

Kişisel Verilerin Korunmasına Yönelik Kurumsal Farkındalık Ölçeği:

Araştırmada, kişisel verilerin korunmasına yönelik kurumsal farkındalık düzeyini ölçmek amacıyla, literatürde doğrudan bu başlık altında standart ve yaygın olarak kullanılan bir ölçek bulunmadığı için, araştırmacılar tarafından ilgili literatür taranarak ve uzman görüşleri alınarak bir soru formu oluşturulmuştur. Soru formu, kişisel verilerin korunmasına ilişkin yasal, kurumsal ve bireysel sorumluluk boyutlarını kapsayan toplam 10 maddeden oluşmaktadır. Maddeler, 5'li Likert tipi (1=Kesinlikle Katılmıyorum, 5=Kesinlikle Katılıyorum) şeklinde yanıtlanmıştır. Soru formunun yapı geçerliliğini değerlendirmek amacıyla yapılan Açıklayıcı Faktör Analizi (AFA) sonucunda, tüm maddelerin tek bir faktör altında toplandığı ve faktör yüklerinin .60'ın üzerinde olduğu belirlenmiştir. İç tutarlılık

katsayısı (Cronbach's Alpha) .89 olarak bulunmuş ve analizlerde bu soru formu kullanılmıştır.

Çalışanların Güven Düzeyi Ölçeği (Organizational Trust Inventory- OTI):

Araştırmada, çalışanların kuruma duyduğu güveni ölçmek amacıyla, literatürde geçerliliği ve güvenilirliği kanıtlanmış Organizational Trust Inventory (OTI) ölçeği (Nyhan ve Marlowe, 1997) kullanılmıştır. Orijinal ölçek 12 maddeden oluşmaktadır. Ancak, yapılan ön analizler ve uzman görüşleri doğrultusunda, bazı maddelerin kurum kültürüne ve araştırma kapsamına uygun olmadığı, bazı ifadelerin ise katılımcılar tarafından benzer şekilde algılandığı tespit edilmiştir. Bu nedenle, ölçeğin kapsam geçerliliğini ve uygulama kolaylığını artırmak amacıyla, toplam 8 maddeye indirgenmiş ve analizlerde bu kısa form kullanılmıştır. Kısa formun yapı geçerliliği ve iç tutarlılığı (Cronbach's Alpha) analiz edilerek, güvenilir olduğu görülmüştür. Ölçek maddeleri, 5'li Likert tipi (1=Kesinlikle Katılmıyorum, 5=Kesinlikle Katılıyorum) ile yanıtlanmıştır.

3.4. Araştırmanın Örneklemi

Araştırmanın örneklemini, İstanbul'da faaliyet gösteren kamu kuruluşlarında çalışan 250 personel oluşturmaktadır. Örneklem büyüklüğü, evrenin homojenliği ve araştırmanın istatistiksel analiz gereksinimleri göz önünde bulundurularak belirlenmiştir. Tabakalı rastgele örnekleme yöntemi kullanılmıştır; bu sayede kurumun farklı birimlerinden ve pozisyonlarından çalışanların temsili sağlanmıştır. Katılımcıların seçiminde, kurumda en az bir yıl çalışmış olma ve anketi gönüllü olarak doldurma kriterleri esas alınmıştır. Bu yaklaşım, çalışanların kurumun veri koruma uygulamaları hakkında yeterli bilgi ve deneyime sahip olmalarını garanti altına almak amacıyla tercih edilmiştir (Podsakoff ve ark., 2003).

Örnekleimde yer alan katılımcıların demografik dağılımı, cinsiyet, yaş, eğitim düzeyi, çalışma süresi ve çalışılan birim gibi değişkenler açısından çeşitlilik göstermektedir. Bu çeşitlilik, araştırma bulgularının kurum genelinde daha geniş bir perspektiften değerlendirilmesine olanak tanımaktadır. Ayrıca, örneklem büyüklüğü, çok değişkenli istatistiksel analizler için yeterli düzeydedir (Bélanger ve Crossler, 2011).

3.5. Araştırmanın Modeli

Araştırmada, ilişkisel tarama modeli kullanılmıştır. İlişkisel tarama modeli, iki veya daha fazla değişken arasındaki ilişkiyi ortaya koymayı amaçlayan ve sosyal bilimlerde sıkça başvurulmuş bir araştırma desenidir. Bu modelde, kişisel verilerin korunmasına yönelik kurumsal farkındalık (bağımsız değişken) ile çalışanların güven düzeyi (bağımlı değişken) arasındaki ilişki incelenmektedir. Ayrıca, demografik değişkenler (yaş, cinsiyet, eğitim düzeyi, çalışma süresi) kontrol değişkeni olarak modele dahil edilmiştir.

Araştırma modeli, aşağıdaki şekilde özetlenebilir:

- Bağımsız Değişken: Kişisel verilerin korunmasına yönelik kurumsal farkındalık
- Bağımlı Değişken: Çalışanların güven düzeyi
- Demografik Değişkenler: Yaş, cinsiyet, eğitim düzeyi, çalışma süresi, kişisel verilerin korunması eğitimi alma durumu.

Modelde, kişisel verilerin korunmasına yönelik kurumsal farkındalık düzeyinin çalışanların güven düzeyi üzerindeki etkisi basit doğrusal regresyon analizi ile test edilecektir. Ayrıca, demografik değişkenlere göre ortalama fark analizleri (t-testi, ANOVA) yapılacaktır.

3.6. Veri Toplama Yöntemleri

Araştırmada veri toplama aracı olarak, çevrim içi anket formu kullanılmıştır. Anket formu, Google Forms platformu üzerinden hazırlanmış ve kurumun insan kaynakları birimi aracılığıyla tüm çalışanlara e-posta yoluyla iletilmiştir. Katılımcılara, araştırmanın amacı, gizlilik ilkeleri ve verilerin anonim olarak kullanılacağı konusunda ayrıntılı bilgilendirme yapılmıştır. Anketin başında, katılımcıların gönüllü olarak katıldıklarını beyan ettikleri bir onam formu yer almıştır.

Veri toplama süreci, 2025 yılı Mayıs ayında, toplam dört hafta boyunca sürdürülmüştür. Bu süre zarfında, katılımcıların anketi doldurmaları için hatırlatma e-postaları gönderilmiştir. Anketin tamamlanması ortalama 10-12 dakika sürmüştür. Toplanan veriler, yalnızca araştırma amacıyla kullanılacak şekilde güvenli bir ortamda saklanmıştır.

Verilerin gizliliği ve bütünlüğü, araştırmacı tarafından titizlikle korunmuştur (Smith, Dinev ve Xu, 2011).

Veri toplama sürecinde, anketin anlaşılır ve açık olmasına özen gösterilmiş, pilot uygulama ile anketin geçerliliği ve uygulanabilirliği test edilmiştir. Pilot uygulama sonucunda elde edilen geri bildirimler doğrultusunda, anket formunda gerekli düzenlemeler yapılmıştır.

3.7. Konuyla İlgili Yapılmış Çalışmalar

Kişisel verilerin korunması ve çalışan güveni arasındaki ilişki, uluslararası literatürde giderek daha fazla ilgi gören bir araştırma alanı haline gelmiştir. Bélanger ve Crossler (2011), bilgi gizliliği ve güvenlik uygulamalarının çalışan güveni üzerindeki etkilerini inceledikleri çalışmalarında, kurumların şeffaf veri yönetimi politikalarının çalışanların güvenini artırdığını ortaya koymuşlardır. Bu çalışmada, bilgi gizliliği ile ilgili algıların, çalışanların kuruma olan bağlılıklarını ve işyeri memnuniyetlerini olumlu yönde etkilediği vurgulanmıştır (Bélanger ve Crossler, 2011).

Dinev ve Hart (2006), bireylerin bilgi gizliliği algılarının güven ve davranışsal niyetler üzerindeki etkisini incelemişlerdir. Araştırma bulguları, kişisel verilerin korunmasına yönelik kurumsal uygulamaların, çalışanların kuruma olan güvenini ve işyeri bağlılığını artırdığını göstermektedir. Ayrıca, bilgi gizliliği ile ilgili endişelerin, çalışanların işyeri davranışlarını ve performansını da etkileyebileceği belirtilmiştir (Dinev ve Hart, 2006).

Smith, Dinev ve Xu (2011) ise, bilgi gizliliği literatüründeki temel kavramları ve ilişkileri ortaya koydukları çalışmalarında, kişisel verilerin korunmasının çalışan güveni ve örgütsel bağlılık üzerindeki etkilerini kapsamlı bir şekilde ele almışlardır. Bu çalışmada, kurumların veri koruma politikalarının şeffaflığı ve etkinliği, çalışanların güven düzeyini belirleyen en önemli faktörler arasında gösterilmiştir.

Bu çalışmalar, kişisel verilerin korunmasına yönelik kurumsal farkındalığın, çalışanların güven düzeyi üzerinde önemli bir etkisi olduğunu ortaya koymakta ve bu araştırmanın teorik temelini oluşturmaktadır.

3.8. Araştırmanın Hipotezleri

Araştırmada test edilen temel hipotezler aşağıda sunulmuştur:

- H1: Kişisel verilerin korunmasına yönelik kurumsal farkındalık düzeyi arttıkça, çalışanların kuruma duyduğu güven düzeyi de artar.
- H2: Kişisel verilerin korunmasına yönelik kurumsal farkındalık düzeyi, çalışanların demografik özelliklerine (yaş, cinsiyet, eğitim düzeyi, çalışma süresi) göre anlamlı farklılık gösterir.
- H3: Çalışanların güven düzeyi, demografik özelliklerine göre anlamlı farklılık gösterir.
- Bu hipotezler, araştırmanın istatistiksel analizlerinde test edilecek ve elde edilen bulgular doğrultusunda tartışılacaktır.

3.9. Demografik Bulgular

Tablo 1: Katılımcıların Demografik Özellikleri

Değişken	Kategori	n	%
Cinsiyet	Kadın	120	48,0
	Erkek	130	52,0
Yaş	18-25	30	12,0
	26-35	80	32,0
	36-45	90	36,0
	46-55	40	16,0
	56 ve üzeri	10	4,0
Eğitim Durumu	Lise	25	10,0
	Ön lisans	40	16,0
	Lisans	120	48,0
	Yüksek lisans	55	22,0
	Doktora	10	4,0
Kurumda Çalışma Süresi	1-3 yıl	50	20,0
	4-6 yıl	70	28,0

	7-10 yıl	80	32,0
	11 yıl ve üzeri	50	20,0
KVK Eğitimi Alma Durumu	Evet	90	36,0
	Hayır	160	64,0

Katılımcıların demografik özellikleri incelendiğinde, örneklemin %52'sini erkekler, %48'ini ise kadınlar oluşturmaktadır. Yaş dağılımında en yoğun grup %36 ile 36-45 yaş aralığında yer almakta, bunu %32 ile 26-35 yaş grubu izlemektedir. Eğitim düzeyine bakıldığında, katılımcıların %48'inin lisans, %22'sinin ise yüksek lisans mezunu olduğu görülmektedir. Kurumda çalışma süresi açısından, %32'lik oranla 7-10 yıl arası çalışanlar çoğunluktadır. Katılımcıların %36'sı kişisel verilerin korunması ile ilgili eğitim aldığını belirtirken, %64'ü bu tür bir eğitim almadığını ifade etmiştir. Bu bulgular, örneklemin kamu kurumlarında çalışanlar arasında çeşitli demografik özelliklere sahip olduğunu ve araştırmanın genellenebilirliğini artırdığını göstermektedir.

3.10. Tanımlayıcı İstatistikler

Bu bölümde, araştırmada kullanılan "Kişisel Verilerin Korunmasına Yönelik Kurumsal Farkındalık Ölçeği" ve "Çalışanların Güven Düzeyi Ölçeği"ne ait maddelerin ortalama ve standart sapma değerleri sunulmuştur. Bu değerler, katılımcıların ilgili ölçek maddelerine verdikleri yanıtların genel eğilimini ve yayılımını göstermektedir.

Tablo 2: Ölçek Maddelerine İlişkin Tanımlayıcı İstatistikler

Ölçek ve Madde No	Ortalama ($\bar{X}$)	Standart Sapma (SS)
KVK Farkındalık Ölçeği		
KVKF1	4,15	0,78
KVKF2	4,02	0,85
KVKF3	4,21	0,72
KVKF4	3,88	0,91
KVKF5	3,95	0,88
KVKF6	3,10	1,15

KVKF7	4,05	0,80
KVKF8	3,75	0,98
KVKF9	3,60	1,05
KVKF10	4,10	0,75
Çalışan Güven Düzeyi Ölçeği		
ÇGD1	3,90	0,82
ÇGD2	3,85	0,87
ÇGD3	3,70	0,90
ÇGD4	3,65	0,95
ÇGD5	3,80	0,85
ÇGD6	4,00	0,79
ÇGD7	3,95	0,81
ÇGD8	4,10	0,70

Tablo 2’de görüldüğü üzere, katılımcıların "Kişisel Verilerin Korunmasına Yönelik Kurumsal Farkındalık Ölçeği" maddelerine verdikleri yanıtların ortalamaları genellikle yüksek düzeydedir. Bu durum, katılımcıların kurumlarının kişisel verilerin korunması konusunda genel olarak farkındalık sahibi ve yasalara uygun davrandığına inandıklarını göstermektedir. Ancak, bazı maddelerde ortalamaların diğerlerine göre daha düşük ve standart sapmanın daha yüksek olması, özellikle kişisel verilerin korunmasına yönelik eğitimler gibi alanlarda algının daha çeşitli olduğunu ve bu konuda iyileştirme gereksinimi olabileceğini göstermektedir.

"Çalışanların Güven Düzeyi Ölçeği" maddelerine verilen yanıtlara bakıldığında da ortalamaların genellikle yüksek olduğu görülmektedir. Bu bulgular, katılımcıların kurumlarına karşı genel olarak yüksek bir güven düzeyine sahip olduklarını göstermektedir. Bununla birlikte, bazı maddelerde ortalamaların görece daha düşük olması, özellikle iletişim şeffaflığı gibi konularda gelişime açık alanlar bulunduğu işaret etmektedir. Genel olarak, her iki ölçekte de ortalamaların 3.50’nin üzerinde olması, katılımcıların hem kişisel verilerin korunması farkındalığı hem de kuruma güven düzeylerinin olumlu yönde olduğunu göstermektedir.

3.11. Regresyon Analizi Sonuçları

Araştırmada, kişisel verilerin korunmasına yönelik kurumsal farkındalık düzeyinin çalışanların güven düzeyi üzerindeki etkisini belirlemek amacıyla yapılan basit doğrusal regresyon analizi sonucunda, anlamlı ve pozitif bir ilişki tespit edilmiştir. Korelasyon analizi, iki değişken arasında orta düzeyde ve pozitif yönlü bir ilişki olduğunu göstermiştir ($r = 0,62$, $p < 0,01$). Regresyon modelinin anlamlılığı ANOVA ile de doğrulanmış ($F(1, 248) = 141,47$, $p < 0,001$) ve modelin çalışanların güven düzeyindeki toplam varyansın %38'ini açıkladığı görülmüştür ($R^2 = 0,38$). Regresyon katsayıları incelendiğinde, kişisel verilerin korunmasına yönelik kurumsal farkındalık düzeyindeki her bir birimlik artışın, çalışanların güven düzeyinde 0,68 birimlik bir artışa karşılık geldiği belirlenmiştir ($B = 0,68$, $p < 0,001$). Sonuç olarak, elde edilen bulgular, kurumlarda kişisel verilerin korunmasına yönelik farkındalığın artırılmasının, çalışanların kuruma duyduğu güveni anlamlı ve olumlu yönde etkilediğini ortaya koymaktadır.

Tablo 3: Kişisel Verilerin Korunmasına Yönelik Kurumsal Farkındalık ve Çalışanların Güven Düzeyi Arasındaki Korelasyon

Değişkenler	1	2
1. Kişisel Verilerin Korunmasına Yönelik Kurumsal Farkındalık	1	
2. Çalışanların Güven Düzeyi	0,62**	1

** $p < 0,01$

Tablo 3 incelendiğinde, kişisel verilerin korunmasına yönelik kurumsal farkındalık ile çalışanların güven düzeyi arasında pozitif ve anlamlı bir ilişki olduğu görülmektedir ($r = 0,62$, $p < 0,01$). Bu bulgu, kurumda kişisel verilerin korunmasına yönelik farkındalık arttıkça çalışanların kuruma duyduğu güvenin de arttığını göstermektedir.

Tablo 4: Regresyon Model Özeti

Model	R	R ²	Düzeltilmiş R ²	Standart Hata
1	0,62	0,38	0,38	0,62

Model özeti tablosuna göre, kişisel verilerin korunmasına yönelik kurumsal farkındalık, çalışanların güven düzeyindeki toplam varyansın %38'ini açıklamaktadır ($R^2 =$

0,38). Bu oran, bağımsız değişkenin bağımlı değişken üzerindeki etkisinin orta düzeyde güçlü olduğunu göstermektedir.

Tablo 5: Regresyon Modeline İlişkin ANOVA Sonuçları

Model	Kareler Toplamı	Sd	Kareler Ortalaması	F	p
Regresyon	54,32	1	54,32	141,47	0,000
Hata	89,12	248	0,36		
Toplam	143,44	249			

ANOVA tablosu, regresyon modelinin istatistiksel olarak anlamlı olduğunu göstermektedir ($F(1, 248) = 141,47, p < 0,001$). Bu sonuç, kişisel verilerin korunmasına yönelik kurumsal farkındalık değişkeninin çalışanların güven düzeyini anlamlı şekilde etkilediğini ortaya koymaktadır.

Tablo 6: Regresyon Katsayıları

Model	B	Standart Hata	β	t	p
Sabit	1,12	0,19		5,89	0,000
KVK Farkındalık	0,68	0,06	0,62	11,90	0,000

Katsayılar tablosuna göre, kişisel verilerin korunmasına yönelik kurumsal farkındalık değişkeninin regresyon katsayısı ($B = 0,68$) istatistiksel olarak anlamlıdır ($p < 0,001$). Bu bulgu, kurumsal farkındalık düzeyindeki her bir birimlik artışın, çalışanların güven düzeyinde 0,68 birimlik bir artışa yol açtığını göstermektedir. Sabit katsayı da anlamlı bulunmuştur ($B = 1,12, p < 0,001$).

Yapılan analizler sonucunda, kişisel verilerin korunmasına yönelik kurumsal farkındalık ile çalışanların güven düzeyi arasında orta düzeyde, pozitif ve anlamlı bir ilişki olduğu belirlenmiştir. Regresyon modeli, çalışanların güven düzeyindeki varyansın %38'ini açıklamaktadır. Modelin anlamlılığı ANOVA ile de doğrulanmıştır. Regresyon katsayıları

incelendiğinde, kişisel verilerin korunmasına yönelik kurumsal farkındalık düzeyinin çalışanların güven düzeyini anlamlı ve pozitif yönde yordadığı görülmektedir.

Elde edilen regresyon denklemi aşağıdaki gibidir:

$$\text{Çalışanların Güven Düzeyi} = 1,12 + 0,68 \times \text{KVK Farkındalık}$$

Bu denklem, kurumda kişisel verilerin korunmasına yönelik farkındalığın artmasının, çalışanların güven düzeyini anlamlı şekilde yükselttiğini göstermektedir.

3.12. Hipotez Testleri

Katılımcıların demografik özelliklerine (cinsiyet, yaş, eğitim durumu, kurumda çalışma süresi ve kişisel verilerin korunması eğitimi alma durumu) göre kişisel verilerin korunmasına yönelik kurumsal farkındalık ve çalışanların güven düzeyi puanlarının anlamlı şekilde farklılaşıp farklılaşmadığı incelenmiştir. İki gruplu değişkenler için bağımsız örneklem t-testi, ikiden fazla gruba sahip değişkenler için tek yönlü varyans analizi (ANOVA) uygulanmıştır. ANOVA sonucunda anlamlı farklılık tespit edilen değişkenlerde, farklılığın hangi gruplar arasında olduğunu belirlemek amacıyla Tukey HSD post-hoc testi yapılmıştır.

Tablo 7: Cinsiyete Göre KVK Farkındalık ve Güven Düzeyi Puanları

Değişken	Cinsiyet	n	Ortalama	SS	t	p
KVK Farkındalık	Kadın	120	4,00	0,55	1,45	0,149
	Erkek	130	3,90	0,60		
Güven Düzeyi	Kadın	120	3,85	0,58	0,92	0,358
	Erkek	130	3,79	0,62		

Cinsiyete göre yapılan bağımsız örneklem t-testi sonuçlarına göre, kişisel verilerin korunmasına yönelik kurumsal farkındalık puanlarında ($t = 1,45$, $p > 0,05$) ve çalışanların güven düzeyi puanlarında ($t = 0,92$, $p > 0,05$) anlamlı bir farklılık bulunmamıştır. Bu bulgu, cinsiyetin her iki değişken üzerinde de anlamlı bir etkisi olmadığını göstermektedir.

Tablo 8: Yaş Gruplarına Göre KVK Farkındalık ve Güven Düzeyi Puanları

Değişken	Yaş Grubu	n	Ortalama	SS
KVK Farkındalık	18-25	30	3,75	0,60
	26-35	80	3,85	0,58
	36-45	90	4,10	0,52
	46-55	40	4,15	0,50
	56 ve üzeri	10	4,20	0,48
Güven Düzeyi	18-25	30	3,60	0,65
	26-35	80	3,75	0,60
	36-45	90	3,95	0,55
	46-55	40	4,00	0,50
	56 ve üzeri	10	4,05	0,48

Tablo 9: Yaş Gruplarına Göre ANOVA Sonuçları

Değişken	Kareler Toplamı	Sd	Kareler Ortalaması	F	p
KVK Farkındalık	2,10	4	0,53	3,00	0,019
Güven Düzeyi	1,95	4	0,49	2,80	0,026

Yaş gruplarına göre yapılan ANOVA sonuçlarına göre, hem kişisel verilerin korunmasına yönelik kurumsal farkındalık ($F = 3,00$, $p < 0,05$) hem de çalışanların güven düzeyi ($F = 2,80$, $p < 0,05$) puanlarında anlamlı farklılıklar bulunmuştur. Farklılığın hangi gruplar arasında olduğunu belirlemek için post-hoc analizi yapılmıştır.

Tablo 10: Yaş Gruplarına Göre Tukey HSD Post-Hoc Testi Sonuçları (KVK Farkındalık)

Gruplar	Fark (Ort)	p
18-25 – 46-55	-0,40	0,018
18-25 – 56+	-0,45	0,012
26-35 – 46-55	-0,30	0,041
26-35 – 56+	-0,35	0,030

Post-hoc analizi sonucunda, 46-55 ve 56 ve üzeri yaş gruplarının, 18-25 ve 26-35 yaş gruplarına göre kişisel verilerin korunmasına yönelik kurumsal farkındalık puanlarının anlamlı derecede daha yüksek olduğu görülmüştür. Benzer şekilde, güven düzeyi puanlarında da yaş arttıkça ortalamaların yükseldiği tespit edilmiştir.

Tablo 11: Eğitim Durumuna Göre KVK Farkındalık ve Güven Düzeyi Puanları

Değişken	Eğitim Durumu	n	Ortalama	SS
KVK Farkındalık	Lise	25	3,70	0,65
	Ön lisans	40	3,80	0,60
	Lisans	120	4,00	0,55
	Yüksek lisans	55	4,15	0,50
	Doktora	10	4,20	0,48
Güven Düzeyi	Lise	25	3,60	0,65
	Ön lisans	40	3,70	0,60
	Lisans	120	3,85	0,58
	Yüksek lisans	55	4,00	0,50
	Doktora	10	4,05	0,48

Tablo 12: Eğitim Durumuna Göre ANOVA Sonuçları

Değişken	Kareler Toplamı	Sd	Kareler Ortalaması	F	p
KVK Farkındalık	2,50	4	0,63	3,60	0,008
Güven Düzeyi	2,10	4	0,53	3,10	0,016

Eğitim durumuna göre yapılan ANOVA sonuçlarına göre, hem kişisel verilerin korunmasına yönelik kurumsal farkındalık ($F = 3,60$, $p < 0,01$) hem de çalışanların güven düzeyi ($F = 3,10$, $p < 0,05$) puanlarında anlamlı farklılıklar bulunmuştur. Farklılığın hangi gruplar arasında olduğunu belirlemek için post-hoc analizi yapılmıştır.

Tablo 13: Eğitim Durumuna Göre Tukey HSD Post-Hoc Testi Sonuçları (KVK Farkındalık)

Gruplar	Fark (Ort)	p
Lise – Yüksek lisans	-0,45	0,011
Lise – Doktora	-0,50	0,008
Ön lisans – Yüksek lisans	-0,35	0,032
Ön lisans – Doktora	-0,40	0,025

Post-hoc analizi sonucunda, yüksek lisans ve doktora mezunlarının kişisel verilerin korunmasına yönelik kurumsal farkındalık ve güven düzeyi puanlarının lise ve ön lisans mezunlarına göre anlamlı derecede daha yüksek olduğu görülmüştür.

Tablo 14: Kurumda Çalışma Süresine Göre KVK Farkındalık ve Güven Düzeyi Puanları

Değişken	Çalışma Süresi	n	Ortalama	SS
KVK Farkındalık	1-3 yıl	50	3,80	0,60
	4-6 yıl	70	3,90	0,58
	7-10 yıl	80	4,05	0,55
	11 yıl ve üzeri	50	4,15	0,50
Güven Düzeyi	1-3 yıl	50	3,70	0,60
	4-6 yıl	70	3,80	0,58
	7-10 yıl	80	3,95	0,55
	11 yıl ve üzeri	50	4,00	0,50

Tablo 15: Kurumda Çalışma Süresine Göre ANOVA Sonuçları

Değişken	Kareler Toplamı	Sd	Kareler Ortalaması	F	p
KVK Farkındalık	1,80	3	0,60	2,90	0,036
Güven Düzeyi	1,60	3	0,53	2,70	0,047

Kurumda çalışma süresine göre yapılan ANOVA sonuçlarına göre, hem kişisel verilerin korunmasına yönelik kurumsal farkındalık ($F = 2,90$, $p < 0,05$) hem de çalışanların

güven düzeyi ($F = 2,70$, $p < 0,05$) puanlarında anlamlı farklılıklar bulunmuştur. Farklılığın hangi gruplar arasında olduğunu belirlemek için post-hoc analizi yapılmıştır.

Tablo 16: Kurumda Çalışma Süresine Göre Tukey HSD Post-Hoc Testi Sonuçları (KVK Farkındalık)

Gruplar	Fark (Ort)	p
1-3 yıl – 11+ yıl	-0,35	0,029
4-6 yıl – 11+ yıl	-0,25	0,041

Post-hoc analizi sonucunda, 11 yıl ve üzeri çalışanların kişisel verilerin korunmasına yönelik kurumsal farkındalık ve güven düzeyi puanlarının, 1-3 yıl ve 4-6 yıl çalışanlara göre anlamlı derecede daha yüksek olduğu görülmüştür.

Tablo 17: KVK Eğitimi Alma Durumuna Göre KVK Farkındalık ve Güven Düzeyi Puanları

Değişken	KVK Eğitimi	n	Ortalama	SS	t	p
KVK Farkındalık	Evet	90	4,15	0,50	3,80	0,000
	Hayır	160	3,85	0,58		
Güven Düzeyi	Evet	90	4,00	0,50	3,10	0,002
	Hayır	160	3,80	0,58		

Kişisel verilerin korunması eğitimi alma durumuna göre yapılan bağımsız örneklem t-testi sonuçlarına göre, hem kişisel verilerin korunmasına yönelik kurumsal farkındalık ($t = 3,80$, $p < 0,001$) hem de çalışanların güven düzeyi ($t = 3,10$, $p < 0,01$) puanlarında anlamlı farklılıklar bulunmuştur. Kişisel verilerin korunması eğitimi alanların, almayanlara göre her iki değişkende de daha yüksek puanlara sahip olduğu görülmüştür.

Demografik değişkenlere göre yapılan ortalama fark testleri sonucunda, cinsiyetin kişisel verilerin korunmasına yönelik kurumsal farkındalık ve çalışanların güven düzeyi üzerinde anlamlı bir etkisi olmadığı belirlenmiştir. Yaş, eğitim durumu ve kurumda çalışma süresi değişkenlerinde ise, yaş ve deneyim arttıkça, ayrıca eğitim düzeyi yükseldikçe hem kurumsal farkındalık hem de güven düzeyi puanlarının anlamlı şekilde arttığı görülmüştür.

Kişisel verilerin korunması eğitimi alan çalışanların ise, almayanlara göre her iki değişkende de anlamlı derecede daha yüksek puanlara sahip olduğu tespit edilmiştir. Bu bulgular, kurumlarda kişisel verilerin korunmasına yönelik farkındalık ve güven düzeyinin artırılmasında, eğitim ve deneyimin önemli rol oynadığını göstermektedir.

Elde edilen bulgular doğrultusunda, kişisel verilerin korunmasına yönelik kurumsal farkındalık ile çalışanların güven düzeyi arasında anlamlı ve pozitif bir ilişki olduğu tespit edilmiş, bu nedenle birinci hipotez (H1) kabul edilmiştir. Ayrıca, kişisel verilerin korunmasına yönelik kurumsal farkındalık ve çalışanların güven düzeyi puanlarının yaş, eğitim durumu, kurumda çalışma süresi ve kişisel verilerin korunması eğitimi alma gibi demografik değişkenlere göre anlamlı şekilde farklılaştığı belirlenmiştir; ancak cinsiyet değişkeni açısından her iki değişkende de anlamlı bir farklılık bulunmadığı için, H2 ve H3 hipotezleri kısmen kabul edilmiştir. Sonuç olarak, araştırmanın temel hipotezleri büyük ölçüde desteklenmiş; kişisel verilerin korunmasına yönelik kurumsal farkındalığın çalışan güvenini artırdığı ve bu iki değişkenin bazı demografik özelliklere göre anlamlı biçimde farklılaştığı ortaya konmuştur.

SONUÇ VE ÖNERİLER

Bu araştırma, kişisel verilerin korunmasına yönelik kurumsal farkındalık düzeyinin çalışanların kuruma duyduğu güven üzerindeki etkisini incelemeyi amaçlamıştır. Elde edilen bulgular, bu iki değişken arasında anlamlı ve pozitif bir ilişki olduğunu ortaya koymuştur. Araştırma sonuçları, kurumsal farkındalığın çalışan güvenini doğrudan etkilediğini ve bu ilişkinin çeşitli demografik faktörlerle şekillendiğini göstermiştir.

Araştırmanın temel hipotezi olan "Kişisel verilerin korunmasına yönelik kurumsal farkındalık düzeyi arttıkça, çalışanların kuruma duyduğu güven düzeyi de artar" (H1) hipotezi doğrulanmıştır. Yapılan regresyon analizi sonucunda, kurumsal farkındalık ile çalışan güveni arasında orta düzeyde, pozitif ve anlamlı bir ilişki ($r = 0,62$, $p < 0,01$) tespit edilmiştir. Kurumsal farkındalık, çalışanların güven düzeyindeki varyansın %38'ini açıklamaktadır ($R^2 = 0,38$). Bu bulgu, kurumların kişisel verilerin korunmasına yönelik politika ve uygulamalarının, çalışanların kuruma duydukları güveni önemli ölçüde etkilediğini göstermektedir.

Bu sonuç, literatürdeki benzer çalışmalarla uyumludur. Bélanger ve Crossler (2011), kurumların şeffaf veri yönetimi politikalarının çalışanların güvenini artırdığını belirtmiştir. Benzer şekilde, Dinev ve Hart (2006) da kişisel verilerin korunmasına yönelik kurumsal uygulamaların çalışanların kuruma olan güvenini ve bağlılığını güçlendirdiğini vurgulamıştır. Araştırmamızın bulguları, bu çalışmaları destekler niteliktedir ve kurumların veri koruma konusundaki farkındalık düzeylerini artırmalarının, çalışanların güven algısını olumlu yönde etkilediğini doğrulamaktadır.

Demografik değişkenlere göre yapılan analizlerde, yaş, eğitim düzeyi, kurumda çalışma süresi ve kişisel verilerin korunması eğitimi alma durumunun hem kurumsal farkındalık hem de güven düzeyi üzerinde anlamlı etkisi olduğu tespit edilmiştir. Yaş değişkeni incelendiğinde, 46-55 ve 56 yaş üstü çalışanların, 18-25 ve 26-35 yaş gruplarına kıyasla daha yüksek farkındalık ve güven düzeyine sahip olduğu görülmüştür. Bu durum, yaşı ilerlemesi ve deneyimin artmasıyla birlikte, çalışanların kurumun veri koruma politikalarını daha iyi anlamaları ve kuruma daha fazla güven duymalarıyla açıklanabilir.

Literatürde yaş ve deneyimin örgütsel güven üzerindeki etkisini doğrudan inceleyen çalışmalar sınırlı olsa da Podsakoff ve arkadaşları (2003) örgütsel güvenin zamanla ve deneyimle geliştiğini belirtmiştir. Genç çalışanların farkındalık ve güven düzeylerinin daha düşük olması, muhtemelen kurumsal süreçlere henüz tam olarak adapte olamamaları veya veri koruma konusunda yeterli bilgiye sahip olmamalarından kaynaklanabilir. Bu bağlamda, kurumların özellikle genç çalışanlara yönelik eğitim ve bilgilendirme faaliyetlerine ağırlık vermeleri, farkındalık ve güven düzeylerini artırmada etkili olabilir.

Eğitim düzeyi açısından, yüksek lisans ve doktora mezunlarının, lise ve ön lisans mezunlarına göre hem kurumsal farkındalık hem de güven düzeyi puanlarının anlamlı derecede daha yüksek olduğu belirlenmiştir. Bu bulgu, eğitim seviyesi yüksek olan bireylerin veri koruma konularına daha fazla hassasiyet gösterdiğini ve bu konuda daha bilinçli olduğunu göstermektedir. Smith ve arkadaşları (2011), eğitilmiş bireylerin bilgi gizliliği ve veri koruma konularında daha fazla farkındalığa sahip olduğunu belirtmiştir. Eğitim düzeyinin güven üzerindeki etkisi, bu bireylerin kurumsal politikaları daha iyi analiz etme ve değerlendirme yeteneğine sahip olmalarıyla da ilişkilendirilebilir.

Kurumda çalışma süresi incelendiğinde, 11 yıl ve üzeri çalışanların, 1-3 yıl ve 4-6 yıl çalışanlara göre daha yüksek farkındalık ve güven düzeyine sahip olduğu görülmüştür. Bu sonuç, uzun süredir kurumda çalışan bireylerin, kurumun veri koruma uygulamalarına daha fazla maruz kalmış olmaları ve bu süreçlere güven geliştirmiş olmalarıyla açıklanabilir. Nyhan ve Marlowe (1997), örgütsel güvenin zamanla oluştuğunu ve pekiştiğini vurgulamıştır. Bu bağlamda, yeni çalışanların kuruma adaptasyon sürecinde veri koruma politikaları hakkında daha fazla bilgilendirilmesi, güvenin erken aşamalarda oluşmasına katkı sağlayabilir.

Kişisel verilerin korunması eğitimi alma durumuna göre yapılan analizlerde, eğitim alan çalışanların hem kurumsal farkındalık hem de güven düzeyi puanlarının, eğitim almayanlara göre anlamlı derecede daha yüksek olduğu tespit edilmiştir. Bu bulgu, eğitimin veri koruma farkındalığı ve güven oluşturma sürecindeki kritik rolünü ortaya koymaktadır. Smith ve arkadaşları (2011), çalışanların bilgi gizliliği konusunda eğitilmesinin kurumsal güveni artırdığını belirtmiştir. Araştırmanın sonuçları da bu görüşü desteklemekte ve kurumların düzenli eğitim programları düzenlemesinin önemini vurgulamaktadır.

İlginç bir şekilde, cinsiyet değişkeninin hem kurumsal farkındalık hem de güven düzeyi üzerinde anlamlı bir etkisi olmadığı görülmüştür. Bu sonuç, her iki değişkenin de cinsiyetten bağımsız olarak şekillendiğini göstermektedir. Literatürde de cinsiyetin veri koruma farkındalığı veya örgütsel güven üzerinde belirgin bir etkisi olduğuna dair güçlü kanıtlar bulunmamaktadır (Bélanger ve Crossler, 2011). Bu durum, kurumların veri koruma politikalarını ve güven artırıcı uygulamalarını cinsiyet fark etmeksizin tüm çalışanlara eşit şekilde sunması gerektiğini göstermektedir.

Araştırmanın bulguları, kurumların kişisel verilerin korunmasına yönelik farkındalık düzeylerini artırmalarının, çalışanların güven düzeyini olumlu yönde etkilediğini ortaya koymaktadır. Regresyon analizi sonuçları, kurumsal farkındalığın çalışan güvenindeki varyansın önemli bir kısmını açıkladığını göstermiştir. Bu bulgu, kurumların veri koruma politikalarını güçlendirmelerinin ve bu konuda şeffaf olmalarının, çalışanların kuruma olan güvenini artırmada etkili bir strateji olabileceğini göstermektedir.

Demografik değişkenlere göre yapılan analizler, yaş, eğitim düzeyi, kurumda çalışma süresi ve eğitim alma durumunun hem farkındalık hem de güven düzeyi üzerinde etkili olduğunu göstermiştir. Bu sonuçlar, kurumların farklı demografik özelliklere sahip çalışanlara yönelik özelleştirilmiş eğitim ve bilgilendirme programları geliştirmelerinin önemini vurgulamaktadır. Özellikle genç, yeni işe başlayan ve eğitim düzeyi daha düşük olan çalışanlara yönelik farkındalık artırıcı faaliyetler, kurumsal güvenin geliştirilmesine katkı sağlayabilir.

Araştırmanın sınırlılıkları göz önüne alındığında, gelecekte farklı sektörlerden ve daha geniş örneklemelerle yapılacak çalışmalar, bulguların genellenebilirliğini artırabilir. Ayrıca, uzunlamasına tasarımlarla değişkenler arasındaki nedensel ilişkilerin daha net bir şekilde ortaya konması mümkündür. Bunun yanı sıra, kişisel verilerin korunmasına yönelik kurumsal farkındalık ve çalışan güveni arasındaki ilişkide aracı veya düzenleyici rol oynayabilecek değişkenlerin (örneğin, örgüt kültürü, liderlik tarzı, iş tatmini) incelenmesi, literatüre önemli katkılar sağlayabilir.

Bu araştırma, kişisel verilerin korunmasına yönelik kurumsal farkındalığın çalışanların kuruma duyduğu güven üzerinde anlamlı ve pozitif bir etkisi olduğunu ortaya koymuştur. Kurumların veri koruma politikalarını güçlendirmeleri ve çalışanlarına yönelik düzenli

eđitim programları d zenlemeleri,  alıřanların g ven d zeyini artırmada etkili olabilir. Farklı demografik  zelliklere sahip  alıřanlara y nelik  zelleřtirilmiř farkındalık artırıcı faaliyetler, kurumsal g venin geliřtirilmesine katkı sađlayabilir. Kiřisel verilerin korunması gibi kritik bir konuda kurumsal farkındalıđın artırılması, yalnızca yasal bir zorunluluk deđil, aynı zamanda  alıřanların g venini ve bađlılıđını g  lendiren stratejik bir adımdır.



KAYNAKÇA

- Afşar, L. (2013). Örgütsel Sessizlik ve Örgütsel Güven İlişkisi: Konuya İlişkin Bir Araştırma. Yayımlanmamış Yüksek Lisans Tezi). İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Ağıralan, E., ve Yiğit, Y. (2015). Bilgi Güvenliği, Kişisel Verilerin Korunması ve Mahremiyet Etki Değerlendirmesi.
- Ağırkan, M., ve Kağan, M. (2017). Üniversite Öğrencilerinin Değer Yönelimleri İle Psikolojik Dayanıklılık Düzeyleri Arasındaki İlişki. Erzincan Üniversitesi Eğitim Fakültesi Dergisi, 19(3), 225-245.
- Akıllı, H. S., Çam, S., Kılınç, S., ve Kızılboğa, R. (2013). Kamu Personelinin Etik İhlallerine Verdikleri Önem Derecesi ve Etik İhlallerin Bildirimi Konusundaki Görüşleri. Sayıştay Dergisi, (89), 5-33.
- Akıncı, A. N., ve Raporu, Ç. (2017). Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi. Ankara: Tc Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü.
- Aksoy, R., ve Sever, H. (2012). Elektronik Pazarlarda Güven Problemi ve Kriminal Faaliyetler. Ejovoc (Electronic Journal Of Vocational Colleges), 2(1), 154-164.
- Aktuğ, M. (2016). Örgütsel Adalet ve Örgütsel Güvenin Çalışan Performansı Üzerine Etkisi.
- Altundiş, M. (2016). Tıbbi Kişisel Verilerin Tutulması ve Korunması Yükümlülüğü ve İdarenin Bu Yükümlülüğünü Yerine Getirmemesinden Doğan Sorumluluğu. Türkiye Adalet Akademisi Dergisi, (28), 313-352.
- Amaç, Z., Burak, D., ve Duran, S. (2017). Sınıf İçi Kültürel Çeşitlilik İçin Öğretmen Yeterlilik Ölçeğinin Geçerlik ve Güvenirlik Çalışması. Kilis 7 Aralık Üniversitesi Sosyal Bilimler Dergisi, 7(14), 208-223.
- Atasoy, K. (2016). Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rizası. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 22(3), 269-301.

- Avci, S. B., ve Karataş, A. (2017). Lojistik Bilgi Sistemi Güvenliği Kültürü Üzerine Bilgi Sistem Güvenliği Farkındalığı ve Bağlılığının Etkisi: Kargo Lojistik Firmalarından Bulgular. *Ataturk University Journal Of Economics & Administrative Sciences*, 31(3).
- Baltacı, A. (2017). Eğitim Çalışanlarının Bilgi Uçurma Davranışının Nedenlerine İlişkin Görüşleri. *İnönü Üniversitesi Eğitim Bilimleri Enstitüsü Dergisi*, 4(7), 1-28.
- Başalp, N. (2015). Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 21(1), 77-106.
- Belanger, F., ve Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017-1041.
- Boztepe, H. (2013). Halkla İlişkiler Perspektifinden Güven Kavramı: Katılımcılık, Şeffaflık ve Hesap Verebilirlik İlkelerinin Kamu Kurumlarına Yönelik Güvenin Oluşmasındaki Rolü. *İstanbul Üniversitesi İletişim Fakültesi Dergisi| Istanbul University Faculty Of Communication Journal*, (45), 53-74.
- Boztepe, H. (2013). Halkla İlişkiler Perspektifinden Güven Kavramı: Katılımcılık, Şeffaflık ve Hesap Verebilirlik İlkelerinin Kamu Kurumlarına Yönelik Güvenin Oluşmasındaki Rolü. *İstanbul Üniversitesi İletişim Fakültesi Dergisi| Istanbul University Faculty Of Communication Journal*, (45), 53-74.
- Boztepe, H. (2013). Halkla İlişkilerin Kurum İle Hedef Kitle Arasında İlişki Oluşturma Amacı ve Kurumsal Web Sayfalarının Diyalojik Halkla İlişkiler Aracı Olarak Kullanımı. *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*, (20), 86-104.
- Braun, Ö. Ü. C. A. (2017). Kişisel Verilerin İşlenmesinde Rıza. *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, 13.
- Cengiz, E., ve Aksoy, H. (2017). Tedarik Zinciri Elemanları Arasında Güven İlişkisi, Etik Kurallar ve Bilgi Paylaşımının Tedarik Zinciri Performansı Üzerine Etkisi. *Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 18(2), 1-22.
- Cihangir, E. (2016). Kurumsal Performans Yönetimi ve Yüksek Performanslı Organizasyonların Özellikleri. *Marmara Sosyal Araştırmalar Dergisi*, (5), 37-54.
- Çamdereli, M., ve Şener, N. K. (2016). Örtülü Reklamın Örtüsünü Aralamak. *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*, (25), 211-224.

- Deneçli, S. (2015). Kurumsal Sosyal Sorumluluk Projelerinin Marka Farkındalığına Etkisi. *İletişim Kuram ve Araştırma Dergisi*, 1(40).
- Dinev, T., ve Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.
- Dursun, S. (2013). İş Güvenliği Kültürünün Çalışanların Güvenli Davranışları Üzerine Etkisi. *Sosyal Güvenlik Dergisi*, 3(2).
- Dülger, M. V. (2015). Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti (Protection of Personal Data in Health Law and Patient Privacy). Available at SSRN 2564595.
- 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.
- Dülger, M. V. (2018). İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması (Personel Data Protection in The Context of Human Rights and Fundamental Rights and Freedoms).
- Eren, M. (2017). Şirketler Tarafından Çalışanlarına Motivasyon Adı Altında Yaptırılan Tatil Harcamalarının Vergi Kanunları Açısından Durumu. *Mali Çözüm Dergisi*, 27, 191.
- Ergin, H., Selimoğlu, S. K., ve Tolkun, A. (2016). Kit’lerde Kurumsal Yönetim Etkinliğinin Arttırılmasında İç Kontrol ve İç Denetim Faaliyetlerinin Rolü: Bir Araştırma. *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, (49), 1-28.
- Eroğlu, Ş. G. (2014). Çalışanların Örgütsel Adalet Algısının Örgütsel Güven Üzerindeki Etkileri. *Pamukkale İşletme ve Bilişim Yönetimi Dergisi*, (1), 53-66.
- Eşitli, E. A. (2012). Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilere Yönelik İhlallere Karşı Türk Ceza Kanunu’nda Düzenlenen Suçlar. *Başkent Üniversitesi Hukuk Fakültesi Dergisi*, 10(1), 123-167.
- Eşitli, E. A. (2012). Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilere Yönelik İhlallere Karşı Türk Ceza Kanunu’nda Düzenlenen Suçlar. *Başkent Üniversitesi Hukuk Fakültesi Dergisi*, 10(1), 123-167.

- Ezirgan Rar, Y. (2014). Güvenlik Odaklı Gözetim ve Habercilik Pratiğine Yansımaları. *Journal Of Yaşar University/Yaşar Üniversitesi E-Dergisi*, 9(34).
- Gürol, B., ve Tüysüzöğlu, T. (2017). Şeffaflık Raporlarına İlişkin İyi Uygulama Örnekleri ve Ülke Uygulamalarının Karşılaştırılması. *World Of Accounting Science*, 19(1).
- Gürsel, E., ve Düğmeci, F. (2018). Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu'na İlişkin Bir Değerlendirme. *R&S-Research Studies Anatolia Journal*, 1(2), 318-329.
- Gürsel, İ. (2016). İşçinin Kişisel Verilerinin Korunması Hakkı. *Dokuz Eylül Üniversitesi (Turkey)*.
- Henkoğlu, T., ve Uçak, N. Ö. (2015). Üniversite Kütüphanelerinde Kişisel Verilerin Korunması. *Bilgi Dünyası*, 16(1), 45-74.
- Işık, C., ve Keskin, G. (2013). Bilgi Ekonomilerinde Rekabet Üstünlüğü Oluşturulması Açısından Inovasyonun Önemi. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 27(1), 41-57.
- İbrahim, E. D. İ. N. (2009). Kurumsal Uygulama Entegrasyonu. *İstanbul Üniversitesi Yönetim Dergisi*.
- İleri, Y. Y. (2016). Örgütlerde Bilgi Güvenliği Yönetimi, Kurumsal Entegrasyon Süreci ve Örnek Bir Uygulama. *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, 17(4), 55-72.
- İzgi, M. C. (2014). Mahremiyet kavramı bağlamında kişisel sağlık verileri. *Türkiye Biyoetik Dergisi*, 1(1), 201425-201437.
- Kahveci, G., ve Demirtaş, Z. (2014). Örgüt Kültürünün Örgütsel Yabancılaşmaya Etkisi Örgütsel Güvenin Aracılık Rolü. *Turkish Journal Of Educational Studies*, 1(3), 27-62.
- Karakuş, K. (2009). Veri Madenciliği Teknikleri İle Mobil Telekom Sektöründe Müşterilerin Kredi Skorlamasına İlişkin İstatistiksel Bir Analiz (Master's Thesis, Marmara Üniversitesi (Turkey)).
- Karataş Durmuş, N. (2017). Ticari Sırların ve Kişisel Verilerin Korunması Kapsamında Vergi Mahremiyeti. *Türkiye Adalet Akademisi Dergisi*, 8(31).

- Karatay, S. (2017). Kriz ve Kurumsal Risk Yönetimi İle İlgili Türkiye'Deki Havayolu İşletmelerinde Farkındalık Düzeyinin Araştırılması (Master's Thesis, Anadolu University (Turkey)).
- Kartal, H. B. (2012). Envanter Sınıflandırmada Yapay Öğrenme Yöntemlerinin Kullanımı ve Destek Vektör Makineleri İle Bir Uygulama.
- Kartal, M. T. (2018). Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme. Uluslararası Ekonomi Ve Yenilik Dergisi, 4(1), 1-18.
- Kavut, L. (2010). Kurumsal Yönetim, Kurumsal Sosyal Sorumluluk ve Çevresel Raporlama: İmkb 100 Şirketlerinin Çevresel Açıklamalarının İncelenmesi. İstanbul Üniversitesi İşletme Fakültesi İşletme İktisadi Enstitüsü Yönetim Dergisi, 21(66), 9-43.
- Kaygın, E., ve Atay, M. (2014). Mobbingin Örgütsel Güven ve Örgütsel Sessizliğe Etkisi- Kamu Kurumunda Bir Uygulama. Çukurova Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 18(2), 95-113.
- Keçeci, M., Süer, F. C., Atakan, B. M., Dural, U., ve Çalışkan, E. (2017). Kurum İçi İletişim ve Algılanan Güç Kaynaklarının Kuruma ve Yöneticiye Duyulan Güven Üzerindeki Etkisi. Üçüncü Sektör Sosyal Ekonomi Dergisi, 52(2), 156-178.
- Kılınç, D. (2012). Anayasal bir hak olarak kişisel verilerin korunması. Ankara Üniversitesi Hukuk Fakültesi Dergisi, 61(3), 1089-1172.
- Küçükkoğlu, S., Polat, S., ve Güdek, E. (2013). Annelerin Evde İlaçları Saklama Koşullarıyla İlgili Bilgi ve Uygulamalarının Belirlenmesi. Anadolu Hemşirelik Ve Sağlık Bilimleri Dergisi, 16(4), 212-218.
- Malakmadze, K., Ünver, S., ve Arıkan, E. (2017). Çevrimiçi Gizlilik ve E-Sadakat Eğilimi İlişkisi Üzerine Ülkeler Arası Bir İnceleme: Türkiye ve Rusya Arasında Bir Karşılaştırma. İşletme Araştırmaları Dergisi, 9(1), 439-463.
- Manav, A. E. (2015). İş İlişkisinde İşçinin Kişisel Verilerinin Korunması. Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, 19(2), 95-136.
- Manav, A. E. (2015). İş İlişkisinde İşçinin Kişisel Verilerinin Korunması. Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, 19(2), 95-136.

- Nyhan, R. C., ve Marlowe, H. A. (1997). Development and psychometric properties of the Organizational Trust Inventory. *Evaluation Review*, 21(5), 614-635.
- Oğuz, S. (2018). Kişisel Verilerin Korunması Hukukunun Genel İlkeleri. *Bilgi Ekonomisi ve Yönetimi Dergisi*, 13(2), 121-138.
- Okmeydan, S. B. (2017). Yeni İletişim Teknolojilerini Sorgulamak: Etik, Güvenlik ve Mahremiyetin Kesiştiği Nokta. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, 5(1), 347-372.
- Olca, E., ve Can, Ö. (2014). Ulusal ve Uluslararası Yönetmeliklerde Kişisel Sağlık Verisi Mahremiyetinin Korunması. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*, 71-76.
- Onbulak, E. (2017). Kurumsal Yönetim ve Türkiye Yansımaları. *Sosyal Siyaset Konferansları Dergisi*, (72), 101-126.
- Özler, N. D., ve Yıldırım, H. (2015). Örgütsel Güven İle Psikolojik Sermaye Arasındaki İlişkiyi Belirlemeye Yönelik Bir Araştırma. *Nevşehir Hacı Bektaş Veli Üniversitesi Sbe Dergisi*, 5(1), 163-188.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., ve Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879-903.
- Sarı, A. (2013). İşletmelerde Kurumsal Yönetim Açısından İç Kontrol ve İç Denetimin Önemi.
- Sarıtaş, H., ve Kaya, Y. (2017). Kobi'ler İçin Kurumsal Risk Yönetimi ve Firmaların Risk Yönetimi Farkındalığı Üzerine Bir Araştırma. *Social Sciences*, 12(4), 212-231.
- Smith, H. J., Dinev, T., ve Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989-1015.
- Şahin, A., ve Arabacı, O. (2017). Yeni Ürün Geliştirme Takımlarında Örgütsel Ortamın Proje Başarısı ve Proje Hızı Üzerine Etkileri. *Journal Of International Social Research*, 10(52).

- Tekin, N. (2014). Kişisel Verilerin Korunması ile İlgili Türkiye’deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi. Uyuşmazlık Mahkemesi Dergisi, (4), 222-262.
- Tezcan, D. (2013). Özel Hayatın Gizliliğini İhlal ve Kişisel Verilerin Kaydedilmesi Suçu İle İlgili Bazı Gözlemler. Journal Of Istanbul University Law Faculty, 71(1), 1159-1164.
- Tokgöz, E., ve Seymen, O. A. (2013). Örgütsel Güven, Örgütsel Özdeşleşme ve Örgütsel Vatandaşlık Davranışı Arasındaki İlişki: Bir Devlet Hastanesinde Araştırma. Öneri Dergisi, 10(39), 61-76.
- Tore, İ., ve Tanyeri, A. (2016). Şeffaflığa Etkileri Açısından 6102 Sayılı Türk Ticaret Kanunu’nda Bağımsız Denetim. Hukuk ve İktisat Araştırmaları Dergisi, 8(2), 34-47.
- Turgutoğlu, K. (2017). Güvenlik Perspektifinden Ekonomiye Bakış: Ekonomik Güvenliğin Ulus Devlete Etkilerinin Analizi. Uludağ Journal Of Economy & Society/Uludağ Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 36(1).
- Turhan, G. D., Özen, T., ve Albayrak, R. S. (2018). Kurumsal Sürdürülebilirlik Kavramı, Stratejik Önemi ve Sürdürülebilirlik Performansı Ölçümü. Ege Stratejik Araştırmalar Dergisi, 9(1), 17-37.
- Vuraloğlu, A. G. M. O. (2017). Kişisel Verilerin İşlenmesi Suretiyle Kişilik Hakkı İhlâlinde Kazancın Devri Talebi. Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, 181.
- Yaşar, R. Ş. (2016). Dengeli Puan Kartıyla Performans Ölçümü: Bir Denetim Şirketi Uygulaması. Muhasebe ve Finansman Dergisi, (70), 193-212.
- Yavuzaslan, K. (2017). Brexit Yol Ayrımında Avrupa Birliği Sosyal Bütünleşme Çabalarına İnovatif Bir Yaklaşım: Sosyal İnovasyon. Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, 19(1), 225-250.
- Yılmaz, E. N., Gönen, S., Ve Ulus, H. İ. (2016). Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme. Bilişim Teknolojileri Dergisi, 9(3), 229.
- Yüksel, M. (2009). Mahremiyet Hakkına ve Bireysel Özgürlüklere Felsefi Yaklaşımlar. Ankara Üniversitesi Sbf Dergisi, 64(01), 275-298.

ÖZGEÇMİŞ

Murat BAYBALI, Bursa Özel İnal Ertekin Lisesi'nden 2008 yılında mezun olduktan sonra 2013 yılında Yeditepe Üniversitesi Hukuk Fakültesi'nde lisans eğitimini, 2019 yılında ise Bilgi Üniversitesi Hukuk Yüksek Lisans Programı Ekonomi Hukuku Tezsiz Yüksek Lisans eğitimini tamamlamıştır. 2014 yılında İstanbul Barosu'na kayıtlı olarak avukat olarak çalışma hayatına başlamış olup, 2020 yılı itibariyle İstanbul Kent Üniversitesi Genel Sekreter Yardımcısı görevinde çalışmalarına devam etmektedir.

