İBN HALDUN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI

YÜKSEK LİSANS TEZİ

TELE ÇALIŞMADA İZLEME VE GÖZETLEME ARAÇLARININ KİŞİSEL VERİLERİN KORUNMASI BAĞLAMINDA DEĞERLENDİRİLMESİ

ABDÜLMECİT GÜLDAĞI

TEZ DANIŞMANI
PROF. DR. YELİZ BOZKURT GÜMRÜKÇÜOĞLU

İSTANBUL, 2025

İBN HALDUN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI

YÜKSEK LİSANS TEZİ

TELE ÇALIŞMADA İZLEME VE GÖZETLEME ARAÇLARININ KİŞİSEL VERİLERİN KORUNMASI BAĞLAMINDA DEĞERLENDİRİLMESİ

ABDÜLMECİT GÜLDAĞI

TEZ JÜRİSİ ÜYELERİ
PROF. DR. YELİZ BOZKURT GÜMRÜKÇÜOĞLU
(TEZ DANIŞMANI)
PROF. DR. FATMA BURCU SAVAŞ KUTSAL
PROF. DR. ARZU ARSLAN ERTÜRK

İSTANBUL, 2025

AKADEMİK DÜRÜSTLÜK BEYANI

Bu çalışmada yer alan tüm bilgilerin akademik kurallara ve etik ilkelere uygun olarak toplanıp sunulduğunu, söz konusu kurallar ve ilkelerin zorunlu kıldığı çerçevede, çalışmada özgün olmayan tüm bilgi ve belgelere, alıntılama standartlarına uygun olarak referans verilmiş olduğunu beyan ederim.

Ad Soyadı: Abdülmecit Güldağı
İmza:

ÖZ

TELE ÇALIŞMADA İZLEME VE GÖZETLEME ARAÇLARININ KİŞİSEL VERİLERİN KORUNMASI BAĞLAMINDA DEĞERLENDİRİLMESİ

Güldağı, Abdülmecit
Özel Hukuk Yüksek Lisans Programı
Öğrenci Numarası: 224055005
Open Researcher and Contributor ID (ORC-ID): 0000-0001-8013-6693
Ulusal Tez Merkezi Referans Numarası: 10729531

Tez Danışmanı: Prof. Dr. Yeliz Bozkurt Gümrükçüoğlu
Temmuz 2025, 322 Sayfa

Bu tezde, tele çalışma ilişkilerinde kullanılan izleme ve gözetleme araçları, kişisel verilerin korunması hukuku bağlamında incelenmektedir. Dijitalleşmenin hız kazanmasıyla birlikte yaygınlaşan tele çalışma uygulamaları, çalışma ilişkilerinde önemli değişimlere yol açmış; bu durum, işverenlerin yönetim hakkı ile çalışanların kişisel verilerinin korunması arasındaki dengenin kurulmasını hukuki ve teknik açılardan karmaşıklaştırmıştır. Bu doğrultuda çalışmanın ilk bölümünde, tele çalışmanın tarihsel gelişimi, tanımı ve hukuki çerçevesi, uluslararası düzenlemeler ile Avrupa Birliği ve Türk hukuku karşılaştırmalı olarak ele alınmıştır. İkinci bölümde, tele çalışma süreçlerinde kullanılan fiziksel, elektronik, biyometrik ve yapay zekâ tabanlı izleme yöntemleri sistematik olarak değerlendirilmiştir. Üçüncü bölümde ise elde edilen kişisel verilerin işlenmesinin hukuki sonuçları, hukuka uygunluk şartları, veri sorumlularının yükümlülükleri ve çalışanların hakları ayrıntılı biçimde açıklanarak, veri güvenliğine ilişkin teknik ve idari tedbirler sunulmuştur. Çalışma, disiplinler arası bir yaklaşımla, işverenlerin yönetimsel menfaatleri ile çalışanların özel hayat ve kişisel veri koruma hakları arasında ölçülü ve dengeli bir hukuki çerçeve oluşturmayı hedeflemektedir.

Anahtar Kelimeler: İzleme ve Gözetleme, Kişisel Verilerin Korunması, Tele Çalışma.

ABSTRACT

A LEGAL EVALUATION OF MONITORING AND SURVEILLANCE TOOLS IN TELEWORK FROM THE PERSPECTIVE OF PERSONAL DATA PROTECTION

Güldağı, Abdülmecit
MA in Private Law Program
Student ID: 224055005
Open Researcher and Contributor ID (ORC-ID): 0000-0001-8013-6693
National Thesis Center Referance Number: 10729531

Thesis Supervisor: Prof. Yeliz Bozkurt Gümrükçüoğlu
July 2025, 322 Pages

This thesis examines the monitoring and surveillance tools used in teleworking relationships within the framework of personal data protection law. With the acceleration of digitalization, the widespread adoption of telework has led to significant transformations in employment relations, rendering the balance between employers' managerial authority and employees' personal data protection rights increasingly complex from both legal and technical perspectives. In this context, the first part of the study analyzes the historical development, definition, and legal framework of telework through a comparative evaluation of international, European Union, and Turkish regulations. The second part systematically examines physical, electronic, biometric, and AI-based monitoring methods employed in teleworking environments. The third part evaluates the legal consequences of personal data processing, the conditions of lawfulness, the obligations of data controllers, the rights of data subjects, and the necessary technical and administrative security measures. Adopting an interdisciplinary approach, the study aims to establish a comprehensive legal framework that ensures a proportionate and balanced reconciliation between employers' managerial interests and employees' privacy and data protection rights.

Keywords: Monitoring and Surveillance, Personal Data Protection, Telework.

İÇİNDEKİLER

SEMBOLLER VE KISALTMALAR LİSTESİ

AB	Avrupa Birliği
ADM	Automated Decision-Making (Otomatik Karar Alma)
AI	Artificial Intelligence (Yapay Zekâ)
AI ACT	European Union Artificial Intelligence Act (Avrupa Birliği Yapay Zekâ Tüzüğü)
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
BAG	Bundesarbeitsgericht (Alman Federal İş Mahkemesi)
BCI	Brain-Computer Interface (Beyin-Bilgisayar Arayüzü)
BDSG	Bundesdatenschutzgesetz (Alman Federal Veri Koruma Kanunu)
BetrVG	Betriebsverfassungsgesetz (Alman İşyeri Teşkilat Yasası)
BIPA	Biometric Information Privacy Act (Biyometrik Bilgi Gizliliği Kanunu)
BM	Birleşmiş Milletler
BYOD	Bring Your Own Device (Kendi Cihazını Getir)
CCPA	California Consumer Privacy Act (California Tüketici Gizliliği Kanunu)
CCTV	Closed-Circuit Television (Kapalı Devre Televizyon)
CNIL	Commission Nationale de l'Informatique et des Libertés (Fransız Veri Koruma Otoritesi)
CNPD	Comissão Nacional de Proteção de Dados (Portekiz Kişisel Verileri Koruma Kurumu)
COVID-19	Coronavirus Disease 2019 (Koronavirüs Hastalığı 2019)
CPRA	California Privacy Rights Act (California Gizlilik Hakları Kanunu)
CSE	Comité Social et Économique (Sosyal ve Ekonomik Komite)
CSL	Cybersecurity Law (Siber Güvenlik Kanunu)
ÇSGB	Çalışma ve Sosyal Güvenlik Bakanlığı
DLP	Data Loss Prevention (Veri Kaybı Önleme)
DPA	Data Processing Agreement (Veri İşleme Sözleşmesi)
DPIA	Data Protection Impact Assessment (Veri Koruma Etki Değerlendirmesi)
DPO	Data Protection Officer (Veri Koruma Görevlisi)

DSL	Data Security Law (Veri Güvenliği Kanunu)
DVR	Digital Video Recorder (Dijital Video Kaydedici)
ECPA	Electronic Communications Privacy Act (Elektronik İletişim Gizliliği Yasası)
EDPB	European Data Protection Board (Avrupa Veri Koruma Kurulu)
GDPR	General Data Protection Regulation (Genel Veri Koruma Tüzüğü)
GPS	Global Positioning System (Küresel Konumlama Sistemi)
GSM	Global System for Mobile Communications (Mobil İletişim için Küresel Sistem)
HDPA	Hellenic Data Protection Authority (Yunan Kişisel Verileri Koruma Kurumu)
HITL	Human-in-the-loop (Döngü İçinde İnsan)
HOTL	Human-on-the-loop (Döngü Üzerinde İnsan)
ICO	Information Commissioner's Office (Bilgi Komiserliği Ofisi)
ILO	International Labour Organization (Uluslararası Çalışma Örgütü)
IoB	Internet of Bodies (Nesnelerin İnterneti - biyometrik sistemler bağlamında)
IOT	Internet of Things (Nesnelerin İnterneti)
IPA	Investigatory Powers Act (Soruşturma Yetkileri Kanunu)
IVR	Intelligent Video Recorder (Akıllı Video Kaydedici)
İşK	4857 Sayılı İş Kanunu
KEP	Kayıtlı Elektronik Posta
KVKK	6698 Sayılı Kişisel Verilerin Korunması Kanunu
MDM	Mobile Device Management (Mobil Cihaz Yönetimi)
MFA	Multi-Factor Authentication (Çok Faktörlü Kimlik Doğrulama)
NGFW	Next-Generation Firewall (Yeni Nesil Güvenlik Duvarı)
NLP	Natural Language Processing (Doğal Dil İşleme)
NVR	Network Video Recorder (Ağ Video Kaydedici)
PECR	Privacy and Electronic Communications Regulations (Mahremiyet ve Elektronik Haberleşme Düzenlemeleri)
RBAC	Role-Based Access Control (Rol Tabanlı Erişim Kontrolü)
RFID	Radio-Frequency Identification (Radyo Frekansı ile Tanımlama)

RIPA	The Regulation of Investigatory Powers Act (Soruşturma Yetkilerinin Düzenlenmesi Kanunu)
SGK	Sosyal Güvenlik Kurumu
TBK	6098 Sayılı Türk Borçlar Kanunu
TCK	Türk Ceza Kanunu
TMK	Türk Medeni Kanunu
UMTS	Universal Mobile Telecommunications System (Evrensel Mobil Telekomünikasyon Sistemi)
UTM	Unified Threat Management (Birleşik Tehdit Yönetimi)
VDI	Virtual Desktop Infrastructure (Sanal Masaüstü Altyapısı)
VERBİS	Veri Sorumluları Sicili
VPN	Virtual Private Network (Sanal Özel Ağ)
Wi-Fi	Wireless Fidelity (Kablosuz Bağlantı)

BÖLÜM I

GİRİŞ

Dijitalleşme süreci, son yıllarda kazandığı ivmeyle çalışma yaşamının paradigmalarını köklü bir biçimde dönüştürmüştür. Bilgi ve iletişim teknolojilerindeki gelişmeler ile COVID-19 pandemisinin küresel ölçekteki hızlandırıcı etkisi, işin fiziksel olarak işyeri sınırları dışına taşındığı tele çalışma modelini birçok sektör için yaygın ve kalıcı bir uygulama hâline getirmiştir. Bu dönüşüm, iş süreçlerinde esneklik ve verimlilik gibi önemli avantajlar sağlarken, çalışma ilişkilerinin mekânsal ve zamansal sınırlarını ortadan kaldırarak işverenin yönetim hakkı ile çalışanların temel hak ve özgürlükleri arasında yeni ve karmaşık hukuki tartışmalar doğurmuştur.

Tele çalışmanın doğası gereği uzaktan gerçekleştirilen iş görme edimlerinin denetlenmesi ihtiyacı, bu kapsamda kullanılan teknolojik izleme ve gözetleme araçlarının hukuki boyutunu ön plana çıkarmıştır. İşverenin yönetim hakkını etkili şekilde sürdürebilmesi, giderek daha fazla dijital araca dayalı denetim mekanizmalarının geliştirilmesini ve bu uygulamaların hukuka uygunluk çerçevesinde değerlendirilmesini zorunlu kılmaktadır. Bu yeni çalışma düzeninin merkezinde, işverenin iş süreçlerini yönetme ve verimliliği denetleme ihtiyacı ile çalışanın Anayasa ve uluslararası sözleşmelerle güvence altına alınmış özel hayatının gizliliği ve kişisel verilerinin korunması hakkı arasındaki hassas denge yer almaktadır.

Küresel ölçekte yaygınlaşan ve Avrupa Birliği gibi otoriteler tarafından dahi "aşırı" ve "müdahaleci" olarak değerlendirilen otomatik yüz tanıma, iletişim içeriklerinin taranması, konum takibi ve hatta tele çalışanların klavye hareketlerinin ve ekran etkinliklerinin izlenmesi gibi gelişmiş izleme teknikleri, çalışma yaşamında yeni ve karmaşık bir dönem başlatmıştır[1]. Bu teknolojiler, yalnızca toplanan veri hacmini

[1] Chris Jay Hoofnagle vd., "The European Union General Data Protection Regulation: What It Is and What It Means", Information & Communications Technology Law 28, sy 1 (2019): 469; Kirstie Ball,

katlanarak artırmakla kalmamış, aynı zamanda bu verileri işleyerek bireyler hakkında otomatik kararlar alınmasına olanak tanıyan analitik kapasiteyi de geliştirmiştir. Bu durum, çalışanların hassas niteliklerine dayalı örtük veya açık ayrımcılık riskini doğururken, diğer yandan işverenlerin bu uygulamaları verimlilik gerekçesiyle meşrulaştırmasına zemin hazırlamaktadır.

Bu bağlamda tezin temel amacı; tele çalışma ilişkilerinde kullanılan izleme ve gözetleme araçlarını, kişisel verilerin korunması hukuku çerçevesinde disiplinler arası bir yaklaşımla analiz etmek ve işverenlerin menfaatleri ile çalışanların özel hayat ve kişisel verilerini koruma hakları arasında ölçülü ve dengeli bir hukuki çerçevenin nasıl oluşturulabileceğini ortaya koymaktır. Bu amaç doğrultusunda çalışma, yalnızca Türk Hukuku ile sınırlı kalmayacak; Uluslararası Çalışma Örgütü (International Labour Organization - ILO), Avrupa Birliği (AB) düzenlemeleri ile Almanya, Fransa, Amerika Birleşik Devletleri ve Birleşik Krallık gibi mukayeseli hukuk örneklerindeki düzenleme ve uygulamaları da inceleyerek bütüncül bir perspektif sunacaktır.

Bu hedefe ulaşmak amacıyla tez, temel olarak üç ana bölüm üzerine kurgulanmıştır:

Birinci bölümde, öncelikle uzaktan çalışma ve tele çalışma kavramları; tarihsel gelişimleri, tanımları, unsurları ve hukuki çerçeveleriyle ele alınacaktır. Bu kapsamda, Uluslararası Çalışma Örgütü ve Avrupa Birliği düzenlemeleri ışığında tele çalışmaya ilişkin uluslararası standartlar incelenecek ve Türk Hukuku'ndaki düzenlemeler ile tarafların hak ve yükümlülükleri detaylı bir şekilde ele alınacaktır.

İkinci bölümde, tele çalışma süreçlerinde kullanılan izleme ve gözetleme yöntemleri sistematik bir şekilde sınıflandırılacaktır. Bu kapsamda, fiziksel, elektronik, biyometrik ve yapay zekâ tabanlı izleme yöntemleri, teknik ve işlevsel yönleriyle ve kullanım amaçları bakımından analiz edilecektir. Ayrıca bölümde, iş ilişkileri kapsamında kullanılan izleme uygulamalarına ilişkin uluslararası ve mukayeseli hukuk sistemlerindeki normatif çerçeve ile Türk Hukuku'ndaki düzenlemelere yer verilecektir.

"Surveillance in the Workplace: Past, Present, and Future", Surveillance & Society 4, sy 20 (2022): 458-59.

Üçüncü ve son bölümde ise izleme ve gözetleme araçlarıyla elde edilen kişisel verilerin işlenmesinin hukuki sonuçları, 6698 sayılı Kişisel Verilerin Korunması Kanunu çerçevesinde değerlendirilecektir. Bu bölümde veri işleme faaliyetlerinin hukuka uygunluk şartları, veri sorumlusu olan işverenin yükümlülükleri, veri sahibi olan çalışanların hakları ve veri güvenliğinin sağlanması için alınması gereken teknik ve idari tedbirler ayrıntılı bir biçimde açıklanarak somut çözüm önerileri sunulacaktır.

Tüm bu bölümler çerçevesinde bu tez, tele çalışma uygulamalarında işverenin yönetim hakkı ile işçinin kişisel verilerini koruma hakkı arasındaki dengeyi sağlayacak hukuki mekanizmalar önermeyi hedeflemektedir. Disiplinler arası bir bakış açısıyla, tele çalışmadaki izleme ve gözetleme pratiklerini kişisel verileri koruma hukuku perspektifinden değerlendiren bu çalışma, yalnızca öğretiye katkı sağlamayı değil, aynı zamanda uygulamada karşılaşılan hukuki sorunlara etkili ve uygulanabilir çözümler sunmayı amaçlamaktadır.

BÖLÜM II

GENEL OLARAK UZAKTAN ÇALIŞMA VE TELE ÇALIŞMA

2.1. Uzaktan Çalışma

Günümüzde gittikçe yaygınlık kazanan uzaktan çalışma uygulamaları, işveren ve çalışan açısından çalışma yeri ve süreleri bakımından önemli ölçüde esneklik sağlamakla birlikte, klasik iş ilişkisinden ayrılan ve atipik çalışma ilişkileri kategorisinde değerlendirilen özgün hukuki ve teknik sorunları da gündeme getirmektedir. Uzaktan çalışma, İş Kanunu'nun 14. maddesinin 4. fıkrası kapsamında *"işçinin, işveren tarafından oluşturulan iş organizasyonu kapsamında iş görme edimini evinde ya da teknolojik iletişim araçları ile işyeri dışında yerine getirmesi esasına dayalı ve yazılı olarak kurulan iş ilişkisi"* şeklinde tanımlanmaktadır. Bu kavram, öğretide ve mevzuatta "evde çalışma" ve "tele çalışma" alt türlerini kapsayan bir üst başlık şeklinde ele alınmaktadır[2]. Her ne kadar çalışma konumuz tele çalışma

[2] Sarper Süzek ve Süleyman Başterzi, *İş Hukuku*, 24. bs (Beta, 2024), 284 vd.; Nuri Çelik vd., *İş Hukuku Dersleri*, 36. bs (Beta, 2023), 226 vd.; Hamdi Mollamahmutoğlu vd., *İş Hukuku*, Güncellenmiş 7 (Lykeion, 2022), 142-43; Emine Tuncay Senyen Kaplan, *Bireysel İş Hukuku*, 2. (Yetkin Yayınevi, 2023), 158; Ercan Akyiğit, *İş Hukuku*, 15. bs (Seçkin, 2024), 171-74; Halûk Hâdi Sümer, *İş Hukuku*, Güncellenmiş 27. (Seçkin Yayıncılık, 2024), 50 vd.; Ufuk Aydın, *Bireysel İş Hukuku*, 7. bs (Nisan Kitabevi, 2023), 125 vd.; Mustafa Alp, "Tele Çalışma (Uzaktan Çalışma)", içinde *Sarper SÜZEK'e Armağan* (İstanbul, 2011), 1:795 vd.; Yeliz Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office Uygulamasına İlişkin Türk ve Alman Hukuku'nda Mukayeseli Bir Değerlendirme", *Koronavirüs Döneminde Güncel Hukuki Meseleler Sempozyumu: Bildiri Tam Metin Kitabı 29-30 Mayıs 2020*, İbn Haldun Üniversitesi Yayınları, 2020, 145 vd.; Yeliz Bozkurt Gümrükçüoğlu ve F. Burcu Savaş Kutsal, "Uzaktan Çalışma", içinde *Zorlayıcı Sebeplerin İş İlişkisine Etkisi*, ed. Saim Ocak (Adalet Yayınevi, 2023), 51 vd.; Orhan Ersun Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", *Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi*, sy 26 (2010): 525 vd.; Dilek Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", *Sicil İş Hukuku Dergisi* 36 (2016): 148 vd.; Mustafa Alp, "Corona Günlerinde Uzaktan (Evden) Çalışma, Telafi Çalışması ve Ücret İndirimi", içinde *Pandemi Sürecinde İş Hukuku*, ed. Gülsevil Alpagut (On İki Levha Yayıncılık, 2020), 103-8; Erdem Özdemir, "Uzaktan Çalışma Yönetmeliği Karşısında Tele Çalışma", *Çimento İşveren Dergisi* 35, sy 3 (2021): 8-41; Merve Kutlu ve Ali Uçar, "Tarafların Hak ve Borçları Kapsamında Koronavirüs Pandemisinde Uzaktan Çalışma", içinde *İş Hukukunda Yeni Yaklaşımlar V.*, ed. Kübra Doğan Yenisey ve Seda Ergüneş Emrağ (On İki Levha Yayıncılık, 2022), 253 vd.; Beyza Öztürk İnal, *Uzaktan Çalışma* (Platon Hukuk, 2022); Gonca Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma" (Doktora Tezi, Ankara Üniversitesi, 2014).

ile sınırlı olsa da konunun anlaşılabilmesi için uzaktan çalışma kavramı üzerinde durulacak ve bu çalışma biçimini diğer çalışma türlerinden ayıran özellikleri açıklanacaktır. Ardından evde çalışma ile bu çalışma biçimine uygulanacak hükümler değerlendirilecektir. Evde çalışma, tele çalışma ile ilişkisi ölçüsünde sınırlı olarak incelenecek olup konumuzu teşkil eden tele çalışma ise daha kapsamlı incelenecektir. Bu çerçevede tele çalışmanın tarihsel gelişimi, iş ilişkilerine etkileri, tanımı, unsurları, türleri ve tele çalışmaya ilişkin hukuki düzenlemeler ele alınacaktır.

2.1.1. Tarihi Gelişimi ve Yaygınlaşması

Tarım toplumlarında bireyler, temel ihtiyaçlarını karşılamak ve gelir elde etmek amacıyla üretim faaliyetlerini genellikle ev ortamında, günümüzdeki karşılığıyla uzaktan çalışma biçiminde gerçekleştirmişlerdir. Ancak Sanayi Devrimi'nin ardından üretimin fabrikalara taşınması, bu çalışma yönteminin yaygınlığını önemli ölçüde azaltmıştır. Bununla birlikte, uzaktan çalışma modeli tamamen ortadan kalkmamıştır. Zamanla yaşanan gelişmelerle içeriği yenilenen bu model, teknolojik ilerlemeler ve bilhassa COVID-19 pandemisinin hızlandırıcı etkisiyle tekrar önem kazanmış ve yaygınlığı artmıştır[3]. Nitekim, bilgi ve işlem teknolojilerinin gelişmesiyle birlikte uzaktan çalışma oranı giderek artış göstermekte ve bu model birçok sektörde daha da yaygınlaşmaktadır[4].

Bununla birlikte, tele çalışma uygulamalarına yönelik güncel yönelim, tek yönlü bir gelişimden ziyade, iki karşıt dinamiğin etkileşimiyle şekillenen bir sürece işaret

---

[3] A. Can Tuncay, "Pandemi Gölgesinde Evden Çalışma", *Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi* 18, sy 72 (2021): 23-52; Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 145 vd.; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 2; Öztürk İnal, *Uzaktan Çalışma*, 1; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 527; Kutlu ve Uçar, "Tarafların Hak ve Borçları Kapsamında Koronavirüs Pandemisinde Uzaktan Çalışma", 253 vd.; Levent Akın, "Türk Çalışma Yaşamında Pandemi Sürecinde Uzaktan/Evden Çalışma ve Olası Sonuçları", *Otto Kaufmann Armağanı (Ed. Hekimler, A.)*, 2021, 261-300.

[4] Küresel çapta yapılan bir araştırmada pandemi sonrasında çalışanların %19'unun tamamen, %29'unun ise kısmen uzaktan çalışma düzenine geçtiğini göstermektedir. Pandemi öncesinde bu oranlar sırasıyla %10 ve %20 olarak kaydedilmiş olup, uzaktan çalışma yöntemini kullanan toplam çalışan oranı %30'dan %48'e yükselmiştir. Bu araştırma, Gartner COVID-19 Crisis Benchmarking Against Your Peers Webinar Poll (421 İK lideri, 2 Nisan 2020), 2020 Gartner Cost Cutting and Employee Experience Survey (4,535 çalışan) ve COVID-19: How Finance Leaders Are Responding to the Emerging Situation Webinar Poll (317 finans lideri, 26 Mart 2020) olmak üzere üç anketten yararlanılarak oluşturulmuştur. Andrea Granieri, *How the Remote Work Revolution Will Change the Employer- Employee Relationship*, 2020.

etmektedir. Bir yanda çalışanlar, esnek çalışma koşullarını kalıcı bir beklenti hâline getirmişken; diğer yanda, işverenlerin, çalışanların fiziksel olarak ofise dönmesine yönelik eğilimi güçlendirmektedir. Bu çift yönlü gerilim, genel gidişatın "hibrit" modele doğru evrildiğini ortaya koymaktadır[5].

2.1.2. Uzaktan Çalışma Tanımı, Unsurları ve Geleneksel Çalışma Biçimlerinden Ayrılan Yönleri

Uzaktan çalışma modellerinin yaygınlaşması, işçi-işveren ilişkilerinde yeni hukuki sorunların ve düzenleme ihtiyacının ortaya çıkmasına neden olmuştur. İş hukukunun temel kavramlarından olan işin yapılacağı yer ve işyeri, teknolojideki gelişmelerle birlikte geleneksel tanımlarının dışına çıkarak daha esnek ve dinamik bir niteliğe kavuşmuştur[6]. Uzaktan çalışma modelinde karşılaşılabilecek hukuki sorunlar, kapsamlı hukuki düzenlemeleri zorunlu kılmaktadır. Bu konular arasında çalışma sürelerinin tespiti ve denetimi, iş sağlığı ve güvenliği önlemlerinin etkin bir şekilde

---

[5] Günümüz çalışma düzeni, çalışanların kalıcı hale gelen esneklik talebi ile yönetimin artan ofise dönüş baskısı arasında belirginleşen bir gerilimle şekillenmektedir. Yapılan araştırmalar, uzaktan çalışmaya uygun ABD'li çalışanların %51'inin hibrit bir düzende çalıştığını ve %60'ının bu modeli tercih ettiğini ortaya koyarken, pandemi öncesi döneme kıyasla dünya genelinde uzaktan çalışılan gün sayısının haftada ortalama 0,3'ten 1,3'e yükselmesi bu esneklik beklentisinin yerleşik hale geldiğini teyit etmektedir. Buna karşılık, küresel CEO'ların %83'ünün önümüzdeki üç yıl içinde ofise tam zamanlı dönüş beklemesi ve bu oranın bir önceki yıl %64 seviyesinde olması, yönetici kanadındaki beklentilerin keskin bir artış içinde olduğunu göstermektedir; nitekim şirketlerin %90'ının 2024 yılı sonuna kadar ofise dönüş politikalarını uygulamayı planladığı rapor edilmektedir. Çalışan beklentileri ile yönetim baskısı arasındaki bu çatışma, çalışanların haftanın belirli günlerinde ofiste bulunmasını zorunlu kılan yapılandırılmış hibrit modelin yaygınlaşmasına zemin hazırlamıştır; öyle ki, ABD'de bu tür programlara sahip şirketlerin oranı %43'e ulaşarak 2023 yılı başındaki seviyesinin iki katını aşmıştır. Bknz. Gallup Inc, "Indicator: Hybrid Work", Gallup.Com, erişim 17 Eylül 2025, https://www.gallup.com/401384/indicator-hybrid-work.aspx; Cem Avcıoğlu, "Uzaktan Çalışmaya Dair Veriler Dönüşümün Kalıcılığına İşaret Ediyor", TSKB, 29 Ağustos 2025, https://www.tskb.com.tr/blog/genel/uzaktan-calismaya-dair-veriler-donusumun-kaliciligina-isaret-ediyor; "KPMG 2024 CEO Outlook - KPMG Turkey", KPMG, 02 Aralık 2024, https://kpmg.com/tr/en/home/insights/2024/12/2024-ceo-outlook.html; "Uzaktan Çalışma Öldi mü? İmdi Yürek Yırtılır", erişim 17 Eylül 2025, https://incturkiye.com/makaleler/uzaktan-calisma-oldi-mu-imdi-yurek-yirtilir?uuid=sAUPWH3Gp.

[6] Kübra Doğan Yenisey, "Üretimin Değişen Yapısının 'İşyeri' Kavramına Etkisi," içinde Ekonomik ve Teknolojik Gelişmelerin İş Hukuku ve Sosyal Güvenlik Hukukuna Etkileri, Prof. Dr. Münir Ekonomi 85. Doğum Günü Armağanı (Oniki Levha Yayıncılık, 2021), 161 vd.; Gülsevil Alpagut, "Dijitalleşen Çalışma Yaşamında İş Sözleşmesinin Unsurları", içinde Ekonomik ve Teknolojik Gelişmelerin İş Hukuku ve Sosyal Güvenlik Hukukuna Etkileri, Prof. Dr. Münir Ekonomi 85. Doğum Günü Armağanı (On İki Levha Yayıncılık, 2021), 100 vd.; Nurşen Caniklioğlu ve Melis Kutlu, "Tele Çalışmada İşyeri Kavramı", İstanbul Aydın Üniversitesi Hukuk Fakültesi Dergisi 10, sy 2 (2024): 119 vd.

uygulanması ve iş görme ediminde kullanılan araç-gereçlerin maliyet ile diğer masrafların paylaşımı yer almaktadır[7].

Uzaktan çalışma kavramının açık bir biçimde tanımlanması ve hukuki çerçevesinin netleştirilmesi, söz konusu çalışma modelinin uygulanabilirliği ve sürdürülebilirliği açısından kritik öneme sahiptir[8]. Uzaktan çalışma kavramının netleştirilmesi ihtiyacı, özellikle farklı ülkelerde kullanılan terimlerin çeşitliliği nedeniyle uluslararası bir boyut kazanmaktadır. Ülkeler arasında benzer anlamlara gelen terimlerin eş zamanlı veya birbirinin yerine kullanılması kavramsal belirsizliği derinleştirmektedir[9]. Nitekim uluslararası öğretide "work at distance", "remote work" ve "home office" gibi genel ifadelerin yanı sıra, "telework", "work at home" ve "home-based work" gibi daha spesifik alt kategoriler de dikkat çekmektedir[10]. Bu çalışma kapsamında zaman zaman tele çalışmayı da içine alan bir üst kavram olması nedeniyle uzaktan çalışma terimi tercih edilmiştir.

Terimlerin farklı şekillerde veya birbirinin yerine kullanılması, karşılaştırmalı hukuk alanında kavramların tanımlanması açısından farklı yaklaşımların ortaya çıkmasına neden olmaktadır. Örneğin Uluslararası Çalışma Örgütü, uzaktan çalışmayı, *"işin tamamının veya bir kısmının olağan çalışma yerinden farklı bir alternatif mekânda yerine getirilmesi durumu"* olarak tanımlamaktadır. ILO'ya göre uzaktan çalışma, çalışanın mesleki niteliği ve istihdam durumuna göre belirlenen, genellikle işin yapılmasının beklendiği yerin dışında kalan çeşitli mekânlarda gerçekleştirilebilmektedir[11]. Mukayeseli hukuk kapsamında ele alınacak olursa,

---

[7] 4857 sayılı İş Kanunu'nun 14. maddesinde 2016 yılında 6715 sayılı Kanun ile yapılan düzenlemeden önceki dönem için ortaya çıkan ihtiyaca ilişkin bknz. Murat Kandemir, İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma (Legal Kitapevi, 2011), 106; Müjdat Şakar ve Duygu Erkan Şahin, "Esnek Çalışma Modellerinden Uzaktan Çalışma ve Uzaktan Çalışanların Sigortalılığı", SGD-Sosyal Güvenlik Dergisi 11, sy 2 (2021): 249-67.

[8] Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 527-28.

[9] "Covid-19: Guidance for Labour Statistics Data Collection", International Labour Office, 05 Haziran 2020, 3, https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@dgreports/@stat/documents/publication/wcms_747075.pdf.

[10] Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 155; Luca Ratti ve Antonio García-Muñoz, "The Regulation of Remote Work. Seeking Balance Through the Articulation of Labour Law Sources: A Comparative Appraisal", *International Journal of Comparative Labour Law and Industrial Relations* 40, sy Issue 3 (2024): 304.

[11] ILO, "Defining and Measuring Remote Work, Telework, Work at Home and Home-Based Work", içinde *ILO Technical Note* (International Labour Office, 2020), 5,

Alman Hukukunda da fiziksel olarak işyeri dışında gerçekleştirilen çalışmalara yönelik terim birliği henüz sağlanamamış durumdadır. Evde çalışma ve tele çalışma kavramları sıklıkla kullanılsa da tele çalışmanın kapsamının daha ayrıntılı bir biçimde ele alınması ve çalışmanın gerçekleştirildiği mekânlara göre alt kategorilere ayrılması gerektiği ileri sürülmektedir[12]. Fransız hukukunda ise Fransız İş Kanunu'nda herhangi bir ayrım yapılmaksızın ilgili hükümler doğrudan tele çalışma (télétravail) başlığı altında düzenlenmiştir[13].

Türk hukukunda uzaktan çalışmaya ilişkin ilk yasal tanım, yukarıda belirtildiği üzere 2016 yılında 4857 sayılı İş Kanunu'nun 14. maddesinde yapılmıştır[14]. Böylece uzaktan çalışma kavramı, esas olarak iki temel unsur üzerine inşa edilmiştir. Bunlardan ilki, işin işveren tarafından belirlenen iş organizasyonu çerçevesinde yürütülmesidir. Bu unsur, uzaktan çalışan işçinin işverenin yönetim, denetim ve organizasyon yetkisi altında faaliyet göstermeye devam ettiğini ve işverenle arasındaki bağı koruduğunu ifade etmektedir. Diğer temel unsur ise işin fiziksel olarak işyeri dışında yerine getirilmesidir. Buna göre uzaktan çalışma ilişkisinde işçinin faaliyetlerini evinde ya da işyeri olarak belirlenen mekânın dışında kalan başka bir alanda gerçekleştirmesi gerekmektedir[15].

Kanun koyucu, bağımlılık unsurunu düzenlerken, işin işverenin organizasyonu dâhilinde yürütülmesi şartını getirerek, iş ilişkisini diğer sözleşme türlerinden ayıran bağımlılık unsurunu vurgulamaktadır[16]. Ancak, işin fiziksel olarak işyeri dışında ifa

---

https://www.ilo.org/publications/defining-and-measuring-remote-work-telework-work-home-and-home-based-work.

[12] Alman Hukukunda kullanılan terimlere ilişkin ayrıntılı bilgi için bknz. Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 155-56.

[13] "Article L1222-9 - Code du travail - Légifrance", erişim 10 Mart 2025, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047864720; Tolga Bal, "Addressing Remote Work Challenges in Türkiye: A New Paradigm for Workplace Safety", *Sosyal Güvenlik Dergisi* 14, sy 2 (2025): 189, https://doi.org/10.32331/sgd.1699858.

[14] Hukukumuzda ise 2016 öncesi uzaktan çalışma öğretide "Uzaktan çalışma (remote work), gezici satış temsilcileri, tele çalışanlar, evde çalışanlar gibi çeşitli isçi gruplarını içeren, diğer bir deyişle klasik anlamda işyerine bağlı olmaksızın işin üstlenilebildiği çalışma şekli" olarak tanımlanmıştır. Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 527.

[15] Çelik vd., *İş Hukuku Dersleri*, 226; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 150; Öztürk İnal, *Uzaktan Çalışma*, 23-28; Serenay Kara, *Uzaktan Çalışmada İş Sağlığı ve Güvenliğinin Hukuki Boyutu* (Seçkin Yayıncılık, 2022), 29; Can Şanlı, "İş Hukukunda Uzaktan Çalışma" (Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, 2023), 9-10.

[16] Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 33; Canan Ünal Adınır, "Tele çalışmada verilerin korunması", içinde *Muhtelif Yönleriyle Kişisel Verilerin Korunması Hukuk*, ed. Kemal Şenocak

edilmesi, klasik iş ilişkilerinde merkezi bir rol oynayan bağımlılık unsurunun geleneksel yöntemlerle değerlendirilmesini zorlaştırmaktadır[17]. Bu nedenle uzaktan çalışma ilişkilerinde bağımlılık, klasik iş ilişkilerine kıyasla daha karmaşık, kritik ve belirleyici bir nitelik kazanır[18]. Geleneksel iş ilişkilerinde bağımlılık unsuru, işçinin belirli bir işyerinde, belirli çalışma süreleri içerisinde ve işverenin emir ve talimatlarına tabi olarak faaliyet göstermesiyle açık biçimde ortaya konulmaktadır[19]. Atipik çalışma modellerinde ise durum farklıdır. İşin gerçekleştirildiği yer, çalışma süreleri ve işverenin talimat yetkisi gibi temel unsurlar değişkenlik göstermektedir. Bu nedenle, bağımlılık unsuru geleneksel iş ilişkilerine kıyasla farklı kriterler ışığında değerlendirilmektedir[20]. Atipik çalışma modellerinde iş görenlerin işveren tarafından oluşturulan iş organizasyonuna entegrasyonu, bağımlılığın tespitinde merkezi bir rol oynamaktadır[21]. İş organizasyonu kavramının açıklanması ve geleneksel anlamda fiziksel olarak işyeri sınırları dışında gerçekleştirilen çalışmaların bu kavrama ne ölçüde dâhil olduğunun belirlenmesi, bağımlılığın tespitinde kritik bir rol oynamaktadır[22]. İş organizasyonu kavramı, İş Kanunu'nun 2. maddesinin 3. fıkrasında düzenlenmiş olup, işin işveren tarafından belirlenen koşullar çerçevesinde yürütülmesi anlamına gelmektedir[23]. Bu kapsamda uzaktan çalışma ilişkilerinde, işçinin işveren tarafından oluşturulan iş organizasyonuna bağlı hareket etmesi bağımlılık unsurunun açık bir göstergesidir[24]. İşverenin yönetim ve denetim yetkisini uzaktan kullanması ve

(Yetkin, 2022), 963; Karsu Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması" (Yüksek Lisans Tezi, Bursa Uludağ Üniversitesi, 2024), 24.

[17] Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 60; Şanlı, "İş Hukukunda Uzaktan Çalışma", 39-43.

[18] Süzek ve Başterzi, *İş Hukuku*, 240 vd.; Çelik vd., *İş Hukuku Dersleri*, 226 vd.; Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 42; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 533; Alp, "Tele Çalışma (Uzaktan Çalışma)", 804 vd.

[19] Süzek ve Başterzi, *İş Hukuku*, 284-86; Çelik vd., *İş Hukuku Dersleri*, 226; Mollamahmutoğlu vd., *İş Hukuku*, 466-67; Emine Tuncay Senyen Kaplan, *Bireysel İş Hukuku*, 2. bs (Yetkin, 2023), 161.

[20] Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 149.

[21] Çelik vd., *İş Hukuku Dersleri*, 226; Ali Güzel, "Fabrikadan İnternete İşçi Kavramı ve Özellikle Hizmet Sözleşmesinin Bağımlılık Unsuru Üzerine Bir Deneme", *Kamu İş, Prof. Dr. Kemal Oğuzman'a Armağan* 4, sy 2 (1997): 109-10; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi".

[22] Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 151.

[23] Alp, "Tele Çalışma (Uzaktan Çalışma)", 799; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 151.

[24] Tankut Centel, "Türk Borçlar Kanunu'nda Hizmet Sözleşmelerinin Tanımı ve Kurulması", *Tisk Akademi* 6, sy 12 (2011): 16-18; Sarper Süzek, *İş Hukuku*, Yenilenmiş 8.Baskı (Beta, 2012), 286; Ender Gülver, "Türk Borçlar Kanunu'nun Evde Hizmet Sözleşmesine İlişkin Hükümleri Üzerine", *Journal of Istanbul University Law Faculty* 72, sy 2 (2014): 106; Alp, "Tele Çalışma (Uzaktan Çalışma)", 813-15;

işçinin fiziksel olarak işyeri sınırlarında bulunmadan iş görmesi, işçinin bağımsız çalıştığı anlamına gelmeyecektir. Özellikle işverenin oluşturduğu iş organizasyonu kapsamında doğrudan ya da dolaylı biçimde yönetim ve denetim faaliyetleri yürütmesi, bağımlılığın varlığına işaret eden önemli göstergelerdendir[25].

Uzaktan çalışmanın ikinci temel unsuru ise mesafedir. Bu unsur, işin fiilen gerçekleştirildiği yer ile işverenin iş sonuçlarını beklediği veya değerlendirdiği yer arasındaki fiziksel ayrılığı ifade etmektedir[26]. Mesafe unsuru, işverenin işi doğrudan ve fiziksel olarak denetleyememesine neden olmakta ve uzaktan çalışmayı geleneksel çalışma biçimlerinden ayıran temel özelliklerden biri olarak karşımıza çıkmaktadır[27]. Bu nedenle, mesafe unsurunun getirdiği denetim zorlukları karşısında, bu çalışma biçiminin hukuki çerçevesini netleştirmek amacıyla ekipman temininden çalışma sürelerinin takibine kadar birçok alanda yeni düzenlemeler geliştirilmesi kritik önem taşımaktadır[28].

Uzaktan çalışma kapsamında işin ifa edildiği yer, klasik anlamdaki işyeri kavramının ötesine geçerek daha geniş biçimde yorumlanmaktadır. Bu bağlamda, işçinin çalışma faaliyetlerini sürdürebileceği her türlü fiziksel ortam, uzaktan çalışmanın mekânsal kapsamı içinde değerlendirilmektedir. Ayrıca, geleneksel tanımıyla fiziksel bir mekân olan işyeri kavramının, dijital ortamların yaygınlaşmasıyla fiziksel sınırlarını aşarak dijital ağlar üzerinden birbirine bağlı bilgisayar sistemlerinden oluşan sanal bir yapıya dönüştüğü belirtilmektedir[29]. Uzaktan çalışanların iş görme edimini ifa ettiği mekân ile diğer çalışanların iş görme edimini ifa ettiği mekân arasında terimsel bir ayrım yapılması ve bu doğrultuda "işyeri" kavramının yeniden tanımlanması gerekliliği ortaya çıkmaktadır. Uzaktan çalışma işverenin ofisi, fabrikası, inşaat sahası, çiftlik gibi işletmenin ekonomik faaliyetlerini yürüttüğü tesisler ya da müşterilere ait işyerleri ve

---

Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 158.

[25] Mollamahmutoğlu vd., *İş Hukuku*, 467; Sevil Doğan, *İş Sözleşmesinde Bağımlılık Unsuru* (Seçkin Yayıncılık, 2016), 73; Kara, *Uzaktan Çalışmada İş Sağlığı ve Güvenliğinin Hukuki Boyutu*, 27 vd.

[26] Süzek ve Başterzi, *İş Hukuku*, 284 vd.; Çelik vd., *İş Hukuku Dersleri*, 226 vd.; Mollamahmutoğlu vd., *İş Hukuku*, 465; Sümer, *İş Hukuku*, 50-54.

[27] Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 53-54; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 150.

[28] Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 9; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 150.

[29] Dilek Dulay, Türk İş Hukukunda Evde Çalışma (Turhan Kitabevi, 2016), 98.

işin doğası gereği kamuya açık alanlarda yürütülmesi zorunlu olan yerlerin dışında gerçekleştirilen çalışma biçimini ifade etmektedir. Bu noktada, işin doğası gereği müşteriye ait işyerlerinde ya da kamuya açık alanlarda gerçekleştirilen çalışmalar ile sabit bir işyerinin bulunmadığı aile işletmelerinde çalışan aile işçilerinin faaliyetlerinde mesafe unsurunun varlığından söz edilemez. Başka bir ifadeyle, işleri gereği sürekli olarak kamuya açık alanlarda bulunan sokak satıcıları veya otobüs şoförleri gibi çalışanlar kapsamında mesafe unsuru gerçekleşmediğinden uzaktan çalışma kapsamında değerlendirilmeyecektir[30].

2.1.3. Uzaktan Çalışmaya Uygulanacak Hükümler

Uzun yıllar boyunca iş hukukuna ilişkin normlarda uzaktan çalışma düzenlenmemiştir. Türk hukukunda uzaktan çalışmaya yönelik normatif düzenleme ihtiyacı son yıllarda giderek artmıştı. Özellikle pandemi döneminde evden çalışmanın yaygınlaşması, teknolojik ilerlemelerin hız kazanması ve küreselleşmenin iş yapma biçimlerini dönüştürmesi sonucunda uzaktan çalışmaya yönelik normatif düzenleme ihtiyacı belirginleştirmiştir[31]. Türk Borçlar Kanunu'nda "evde hizmet sözleşmesi" başlığı altında düzenlenen ve uzun süredir çalışma hayatında uygulama alanı bulan[32] evde çalışma sözleşmesinin hangi kanun kapsamında değerlendirileceği ise uzun yıllar boyunca tartışma konusu olmuştur[33]. Bu bağlamda, evde çalışma ve tele çalışma gibi uzaktan çalışmanın alt türlerinin açık ve kapsamlı bir normatif zemine oturtulması bir zorunluluk olarak ortaya çıkmıştır. Böyle bir düzenleme, uygulamadaki belirsizliklerin

---

[30] "Covid-19: Guidance for Labour Statistics Data Collection", 5.

[31] Banu Sarıbay, "Uzaktan Çalışma Üzerine Sosyolojik Bir Değerlendirme", *Sosyoloji Dergisi*, sy 46 (2023): 221; Ayşen Akbaş Tuna ve Zafer Türkmendağ, "Covid-19 Pandemi Döneminde Uzaktan Çalışma Uygulamaları ve Çalışma Motivasyonunu Etkileyen Faktörler", *İşletme Araştırmaları Dergisi* 12, sy 3 (2020): 3257.

[32] Çelik vd., *İş Hukuku Dersleri*, 226 vd.

[33] İş Kanunu'nda evde çalışmaya ilişkin özel bir düzenleme yapılmadan önce, öğretide ileri sürülen ve Yargıtay tarafından da benimsenen görüşe göre, kanun koyucunun, Türk Borçlar Kanunu'nda evde çalışmayı ayrıca ele almasının amacı, bu kişileri İş Kanunu'nun koruması dışına çıkarmak değildi. Aksine asıl amaç, bu çalışma modelinin kendine has yapısı için tamamlayıcı kurallar getirmekti. Bu yaklaşıma göre, evde çalışanlar için her iki kanunun da birlikte uygulanması hedefleniyordu. Sonuç olarak, evde çalışanlar hem İş Kanunu'nun sağladığı haklardan faydalanmalı hem de bu kanundaki sorumlulukları üstlenmeliydi. Bknz. Süzek, İş Hukuku, 286; Gülver, "Türk Borçlar Kanunu'nun Evde Hizmet Sözleşmesine İlişkin Hükümleri Üzerine", 121; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 157; O dönem için evde hizmet sözleşmesine TBK hükümlerinin uygulanacağına dair görüşler için bknz. Hamdi Mollamahmutoğlu ve Muhittin Astarlı, İş Hukuku, 5. (Turhan Kitabevi, 2012), 422-23; Alp, "Tele Çalışma (Uzaktan Çalışma)", 896.

giderilmesi ve tarafların hak ve yükümlülüklerinin netleştirilmesi açısından kritik öneme sahiptir[34].

Her iki çalışma biçiminin yasal olarak düzenlenmesine yönelik ihtiyaç doğrultusunda, 2016 yılında 6715 sayılı Kanun'un 2. maddesi ile İş Kanunu'nun 14. maddesinde değişikliğe gidilmiştir. Bu değişiklik kapsamında, maddede daha önce yer alan "çağrı üzerine çalışma" ifadesine ek olarak "uzaktan çalışma" kavramı getirilmiş, ayrıca uzaktan çalışma tanımlanarak bu çalışma türüne ilişkin temel esaslar belirlenmiştir[35]. Yapılan düzenleme ile evde çalışma ve tele çalışma, uzaktan çalışmanın alt türleri olarak mevzuatımızda açıkça düzenlenmiştir[36]. İlgili kanun değişikliğinin gerekçesinde, çalışma mevzuatının değişen ekonomik koşullara uyum sağlayacak dinamik bir yapıya kavuşturulması amacıyla evden çalışma ve tele çalışma türlerinin "uzaktan çalışma" çatısı altında birleştirildiği ifade edilmiştir.

İş Kanunu'nun 14. maddesinde yapılan düzenlemeyle birlikte, uzaktan çalışma ilişkilerinde Türk Borçlar Kanunu'nun mu yoksa İş Kanunu'nun mu uygulanacağı yönündeki tereddütler ortadan kalkmış; İş Kanunu'nun uygulanması esası benimsenmiştir. Bu düzenlemeyle uzaktan çalışma, çağrı üzerine çalışmayı düzenleyen 14. maddeye eklenen hükümlerle ele alınmıştır. Ancak, uzaktan çalışma ilişkilerinde büyük önem taşıyan ulaşılabilir olmama hakkına ilişkin bir düzenlemeye yer verilmemesi, öğretide eleştirilere neden olmuştur[37].

Söz konusu kanun değişikliğinin getirdiği bu temel çerçevenin ardından, uzaktan çalışmanın uygulamasına yönelik usul ve esasların belirlenmesi ihtiyacı doğmuştur. Bu doğrultuda, İş Kanunu'nun 14. maddesinin 7. fıkrasında uzaktan çalışmanın usul ve esaslarının; işin niteliği, hangi işlerde uzaktan çalışmanın yapılamayacağı, veri

---

[34] Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 3; Şanlı, "İş Hukukunda Uzaktan Çalışma", 3.
[35] Çelik vd., *İş Hukuku Dersleri*, 226 vd.; Senyen Kaplan, *Bireysel İş Hukuku*, 2. bs, 158; Özdemir, "Uzaktan Çalışma Yönetmeliği Karşısında Tele Çalışma", 11-13; Betül Erkanlı Başbüyük, "Uzaktan Çalışmanın Bir Türü Olarak Tele Çalışmada İşçinin Dinlenme Hakkı", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 29, sy 1 (2023): 661; Seda Ergüneş Emrağ, "4857 Sayılı İş Kanunun Değişik 14. Maddesi Işığında Tele Çalışma", *Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergis* 13, sy 51 (2016): 1415. Düzenlemenin geciktiğine dair eleştiriler için bkz. Tamer Soysal, "Tele Çalışma", *Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi* 1, sy 9 (2006): 158.
[36] Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 148; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 2.
[37] Ayrıntılar için bknz. Mollamahmutoğlu vd., *İş Hukuku*, 465-66; Senyen Kaplan, *Bireysel İş Hukuku*, 2. bs, 158.

koruma gibi hususları içerecek şekilde bir yönetmelikle belirlenmesini öngörmüştür[38]. Düzenleme doğrultusunda çıkarılan Uzaktan Çalışma Yönetmeliği ile uzaktan çalışmanın usul ve esasları belirlenmiş, uzaktan çalışma sözleşmelerinde yer alması gereken zorunlu hükümler de ilgili düzenlemeler çerçevesinde açıkça ortaya konulmuştur[39]. Ancak öğretide söz konusu Yönetmeliğin uzaktan çalışmaya dair tüm hukuki ihtiyaçlara cevap verecek kapsamlı bir düzenleme sunmadığı belirtilmektedir. Yönetmelik'in İş Kanunu'nun 14. maddesindeki uzaktan çalışmaya ilişkin hükümleri tekrar etmekle yetindiği; birçok önemli konuyu tarafların sözleşmeyle belirlemesine bıraktığı ve bu alanlara ilişkin tamamlayıcı (yedek) hukuk kurallarına yer vermediği belirtilmiştir[40].

İş Kanunu'nun 14. maddesi kapsamında yapılan düzenlemelerle, uzaktan çalışmaya ilişkin birçok temel esas belirlenmiştir. Bunlar arasında iş sözleşmesinin yazılı yapılması zorunluluğu[41], sözleşmede bulunması gereken asgari hükümler, işverenin eşit davranma yükümlülüğü ve iş sağlığı ile güvenliği konusundaki sorumlulukları öne çıkmaktadır.

2.1.4. Uzaktan Çalışma Türleri

İşin fiziksel olarak işyeri sınırlarından bağımsız bir mekânda gerçekleştirilmesine dayanan bir çalışma modeli olan uzaktan çalışma, temel olarak evde çalışma ve tele çalışma olmak üzere iki ana türe ayrılmaktadır[42]. Bu iki model, işin ifa edildiği yer, kullanılan araçlar ve işverenin denetim mekanizmaları açısından farklılıklar göstermektedir. Evde çalışma, genellikle daha geleneksel yöntemlerle ve çoğunlukla fiziki bir ürünün ortaya konulmasıyla sürdürülen bir çalışma biçimi iken; tele çalışma,

---

[38] Çelik vd., *İş Hukuku Dersleri*, 226 vd.; Süzek ve Başterzi, *İş Hukuku*, 291; Mollamahmutoğlu vd., *İş Hukuku*, 469.

[39] Uzaktan Çalışma Yönetmeliği, RG, 10.03.2021, Sayı: 31419, https://www.resmigazete.gov.tr/eskiler/2021/03/20210310-2.htm (Erişim Tarihi: 19.05.2025).

[40] Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 76; Kutlu ve Uçar, "Tarafların Hak ve Borçları Kapsamında Koronavirüs Pandemisinde Uzaktan Çalışma", 254; Melis Kutlu, *İş Hukukunda Tele Çalışma* (On İki Levha Yayıncılık, 2025), 117.

[41] İlgili maddede öngörülen yazılı şekil şartının, bir geçerlilik şartı mı yoksa yalnızca ispat şartı mı olarak değerlendirileceği, öğreti ve Yargıtay'ın görüşleri için bknz. Mollamahmutoğlu vd., *İş Hukuku*, 103-4; Sümer, *İş Hukuku*, 50; Kara, *Uzaktan Çalışmada İş Sağlığı ve Güvenliğinin Hukuki Boyutu*, 21; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 157; Öztürk İnal, *Uzaktan Çalışma*, 79.

[42] Özdemir, "Uzaktan Çalışma Yönetmeliği Karşısında Tele Çalışma", 11; Kutlu, *İş Hukukunda Tele Çalışma*, 124-39.

bilgi ve iletişim teknolojilerinin etkin kullanımını esas alan, daha modern ve genellikle hizmet odaklı bir yapı sunmaktadır. Takip eden alt başlıklar altında, uzaktan çalışmanın iki temel türü olan evde çalışma ve tele çalışma incelenecektir. Bu doğrultuda ilk olarak evde çalışma modeline, çalışmamızın esas konusunu oluşturan tele çalışmadan ayrılan yönlerini belirtmek amacıyla değinilecek; ardından tele çalışma kavramı, bir sonraki bölümde kapsamlı olarak ele alınmadan önce ana hatlarıyla açıklanacaktır.

2.1.4.1. Evde Çalışma

2.1.4.1.1. Evde Çalışmanın Tarihsel Gelişimi

Atipik çalışma türlerinin tarihsel olarak en eski biçimi olan evde çalışma, başlangıçta paketleme, dokuma ve işleme gibi el becerisi gerektiren işlerde yaygınken, son otuz yılda yaşanan ekonomik gelişmelerle önemli bir dönüşüm geçirmiştir. Günümüzde bu model, uzmanlık gerektiren işleri de kapsayacak şekilde genişlemiş; maliyetleri düşürme ve küresel rekabete uyum sağlama gibi nedenlerle birçok işletme tarafından tercih edilir hâle gelmiştir[43]. Sunduğu esnek çalışma saatleri ve mekândan bağımsızlık gibi avantajlar, COVID-19 pandemisinin de hızlandırıcı etkisiyle evde çalışmayı pek çok profesyonel meslek grubu için de yaygın bir seçenek hâline getirmiştir[44]. Bu dönüşüm sonucunda evde çalışma, el işçiliği ve tekstil gibi geleneksel alanların yanı sıra çeviri, mimarlık ve bilgisayar programcılığı gibi profesyonel hizmetlerde de sıkça görülmektedir[45].

---

[43] Öner Eyrenci ve Kadriye Bakırcı, *Dünyada ve Türkiye'de Evde Çalışma ve Eve İş Verme* (İstanbul Ticaret Odası, 2000), 7; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 154.

[44] Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 145 vd.; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 2; Öztürk İnal, *Uzaktan Çalışma*, 1; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 527; Kutlu ve Uçar, "Tarafların Hak ve Borçları Kapsamında Koronavirüs Pandemisinde Uzaktan Çalışma", 253 vd.; Sarıbay, "Uzaktan Çalışma Üzerine Sosyolojik Bir Değerlendirme", 228-30.

[45] Süzek ve Başterzi, *İş Hukuku*, 286 vd.; Çelik vd., *İş Hukuku Dersleri*, 226 vd.; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 528; Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 145-46; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 52.

2.1.4.1.2. Tanımı

Genel olarak evde çalışma öğretide işçinin, işverence oluşturulan iş organizasyonu çerçevesinde, işverenin doğrudan gözetimi olmaksızın, fiziksel olarak işyeri sınırlarının dışında, kendi evinde veya belirlediği başka bir mekânda, işveren tarafından belirlenen mal veya hizmet üretimini ücret karşılığı üstlenerek yerine getirdiği atipik bir çalışma biçimi olarak tanımlanmaktadır[46]. Evde çalışma, esasen işyeri kavramından bağımsız bir çalışma biçimi olarak değerlendirilse de, işçinin kendi ikamet ettiği konutta çalışması durumunda bu konut aynı zamanda işin gerçekleştirildiği mekân olarak kabul edilecektir. Bu bağlamda belirtmek gerekir ki, bu çalışma modeli her ne kadar evde çalışma olarak adlandırılsa da mutlaka işçinin kendi evinde gerçekleştirilmesi gerekmemektedir[47]. Kanaatimizce, evden çalışmaya ilişkin yapılacak yasal düzenlemede, bu çalışma biçiminin yalnızca işçinin kendi konutunda mı gerçekleşeceği, yoksa bilgi ve iletişim araçları kullanılmadan konut dışında da yapılabilecek her türlü uzaktan çalışmayı mı kapsadığı açıkça belirtilmelidir.

Evde çalışma modeli uluslararası alanda ilk kez 1996 yılında ILO tarafından kabul edilen 177 Sayılı Evde Çalışma Sözleşmesi ile düzenlenmiştir. Sözleşmenin 1. maddesinde, evde çalışma şu şekilde tanımlanmıştır[48]:

> *(a) evde çalışma terimi, ev işçisi olarak adlandırılacak bir kişi tarafından (i) kendi evinde veya işverenin işyeri dışında seçtiği diğer yerlerde; (ii) ücret karşılığında; (iii) işverenin belirlediği bir ürün veya hizmetin ortaya çıkmasına neden olan çalışmayı ifade eder. Bu kişinin bağımsız bir çalışan olarak kabul edilmesi için gerekli özerklik ve ekonomik bağımsızlık derecesine sahip olmaması durumunda, kullanılan ekipman, malzeme veya diğer girdilerin kim tarafından sağlandığı önemli değildir.*

---

[46] Tuncay, "Pandemi Gölgesinde Evden Çalışma", 23 vd.; Dulay, *Türk İş Hukukunda Evde Çalışma*, 122-28; Süzek ve Başterzi, *İş Hukuku*, 286 vd.; Gülver, "Türk Borçlar Kanunu'nun Evde Hizmet Sözleşmesine İlişkin Hükümleri Üzerine", 103-4; Murat Kandemir, "Evde Çalışma ve 6098 Sayılı Türk Borçlar Kanunu'nun Evde Hizmet Sözleşmesine İlişkin Hükümleri", *Journal of Istanbul University Law Faculty* 72, sy 2 (2014): 144 vd., 2; Rabia Büşra Erafşar, "Türk İş Hukukunda Evden Çalışma", *Yıldırım Beyazıt Hukuk Dergisi*, sy 1 (2022): 282 vd.

[47] Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 528.

[48] "Convention C177 - Home Work Convention, 1996 (No. 177)", erişim 25 Temmuz 2024, https://normlex.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_INSTRUMENT_ID:312322. Sözleşmeye ilişkin ayrıntılı bilgi için bknz. Bölüm 2.2.6.1.1.

Evde çalışmaya ilişkin tanımların belirli unsurlar noktasında birleştiği görülmekte olup aşağıda bu unsurlar incelenecektir.

2.1.4.1.3. Unsurları

Evde çalışma modelinin temel olarak iki unsuru bulunmaktadır. Bunlardan ilki, işçinin işverenin organizasyonu içerisinde ve onun emir ve talimatlarına bağlı olarak çalışması anlamına gelen bağımlılık ilişkisidir. İkinci unsur ise, iş görme ediminin genellikle işçinin kendi konutunda veyahut belirlenen başka bir konumda ifa edilmesi [49].

Evde çalışma modelinde, hukuki bağımlılığın zayıflayabileceği durumlar söz konusu olabilmektedir[50]. Özellikle el emeğine dayalı işlerde, işverenin doğrudan denetim ve talimat verme imkanının sınırlı olması, bağımlılık unsurunun zayıflamasına yol açabilmektedir. Bu bağlamda, her somut olayda işverenin evde çalışan üzerindeki emir ve talimat verme yetkisinin varlığı titizlikle değerlendirilmelidir[51]. Evde çalışma modelinde bağımlılık unsurunun varlığının belirlenmesi için yalnızca tarafların iş görme ve iş verme yükümlülüklerinin incelenmesi yeterli değildir. Bunun yanı sıra, işin fiilen nasıl yerine getirildiğinin değerlendirilmesi de önem taşımaktadır. Bu bağlamda çalışanın iş görme edimini şahsen ifa edip etmediği, işverenin denetimine ve talimatlarına ne ölçüde tabi olduğu ve kendisine verilen görevleri reddetme serbestisine sahip olup olmadığı gibi ölçütler özellikle dikkate alınmalıdır. Ayrıca, çalışanın teorik olarak işi reddetme yetkisi bulunsa bile, bu hakkını işini kaybetme riski olmaksızın kullanabilmesi ve yeni görevler için hazır bulunma yükümlülüğü gibi fiili koşulların varlığı da bağımlılık unsurunun değerlendirilmesinde göz önünde bulundurulmalıdır[52].

---

[49] Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 527 vd.; Dulay, *Türk İş Hukukunda Evde Çalışma*, 86 vd.; Arkın Günay, *Türk Hukukunda ve Karşılaştırmalı Hukukta Evde Çalışma* (Legal Yayıncılık, 2019), 91-93; Erafşar, "Türk İş Hukukunda Evden Çalışma", 282 vd.

[50] Sümer, *İş Hukuku*, 286 vd.; Alp, "Tele Çalışma (Uzaktan Çalışma)", 816; Dulay, *Türk İş Hukukunda Evde Çalışma*, 96; Doğan, *İş Sözleşmesinde Bağımlılık Unsuru*, 99; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 37.

[51] Dulay, *Türk İş Hukukunda Evde Çalışma*, 99; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 155; Günay, *Türk Hukukunda ve Karşılaştırmalı Hukukta Evde Çalışma*, 201.

[52] Halûk Hâdi Sümer, "İş Sözleşmesinin Bağımlılık Unsuru", *Sicil İş Hukuku Dergisi* 19 (2010): 64-65; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 156 Yargıtay'ın vermiş olduğu bir kararda "İş sözleşmesini belirleyen kriter, hukuki ve kişisel bağımlılıktır. Gerçek anlamda hukuki bağımlılık, işçinin işin yürütümüne ve işyerindeki davranışlarına ilişkin talimatlara uyma yükümlülüğünü üstlenmesi ile doğar. İşçi, edimini işverenin karar ve talimatları

İkinci unsur ise iş görme ediminin ev veya belirlenen farklı bir mekânda gerçekleştirilmesidir. Bu unsur bakımından, yukarıda da belirtildiği üzere her ne kadar evde çalışma olarak isimlendirilse de ev dışında farklı bir mekânda da gerçekleştirilebilecektir[53]. Evde gerçekleştirildiği durumlarda ise evin kapsamına, evle bağlantılı bahçe ve avlu gibi alanlar girecektir. Buna karşılık, bağımsız girişe sahip mağaza ve atölyeler ise bu kapsamın dışında tutulmaktadır. Evin ayrılmaz bir parçası olmayan (örneğin, kendi girişleri varsa) konuta bitişik perakende satış dükkanları veya tamir atölyeleri gibi yerler ve öncelikli olarak tarım, hayvancılık, ormancılık, balıkçılık ve su ürünleri yetiştiriciliği amacıyla kullanılan tarım ve bahçe arazileri, meralar veya arsalar bu ev kapsamının dışında sayılacaktır[54].

2.1.4.1.4. Evde Çalışma İlişkin Düzenlemeler

Evde çalışma sözleşmesi, İş Kanunu'nun 2016 tarihli ve 14. maddesinin dördüncü fıkrasında yapılan düzenlemeden önce Türk Borçlar Kanunu'nun 461 ilâ 469. maddeleri arasında yer alan hükümler kapsamında ele alınmaktaydı. İş Kanunu'ndaki düzenlemeyle birlikte evde çalışma modeli de uzaktan çalışma kapsamında değerlendirilmiştir[55]. Evde çalışmanın, İş Kanunu'nda uzaktan çalışma başlığı altında genel bir çerçevede ele alınması ve Kanun'un 4. maddesindeki istisnalar arasında zikredilmemesi, bu çalışma biçiminin doğrudan İş Kanunu'na tabi olduğunu net bir

---

çerçevesinde yerine getirmektedir. İşçinin bu anlamda işverene karşı kişisel bağımlılığı ön plana çıkmaktadır. Bu bağlamda, işveren ile işçi arasında hiyerarşik bir bağ vardır. İş sözleşmesine dayandığı için hukuki; işçiyi kişisel olarak işverene bağladığı için kişisel bağımlılık söz konusudur. İş sözleşmesinde bağımlılık unsurunun içeriğini; işverenin talimatlarına göre hareket etmek ve iş sürecinin ile sonuçlarının işveren tarafından denetlenmesi oluşturmaktadır. İşin işverene ait işyerinde görülmesi, malzemenin işveren tarafından sağlanması, iş görenin işin görülme tarzı bakımından iş sahibinden talimat alması, işin iş sahibi veya bir yardımcısı tarafından kontrol edilmesi, bir sermaye koymadan ve kendine ait bir organizasyonu olmadan faaliyet göstermesi, ücretin ödenme şekli; kişisel bağımlılığın tespitinde dikkate alınacak yardımcı olgulardır. Sayılan bu belirtilerin hiçbiri tek başına kesin bir ölçü teşkil etmez. İşçinin, işverenin belirlediği koşullarda çalışırken kendi yaratıcı gücünü kullanması, işverenin isteği doğrultusunda işin yapılması için serbest hareket etmesi, bu bağımlılık ilişkisini ortadan kaldırmaz. Çalışanın işyerinde kullanılan üretim araçlarına sahip olup olmaması, kâr ve zarara katılıp katılmaması, girişimcinin sahip olduğu karar verme özgürlüğüne sahip olup olmaması, bağımlılık unsuru açısından önemlidir." şeklinde belirtilmiştir. Bknz. Esas No. 2008/12560 Karar No. 2010/4619 Tarihi: 23.02.2010 (erişim tarihi 20.03.2025 https://yargi.calismatoplum.org/pdf/yargitay-kararlari-4806-c7731851.pdf) .

[53] Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 528.

[54] "Covid-19: Guidance for Labour Statistics Data Collection", 6.

[55] Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 149. Kanun koyucunun ilgili maddedeki iradesiyle ayrıntılı bilgi için bknz. Kutlu, *İş Hukukunda Tele Çalışma*, 91-94.

şekilde göstermektedir[56]. Bununla birlikte, İş Kanunu'nda evde çalışmaya özgü detaylı hükümlerin yer almaması durumunda, öğretide bu çalışma modelinin kendine has nitelikleri göz önünde bulundurularak genel hizmet sözleşmesi hükümlerinden ziyade, Türk Borçlar Kanunu'nun evde hizmet sözleşmesine ilişkin özel maddelerinin (TBK m. 461-469) kıyasen uygulanması gerektiği ağırlıklı olarak kabul görmektedir[57].

Evde çalışmaya uygulanacak hükümler çerçevesinde, özellikle iş sağlığı ve güvenliği ile eşitlik ilkesi gibi temel yükümlülükler, bu çalışma modelinin kendine özgü yapısı nedeniyle önemli tartışmaları beraberinde getirir. İşverenin, işçinin özel hayat alanı olan konutuna müdahale etmeden iş sağlığı ve güvenliği denetimi yapma zorunluluğu, konut dokunulmazlığı ile çatışırken[58]; iş kazalarında illiyet bağının tespiti ve ispatı da önemli güçlükler yaratmaktadır[59]. Benzer şekilde, evde çalışanların, işyerindeki emsal çalışanlarla ücret[60], sosyal haklar ve kariyer olanakları gibi konularda ayrımcılığa uğramaması, eşitlik ilkesinin temel bir gereğidir[61] ve bu durum uluslararası düzenlemelerde de vurgulanmıştır[62].

---

[56] Süzek ve Başterzi, *İş Hukuku*, 285; Çelik vd., *İş Hukuku Dersleri*, 221; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 55.

[57] Evde çalışanlara uygulanacak hükümlere ilişkin öğreti görüşleri için bkz. Kutlu, *İş Hukukunda Tele Çalışma*, 110; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 143. Ayrıca, bağımlılık ilişkisinin mevcut olmadığı evde çalışma biçimleri açısından da yine Türk Borçlar Kanunu'nun evde hizmet sözleşmesine yönelik düzenlemelerinin uygulanacağı öğretide benimsenmektedir. Bknz. Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 21.

[58] Murat Engin, "Türk İş Hukukunda Evde Çalışma", *Prof. Dr. Turhan Esener'e Armağan, Ankara*, 2000, 284; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 563; Alp, "Tele Çalışma (Uzaktan Çalışma)", 836; Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 134; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 163.

[59] Alp, "Tele Çalışma (Uzaktan Çalışma)", 837; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 563; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 163; Pelin Tunç Yılmaz, "Uzaktan Çalışmanın Bir Türü Olarak Evde Çalışma", *Sicil İş Hukuku Dergisi*, sy 43 (2020): 270.

[60] Süzek ve Başterzi, İş Hukuku, 445 vd.; Levent Akın, "İş Kazalarından Doğan Hukuksal Sorumlulukta Uygun Nedensellik Bağı", TMMOB İnşaat Mühendisleri Odası Ankara Şubesi, İş Sağlığı ve Güvenliği Sempozyumu Bildiriler Kitabı, Ankara, 2007, 63-76; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 164; Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 178.

[61] Engin, "Türk İş Hukukunda Evde Çalışma", 283; Sarper Süzek, "İş Akdinin Türleri", *Mercek Dergisi*, sy 22 (2001): 31; M. Fatih Uşan, *İş ve Sosyal Sigorta Hukuku Uygulamasında Parça Başına Ücret* (Seçkin Yayıncılık, 2003), 96; Alp, "Tele Çalışma (Uzaktan Çalışma)", 837; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 164. Aksi yönde görüş ilişkin bknz. Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma".

[62] "Convention C184 - Safety and Health in Agriculture Convention, 2001 (No. 184)", erişim 01 Nisan 2025,
https://normlex.ilo.org/dyn/nrmlx_en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C184
Türkiye'nin bu sözleşmeyi henüz onaylamamış olması nedeniyle, sözleşme hükümlerinin iç hukukumuzda doğrudan bir bağlayıcılığı bulunmamaktadır.

2.1.4.2. Evde Çalışma ve Tele Çalışmanın Farkları

Tele çalışma, uzaktan çalışmanın bir alt türü olarak, çalışanların iş görme edimini bilgi ve iletişim teknolojilerinden yararlanarak fiziksel olarak işyeri sınırları dışında yürüttüğü bir çalışma biçimini ifade etmektedir. Geleneksel çalışma düzeninden farklı olarak, tele çalışma mekân bağımsızlığı sağlayarak iş süreçlerinin coğrafi kısıtlardan arındırılmasına olanak tanımaktadır[63]. Dijitalleşmenin hız kazanmasıyla birlikte iş organizasyonlarında önemli bir yer edinen tele çalışma, sağladığı imkânlarla birlikte iş ilişkisi açısından hukuki ve pratik birtakım sorunları da beraberinde getirmektedir[64].

Her ne kadar tele çalışma ve evden çalışma, genel olarak "uzaktan çalışma" kavramı altında ortak bir çerçevede değerlendirilse de bu iki model arasında önemli farklılıklar bulunmaktadır. Tele çalışma ilişkisinin evde çalışmadan temel farkı tele çalışanın bilgi ve iletişim teknolojilerinden faydalanarak işyerine bağlanmasıdır[65]. Evde çalışmaya kıyasla, tele çalışma modelinde işçinin işverene olan bağımlılığının daha sıkı bir şekilde devam ettiği ifade edilebilir[66]. Genellikle bağımlılık ilişkisinin zayıf olması, evde çalışmanın iş sözleşmesi kapsamında değerlendirilip değerlendirilemeyeceğini belirlemeyi güçleştirmektedir[67]. Ancak bu durum, her evde çalışma ilişkisinin zayıf bir bağımlılık unsuru taşıdığı anlamına gelmez; ilişkinin niteliği, işin somut koşullarına ve işverenin denetim yetkisinin derecesine göre ayrıca değerlendirilmelidir.

Tele çalışma modelinde, fiziki olarak işyerinde bulunma zorunluluğu ortadan kalksa da çalışanın işverenin denetim ve talimatlarına iş organizasyonu çerçevesinde bağlı kalmaya devam etmesi, iş ilişkisinde bağımlılık unsurunun büyük ölçüde korunduğunu ortaya koymaktadır[68]. Ek olarak evde çalışmaya özgü işverenin denetim yapma ve

---

[63] Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 552; Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 232; Kutlu, *İş Hukukunda Tele Çalışma*, 179.
[64] Kutlu, *İş Hukukunda Tele Çalışma*, 2; Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 4; Erkanlı Başbüyük, "Uzaktan Çalışmanın Bir Türü Olarak Tele Çalışmada İşçinin Dinlenme Hakkı", 657-58.
[65] Çelik vd., *İş Hukuku Dersleri*, 336 vd.; Senyen Kaplan, *Bireysel İş Hukuku*, 2. bs, 159; Özdemir, "Uzaktan Çalışma Yönetmeliği Karşısında Tele Çalışma", 13; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 54; Dulay, *Türk İş Hukukunda Evde Çalışma*, 152.
[66] Süzek ve Başterzi, *İş Hukuku*, 291; Dulay, *Türk İş Hukukunda Evde Çalışma*, 99.
[67] Evde çalışmalarda sıkı bir bağımlılık aranmaması gerektiği yönünde bknz. Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi"; Kandemir, "Evde Çalışma ve 6098 Sayılı Türk Borçlar Kanunu'nun Evde Hizmet Sözleşmesine İlişkin Hükümleri", 150-51; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 56.
[68] Süzek ve Başterzi, *İş Hukuku*, 292; Dulay, *Türk İş Hukukunda Evde Çalışma*, 99; Şakar ve Erkan Şahin, "Esnek Çalışma Modellerinden Uzaktan Çalışma ve Uzaktan Çalışanların Sigortalılığı", 252-53.

işçinin hakları arasındaki dengenin korunması sorunu, denetimin fiziksel mekândan dijital ortama taşındığı ve işin sonucundan ziyade sürecin izlendiği tele çalışma modelinde köklü bir dönüşüme uğramaktadır. Bununla birlikte işverenin yükümlülükleri de farklılaşmaktadır. Örneğin işverenin iş sağlığı ve güvenliğini sağlama yükümlülüğü dijital yorgunluk gibi psikososyal riskleri, eşitlik ilkesi ise algoritmik ayrımcılık tehdidini de kapsamak zorunda kalmakta; bu durum, çalışanın özel hayatına ve kişisel verilerine yönelik müdahalelerin hukuki sınırlarının yeniden çizilmesini zorunlu kılmaktadır.

2.2. Tele Çalışma

2.2.1. Tele Çalışmanın Tarihi Gelişimi ve Dijitalleşme ile Değişen Dinamikleri

Tele çalışmanın tarihsel gelişimi, bu istihdam biçiminin günümüzde yaygınlaşmasını etkileyen çeşitli sosyal, ekonomik ve yapısal dinamikler çerçevesinde ele alınmaktadır. Uluslararası rekabetin artması, küreselleşme, dönemsel ekonomik krizler, işsizlik oranlarındaki değişimler ve bireylerin iş-yaşam dengesi arayışı gibi çeşitli sosyoekonomik faktörler, bu modelin yaygınlaşmasına zemin hazırlamıştır. Özellikle 1980'li yıllardan itibaren uygulama alanı bulan tele çalışma, 1990'lı yıllarda hız kazanmış[69]; başta bilişim, mühendislik, danışmanlık, tasarım, muhasebe ve çeviri gibi fikri emeğe dayalı meslek gruplarında yaygınlaşmıştır[70]. Ayrıca bazı sektörlerde müşteri hizmetleri, satış ve bankacılık gibi faaliyetlerde de tele çalışmanın yaygın bir istihdam modeli hâline geldiği görülmektedir. Dijital teknolojiler, belirtilen sektörlerde iş süreçlerini yeniden şekillendirmiş, coğrafi sınırlılıkları ortadan kaldırarak küresel yetenek havuzlarına erişimi kolaylaştırmış ve iş süreçlerinde verimlilik artışına olanak tanımıştır[71]. COVID-19 Pandemisi ise bu modeli küresel ölçekte zorunlu ve yaygın bir uygulama hâline getirmiştir[72].

---

[69] Soysal, "Tele Çalışma", 139-40; Kara, *Uzaktan Çalışmada İş Sağlığı ve Güvenliğinin Hukuki Boyutu*, 34.

[70] Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 31; Dulay, *Türk İş Hukukunda Evde Çalışma*, 1.

[71] Alp, "Tele Çalışma (Uzaktan Çalışma)", 801; Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 36; Soysal, "Tele Çalışma", 135-38; Erkanlı Başbüyük, "Uzaktan Çalışmanın Bir Türü Olarak Tele Çalışmada İşçinin Dinlenme Hakkı", 657-58.

[72] Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 145 vd.; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 52; Öztürk İnal, *Uzaktan Çalışma*, 1; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 527; Kutlu ve Uçar, "Tarafların Hak ve

Türkiye'de tele çalışmaya ilişkin ilk yasal düzenleme 2016 yılında 4857 sayılı İş Kanunu'na eklenen hükümle yapılmıştır. 2020 yılında ortaya çıkan pandemi süreci, tele çalışmanın yaygınlaşmasına neden olmuş; bu fiilî gelişmeler de hukuki bir çerçeveye duyulan ihtiyacı artırarak Uzaktan Çalışma Yönetmeliği'nin düzenlenmesine zemin hazırlamıştır. 2021 yılında yürürlüğe Yönetmelik ile tele çalışmanın usul ve esaslarına ilişkin ayrıntılı hükümler getirilmiştir[73]. Böylece tele çalışma hem tarihsel kökleri hem de modern iş yaşamındaki esnekliğiyle, Türkiye'deki çalışma ilişkilerinde önemli bir yere sahip olmuştur[74].

2.2.2. Tele Çalışmanın İş İlişkilerine Etkileri

Son yıllarda teknolojik altyapının güçlenmesi ve dijital dönüşümün hız kazanmasıyla birlikte tele çalışma modeli, iş hayatında giderek daha fazla tercih edilmektedir. Dijitalleşme süreci, yalnızca teknolojik araçların kullanımını değil, aynı zamanda iş süreçlerinin ve organizasyon yapılarının da dijital ortama taşınmasını kapsamaktadır[75]. İşverenler, bu köklü dönüşüme üretim teknikleri ve çalışma düzenleri açısından uyum sağlamak zorunda kalmış, bu durum ise çalışma ilişkilerinde daha esnek bir yapıya geçişi hızlandırmıştır. Özellikle COVID-19 Pandemisi döneminde birçok ülkede zorunlu olarak benimsenen uzaktan çalışma, bu eğilimi geri döndürülemez bir noktaya taşımıştır. Nitekim bu süreçle birlikte çalışanların beklentilerinin de değiştiği, önemli bir kısmının tamamen veya kısmen uzaktan çalışmayı tercih ettiği ve bu modelin iş gücü verimliliği üzerindeki etkilerinin akademik açıdan daha kapsamlı biçimde incelenmeye başlandığı görülmektedir[76].

Borçları Kapsamında Koronavirüs Pandemisinde Uzaktan Çalışma", 253 vd.; Sarıbay, "Uzaktan Çalışma Üzerine Sosyolojik Bir Değerlendirme", 228-30; Kutlu, *İş Hukukunda Tele Çalışma*, 95-97.

[73] Tuna ve Türkmendağ, "Covid-19 Pandemi Döneminde Uzaktan Çalışma Uygulamaları ve Çalışma Motivasyonunu Etkileyen Faktörler", 3248; Şakar ve Erkan Şahin, "Esnek Çalışma Modellerinden Uzaktan Çalışma ve Uzaktan Çalışanların Sigortalılığı", 250.

[74] Kutlu, *İş Hukukunda Tele Çalışma*, 97-99.

[75] Halim Baş, "Türkiye'de Sanal Beyin Göçü: Uzaktan Yurtdışına Çalışanların Deneyimleri Üzerine Nitel Bir Araştırma", İstanbul İktisat Dergisi 72, sy 2 (2022): 920.

[76] Örneğin Amerika Birleşik Devletleri merkezli bir araştırma ve danışmanlık şirketi tarafından yapılan çalışanların uzaktan çalışmaya yönelik görüşlerinin araştırıldığı bir çalışmada, çalışanların %56'sının tamamen uzaktan çalışmayı tercih ederken, %17'sinin uzaktan çalışmayı hiçbir şekilde tercih etmediğini, %78'inin ise haftanın belirli günlerinde uzaktan çalışmak istediğini ortaya konmuştur. Ayrıntılar için bknz. Rebecca Palacios ve George Penn, "Beyond Remote Work: The Hybrid Workforce Model", *Gartner*, 2020, 8.

2.2.2.1. Avantajları

Tele çalışma modeli, tarafların hak ve yükümlülüklerine karşılıklı özen gösterildiği bir çerçevede uygulandığında hem çalışanlar hem de işverenler için önemli kazanımlar sunmaktadır. Avrupa Birliği ülkelerinde yapılan araştırmalar, bu modelin çalışanlar üzerindeki çok yönlü olumlu etkilerini ortaya koymaktadır. Çalışanlar, ofis ortamındaki rahatsızlık ve kesintilerden daha az etkilenerek işlerine daha iyi odaklandıklarını, toplantılarda daha disiplinli olduklarını ve gereksiz konuşmalardan kaçındıklarını belirtmişlerdir[77]. Ayrıca, çalışma ortamlarını kendilerine göre düzenleyebilme esnekliği ve işe gidip gelme süresinin ortadan kalkmasıyla kazanılan zaman, iş-özel hayat dengesine ve psikolojik sağlıklarına olumlu katkı sağlamaktadır[78]. Bu durum yalnızca çalışan memnuniyeti ile sınırlı kalmamakta, doğrudan işveren verimliliğine de yansımaktadır. Nitekim pandemi sırasında Avusturya, Çekya, İtalya, Malta, Portekiz ve İspanya'da işverenlerle yapılan anketler, tele çalışmanın genel olarak iş gücü verimliliğini ve çalışan performansını olumlu yönde etkilediğini ve çalışanların üretkenliğini artırdığını doğrulamaktadır[79].

2.2.2.2. Sınırlılıkları ve Zorlukları

Tele çalışmanın sunduğu avantajların yanı sıra hem çalışanlar hem de iş süreçleri açısından önemli sınırlılıklar ve zorluklar barındırdığı da unutulmamalıdır. Yapılan araştırmalar, tele çalışmanın genellikle daha uzun çalışma saatleri ve esnek programlarla ilişkili olduğunu göstermektedir[80]. Çalışanlar, işin planlanması ve yürütülmesinde daha yüksek düzeyde özerklik elde etse de bu durum her zaman olumlu sonuçlar doğurmamaktadır. Aksine, esnekliğin getirdiği sürekli erişilebilir olma durumu, çalışanların daha uzun ve düzensiz saatlerde çalışmasına, artan iş yükü ve etkili öz yönetim gerekliliği ise işin yoğunlaşarak sosyal olmayan zaman dilimlerine taşmasına neden olabilmektedir. Öğretide, artan özerkliğin aynı zamanda artan iş yükü

---

[77] O. V. Llave vd., *The Rise in Telework: Impact on Working Conditions and Regulations* (European Foundation for the Improvement of Living and Working Conditions (Eurofound), 2022), 31.
[78] Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 145; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 148.
[79] Iñigo Isusi vd., *Working Conditions in Telework During The Pandemic and Future Challenges*, no. WPEF22032 (European Foundation for the Improvement of Living and Working Conditions, 2022), 13.
[80] Llave vd., *The Rise in Telework*, 26-27.

ve kontrol kaybı riskini beraberinde getirdiği bu çelişkili durum, "özerklik paradoksu" olarak adlandırılmaktadır[81]. Bu temel soruna ek olarak, Belçika ve Danimarka gibi ülkelerde yapılan araştırmalar, verimlilik kayıplarının da yaşanabildiğini ortaya koymaktadır. Bu kayıpların arkasında ekip içi iş birliği eksikliği, çocuk bakımı gibi sorumluluklarla iş-yaşam dengesinin bozulması, çalışma materyallerine erişimde yaşanan zorluklar, konsantrasyon problemleri ve teknik aksaklıklar gibi çeşitli faktörler bulunmaktadır[82]. Sonuç olarak, gerekli hukuki ve yapısal altyapı kurulmadığında veya işveren ile çalışan arasındaki güven ve sorumluluk dengesi göz ardı edildiğinde, sosyal izolasyon, dijital yorgunluk ve dinlenme sürelerinin ihlali gibi olumsuzlukların ortaya çıkması kaçınılmazdır[83]. Dolayısıyla, modelin sağladığı esneklik ile beraberinde getirdiği bu sınırlılıklar, sistemin sürdürülebilirliği açısından çalışan haklarını koruyan ve işveren yükümlülüklerini netleştiren dengeli hukuk politikalarının geliştirilmesini zorunlu kılmaktadır[84].

2.2.3. Tanımı

Tele çalışma kavramı, uluslararası düzeyde üzerinde fikir birliğine varılmış kesin bir tanıma henüz sahip olmasa da genellikle uzaktan çalışma modelinin bir alt kategorisi olarak kabul edilmektedir. Hem ülke mevzuatlarında hem de öğretide terimsel olarak farklı şekillerde tanımlanmakta ve yorumlanmaktadır. İş Kanunu 14. maddenin dördüncü fıkrasına göre, tele çalışma*, "işyeri dışında, bilgi işlem teknolojileri aracılığıyla ve işyeri ile bağlantı kurularak iş görme ediminin ifa edildiği bir çalışma biçimi"* olarak tanımlanmıştır[85]. Uluslararası alanda önemli bir referans olan Tele Çalışma Çerçeve Sözleşmesi de benzer bir yaklaşımla tele çalışmayı, *"tele-çalışma, bir iş sözleşmesi ya da iş ilişkisi çerçevesinde, bilgi teknolojileri kullanılarak çalışmanın örgütlenmesi ve/veya yerine getirilmesi biçimidir; bu çalışma, işverenin işyeri sınırları içinde de gerçekleştirilebilecek iken, söz konusu işyerinin dışında ve düzenli bir biçimde yürütülmektedir."* şeklinde tanımlamıştır[86]. Mukayeseli hukuk

[81] Llave vd., The Rise in Telework, 26-27.
[82] Llave vd., The Rise in Telework, 32.
[83] Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 152-53.
[84] Ergüneş Emrağ, "4857 Sayılı İş Kanunun Değişik 14. Maddesi Işığında Tele Çalışma", 1414.
[85] Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 158; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 54.
[86] Çerçeve Sözleşme'ye ilişkin ayrıntılı bilgi için bknz. Bölüm 2.2.6.1.2.

örnekleri incelendiğinde aşağıda belirtilen unsurların korunduğu görülmektedir. Alman hukukunda terim, genellikle telekomünikasyon araçlarıyla fiziksel olarak işyeri sınırları dışında gerçekleştirilen işleri ifade ederken[87]; Fransız hukukunda ise İş Kanunu'nda yer alan tanıma göre tele çalışma, *"işverenin işyerinde de yapılabilecek bir işin, bilgi ve iletişim teknolojileri kullanılarak, çalışanın bu işyeri dışında isteyerek gerçekleştirdiği her türlü işin düzenlenmesi"* olarak belirtilmiştir[88]. Farklı hukuki düzenlemelerdeki tanımlar incelendiğinde ortak noktanın; işin, işverenin organizasyonu dâhilinde, fiziksel olarak işyeri sınırları dışında ve bilişim teknolojileri kullanılarak ifa edilmesi olduğu görülmektedir.

2.2.4. Unsurları

Tele çalışma, onu diğer istihdam biçimlerinden ayıran ve kendine özgü yapısını oluşturan üç temel unsur üzerine kuruludur: Organizasyon, mekân ve teknoloji[89]. Bu unsurlar, tele çalışmanın hukuki ve pratik çerçevesini birlikte şekillendirir. Organizasyon unsuru, işin işverenin yönetim ve denetim yetkisi altında bir iş ilişkisi dâhilinde yürütülmesini ifade ederken; mekân unsuru, bu işin fiziksel olarak işyeri sınırları dışında ifa edilmesini tanımlar[90]. Teknoloji unsuru ise bu iki unsuru birbirine bağlayan, mekânsal ayrılığa rağmen organizasyonel bağın sürdürülmesini sağlayan ayırt edici ve zorunlu bir bileşendir[91].

İlk unsur olan organizasyon unsuru işçinin işverene hukuki ve ekonomik olarak bağlı olmasını ifade eden temel bir unsurdur[92]. Tele çalışmada işçi, işverenin organizasyonu

---

[87] Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 160.
[88] "Article L1222-9 - Code du travail - Légifrance". Pavel Sládek ve Tomáš Sigmund, "Legal Issues of Teleworking", SHS Web of Conferences 90 (2021): 01020, https://www.shs-conferences.org/articles/shsconf/abs/2021/01/shsconf_eccw2020_01020/shsconf_eccw2020_01020.html.
[89] Çelik vd., *İş Hukuku Dersleri*, 226 vd.; Aydın, *Bireysel İş Hukuku*, 125.
[90] Çelik vd., *İş Hukuku Dersleri*, 219; Özdemir, "Uzaktan Çalışma Yönetmeliği Karşısında Tele Çalışma", 13; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 4.
[91] Süzek ve Başterzi, *İş Hukuku*, 291; Çelik vd., *İş Hukuku Dersleri*, 218-19; Yeliz Bozkurt Gümrükçüoğlu vd., *İş Hukukunda Uzman Arabuluculuk* (Ankara, 2023), 96; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 4-5.
[92] Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 33; Kutlu, *İş Hukukunda Tele Çalışma*, 19; Şanlı, "İş Hukukunda Uzaktan Çalışma", 10.

içinde onun emir ve talimatlarına uygun şekilde çalışmakla yükümlüdür[93]. Dolayısıyla, işverenin yönetim ve denetim yetkisi, mekânsal ayrılığa rağmen varlığını sürdürür ve işçi, işverenin belirlediği çalışma düzenine uymak zorundadır[94]. Fiziksel olarak doğrudan bir gözetim imkânı olmasa da iş süreçlerinin elektronik araçlar vasıtasıyla izlenmesi ve denetlenmesi, klasik iş sözleşmesinin temelini oluşturan bu bağımlılık unsurunun varlığını güçlendirmekte iş organizasyonu bağlı kılmaktadır[95]. Bu nedenle, tele çalışmada bağımlılık unsurunun sağlanmasında klasik iş ilişkilerinden farklı olarak bilgi ve iletişim teknolojilerinin etkisi daha etkindir[96].

Tele çalışmanın ikinci unsuru ise işin işveren tarafından belirlenen fiziksel işyerinden bağımsız bir mekânda gerçekleştirilmesidir. Geleneksel çalışma düzenin aksine tele çalışmada işçi, iş görme edimini evde, bir kafede, otelde veya seyahat hâlindeyken yerine getirebilmektedir[97]. Tele çalışmanın mekânsal bağımsızlığı, işçinin işverenin fiziksel denetim alanı dışında çalışmasına olanak tanırken, işverenin emir ve talimatlarına bağlılığını ortadan kaldırmamaktadır[98].

Tam bu noktada, tele çalışmayı tanımlayan asıl ayırt edici nitelik olan teknoloji unsuru devreye girer. Teknoloji unsuru çalışanın bilgi ve iletişim teknolojileri ile iş organizasyona bağlı olmasıdır. Ancak, işin uzaktan yürütülmesi için bilgisayar veya akıllı telefon gibi bilgi ve iletişim teknolojilerinin kullanılması tek başına yeterli değildir; asıl belirleyici olan, bu teknolojik araçlar vasıtasıyla işyeri ile etkin ve sürekli

---

[93] Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 98; Erkanlı Başbüyük, "Uzaktan Çalışmanın Bir Türü Olarak Tele Çalışmada İşçinin Dinlenme Hakkı", 659-60; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 1.
[94] Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 69.
[95] Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 39-40; Erafşar, "Türk İş Hukukunda Evden Çalışma", 294.
[96] Ayrıca belirtmek gerekir ki tele çalışanın, bağlantıda olduğu süre zarfında yalnızca fiilen iş görmesi değil, işverence verilen talimatlara uygun şekilde hazır bulunması da iş görme ediminin ifası kapsamında değerlendirilir. Özellikle tele çalışma modelinde, işçinin belirlenen saatlerde hazır olması, işin sürdürülebilirliği açısından aktif katılım anlamına gelir. Bkz. Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 153.
[97] Kutlu, *İş Hukukunda Tele Çalışma*, 1; Ergüneş Emrağ, "4857 Sayılı İş Kanunun Değişik 14. Maddesi Işığında Tele Çalışma", 1417-18.
[98] Süzek ve Başterzi, *İş Hukuku*, 292; Tuncay, "Pandemi Gölgesinde Evden Çalışma", 40; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 546; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 40; Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 40.

bir bağlantının kurulmuş olmasıdır[99]. İş süreçlerine entegrasyonu sağlayan bu bağlantı, tele çalışmanın tanımlayıcı bir özelliği olarak kabul edilmekte ve işverenin iş organizasyonu içerisinde çalışanın hukuki bağımlılığının devam ettiğini teyit etmektedir[100].

2.2.5. Tele Çalışma Türleri

Dijitalleşmenin iş dünyasındaki yaygınlığının artmasıyla birlikte tele çalışma, tekdüze bir model olmaktan çıkıp farklı uygulama biçimlerine ayrılan çeşitli bir yapıya bürünmüştür[101]. Bu nedenle tele çalışma sözleşmeleri, işin niteliğine ve tarafların ihtiyaçlarına göre farklılık göstermektedir[102]. Öğretide tele çalışma türleri; işin yapıldığı yer, işyeriyle kurulan bağlantının niteliği, çalışma süresi ve yapılan işin türü gibi çeşitli ölçütlere göre sınıflandırılmaktadır. En yaygın sınıflandırma, işin ifa edildiği mekâna göre yapılmaktadır. Bu bağlamda, çalışanın işini kendi evinden yürüttüğü evde tele çalışma[103], işverene ait veya anlaşmalı merkezlerde çalışılan tele merkezler, sürekli hareket hâlinde çalışmayı ifade eden gezici (mobil) tele çalışma ve işyeri ile uzaktan çalışmanın birleştirildiği hibrit (dönüşümlü) tele çalışma gibi modeller öne çıkmaktadır[104]. Bunun yanı sıra tele çalışma, işyeriyle kurulan dijital

---

[99] Çelik vd., *İş Hukuku Dersleri*, 219; Senyen Kaplan, *Bireysel İş Hukuku*, 2. bs, 159; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 533; Alp, "Tele Çalışma (Uzaktan Çalışma)", 807; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 5.

[100] Şanlı, "İş Hukukunda Uzaktan Çalışma", 10.

[101] Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 528; Kutlu, *İş Hukukunda Tele Çalışma*, 125; Sarıbay, "Uzaktan Çalışma Üzerine Sosyolojik Bir Değerlendirme", 228.

[102] Alp, "Tele Çalışma (Uzaktan Çalışma)", 801-5; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 536; Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 43; Erkanlı Başbüyük, "Uzaktan Çalışmanın Bir Türü Olarak Tele Çalışmada İşçinin Dinlenme Hakkı", 660; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 17-18.

[103] ÜÇO'nun yayımladığı COVID-19: İşgücü İstatistikleri Verilerinin Toplanmasına İlişkin Rehber doğrultusunda, tele çalışma türlerinin kavramsal sınırlarının belirlenmesi önem arz etmektedir. Rehberde ele alınan sınıflandırma çerçevesinde, evden uzaktan çalışma, evden tele çalışma, ev esaslı çalışma ve ev esaslı tele çalışma kavramlarının birbiriyle ilişkili olduğu ve uygulamada sıklıkla iç içe geçtiği görülmektedir. Bu bağlamda, evden uzaktan çalışma, çalışanın iş görme edimini geleneksel işyeri yerine kendi evinde gerçekleştirdiği modeldir. Evden tele çalışma ise, uzaktan çalışmaya benzer olmakla birlikte, çalışanların bilgi ve iletişim teknolojilerini aktif kullanarak iş süreçlerini evden yürüttükleri, böylelikle işyerine dijital olarak bağlandıkları bir çalışma biçimidir. Öte yandan, ev esaslı çalışma kavramı, esas iş yerini ev olarak kabul eden ancak bunu varsayılan iş yeri olarak değerlendirmeyen çalışanları ifade etmektedir. Ev esaslı tele çalışma ise bu iki modelin kesişiminde yer alır ve çalışanların hem işlerini ev merkezli olarak yürüttükleri hem de bunu tele çalışma teknolojileri aracılığıyla gerçekleştirdikleri durumu ifade eder. Ayrıntılar için bknz. "Covid-19: Guidance for Labour Statistics Data Collection", 7.

[104] Ufuk Aydın, "Tele Çalışma ve Tele Çalışma Çerçeve Avrupa Sözleşmesi", içinde *Prof. Dr. Devrim Ulucan'a Armağan*, Hukuk Kitapları Serisi 119 (Legal Yayıncılık, 2008), 355-56; Civan, "İş

bağlantının şekline göre çevrim içi ve çevrim dışı olmak üzere ikiye ayrılmaktadır[105]. Son olarak, yapılan işin niteliği gereği ürün arzı ve hizmet arzı esaslı tele çalışma şeklinde bir ayrıma tabi tutulmaktadır[106]. Takip eden bölümlerde, belirtilen sınıflandırmalar ışığında uygulamada öne çıkan tele çalışma modelleri ayrıntılı olarak ele alınacaktır.

2.2.5.1. Evde Tele Çalışma

Dijital teknolojilerin sağladığı yer ve zaman bağımsızlığı sayesinde tele çalışmanın en sık rastlanan türü olan evde tele çalışma, iş dünyasında giderek daha fazla ön plana çıkmaktadır[107]. Temel olarak bu model, işçinin iş görme borcunu evinde, teknolojik cihazlar ve dijital iletişim olanaklarından yararlanarak ifa etmesi esasına dayanır[108]. Bu modelin en belirgin özelliği ve aynı zamanda en temel zorluğu, işin ifa edildiği mekânın özel hayat alanı olan "ev" olmasıdır. Ev, yalnızca bir çalışma alanı değil; aynı zamanda eğitim, çocuk bakımı, ibadet, spor ve sosyal etkinlikler için de kullanılan çok işlevli bir alandır. Özellikle tele çalışmanın yaygınlaşmasıyla birlikte evin çok yönlü kullanımı, çalışanların özel hayatına daha müdahaleci bir şekilde izlenmesi için bir zemin hazırlamıştır[109]. Bu durum, ilerleyen bölümlerde ele alınacağı üzere, işverenin denetim hakkı ile çalışanın özel hayatının gizliliği, konut dokunulmazlığı ve kişisel verilerinin korunması hakkı arasındaki sınırların yeniden çizilmesini gerektiren temel hukuki sorunları beraberinde getirmektedir.

Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 537; Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 152; Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 145 vd.; Özdemir, "Uzaktan Çalışma Yönetmeliği Karşısında Tele Çalışma", 36; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 55.

[105] Alp, "Tele Çalışma (Uzaktan Çalışma)", 807-8; Kutlu, *İş Hukukunda Tele Çalışma*, 70.

[106] Kutlu, *İş Hukukunda Tele Çalışma*, 62-64.

[107] Baş, "Türkiye'de Sanal Beyin Göçü: Uzaktan Yurtdışına Çalışanların Deneyimleri Üzerine Nitel Bir Araştırma", 911-12.

[108] Alp, "Tele Çalışma (Uzaktan Çalışma)", 802-3; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 536; Erkanlı Başbüyük, "Uzaktan Çalışmanın Bir Türü Olarak Tele Çalışmada İşçinin Dinlenme Hakkı", 660.

[109] Kirstie Ball, *Electronic Monitoring and Surveillance in the Workplace: Literature Review and Policy Recommendations* (Publications Office of the European Union, 2021), 54.

2.2.5.2. Tele Merkezden (Uydu Tele) Çalışma

Evde tele çalışmadan farklı bir model olan tele merkezden çalışma; işin, çalışanın özel hayat alanında değil, işverene ait veya anlaşmalı "uydu" ya da "komşu çalışma" merkezlerinde yürütülmesidir[110]. Bu merkezler, işletmelerin iş süreçlerini daha verimli, düzenli ve sürdürülebilir biçimde yürütebilmeleri amacıyla gelişmiş bilgisayar ve iletişim teknolojileriyle donatılmış modern elektronik çalışma ortamlarıdır[111]. İşyeri ile ev arasında bir ara model sunan tele merkezler, çalışanların sosyal izolasyonunu azaltırken, ulaşım masraflarını düşürmek, çevreyi korumak ve bölgesel kalkınmayı desteklemek gibi önemli faydalar da sunar[112]. Hukuki açıdan bakıldığında, tele merkezlerde çalışanlar işverenin doğrudan gözetiminden uzakta olsalar da iş organizasyonunun ayrılmaz bir parçası olarak kabul edilirler[113]. Bu nedenle, evde veya mobil tele çalışmadan farklı olarak fiziki bir mekânda yoğunlaşmış olsalar dahi, bu merkezler hukuken "işyeri" niteliği taşır ve asli işyeri dışında faaliyet göstermeleri bakımından diğer tele çalışma biçimleriyle özdeş bir nitelik arz ederler[114].

2.2.5.3. Hibrit (Dönüşümlü) Tele Çalışma

Son yıllarda, özellikle pandemi sonrası iş dünyasında hızla popülerlik kazanan hibrit (dönüşümlü) tele çalışma modeli, uzaktan çalışma ile işyerinde fiziksel çalışmayı birleştiren esnek bir yapı sunmaktadır[115]. Bu modelin temel amacı, çalışanların belirli günlerde işyerine gelerek sosyal etkileşim ve iş birliği avantajlarından yararlanmasını, diğer günlerde ise uzaktan çalışarak esneklik ve odaklanma imkânı bulmasını sağlamaktır[116]. Bu sayede işverenler ve çalışanlar arasında uyum ve ortak sorumluluk bilincinin gelişimine katkı sağlayan hibrit modelin esnek yapısı, kendi içinde farklı

---

[110] Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 45; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 536; Erkanlı Başbüyük, "Uzaktan Çalışmanın Bir Türü Olarak Tele Çalışmada İşçinin Dinlenme Hakkı", 660.
[111] Soysal, "Tele Çalışma", 149; Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 45; Günay, *Türk Hukukunda ve Karşılaştırmalı Hukukta Evde Çalışma*, 88.
[112] Soysal, "Tele Çalışma", 149; Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 45; Günay, *Türk Hukukunda ve Karşılaştırmalı Hukukta Evde Çalışma*, 88.
[113] Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 45.
[114] Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 90.
[115] Özdemir, "Uzaktan Çalışma Yönetmeliği Karşısında Tele Çalışma", 36; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 5; Şanlı, "İş Hukukunda Uzaktan Çalışma", 13.
[116] Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 55; Palacios ve Penn, "Beyond Remote Work: The Hybrid Workforce Model", 14; Şanlı, "İş Hukukunda Uzaktan Çalışma", 13.

yoğunluklarda uygulanmasına da olanak tanımaktadır. Bunlar; haftada bir günden az süreyle gerçekleştirilen "tamamlayıcı tele çalışma", haftada en az bir gün tele çalışmayı içeren "dönüşümlü tele çalışma" ve çalışma süresinin çoğunluğunun tele çalışma yoluyla tamamlandığı "sürekli tele çalışma" olarak karşımıza çıkmaktadır[117]. Türk Hukuku açısından bakıldığında ise, iş görme ediminin bu şekilde kısmen fiziksel olarak işyeri sınırları içerisinde kısmen de uzaktan yerine getirilmesine ilişkin özel bir yasal düzenleme bulunmamaktadır. Bununla birlikte, öğretide iş hukukunun esnek yapısının bu çalışma biçimine engel teşkil etmediği ve uzaktan çalışmaya ilişkin genel hükümlerin, hibrit modelin uzaktan çalışma kısımları için de kıyasen uygulanacağı kabul edilmektedir[118].

2.2.5.4. Çevrim İçi-Çevrim Dışı Tele Çalışma

Tele çalışma modelleri, çalışanın işyeri ile kurduğu dijital bağlantının niteliğine göre de sınıflandırılmaktadır. Bu ayrım, özellikle işverenin denetim yetkisinin yoğunluğu açısından önem taşır ve iki farklı modele ayrılır: çevrim içi (online) ve çevrim dışı (offline) tele çalışma. Çevrim içi tele çalışma, çalışanın işyerinin ağ sistemine doğrudan ve sürekli bir bağlantı kurarak anlık iletişim ve denetime açık olduğu durumu ifade eder[119]. Buna karşılık, çevrim dışı tele çalışma modelinde ise çalışan, sürekli bir bağlantı olmaksızın işini bağımsız bir şekilde yürütür ve bilgi aktarımını belirli aralıklarla gerçekleştirir. Bu teknik ayrım, iş ilişkisinin özünü oluşturan hukuki bağımlılığı ortadan kaldırmaz[120]. Zira çevrim dışı modelde dahi, işverenin teknik yollarla denetleme ve emir-talimat verme potansiyelini koruduğu hâllerde, iş görme borcunun iş organizasyonu çerçevesinde devam ettiği kabul edilmektedir[121].

---

[117] Aydın, "Tele Çalışma ve Tele Çalışma Çerçeve Avrupa Sözleşmesi", 355-56; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 537.
[118] Mollamahmutoğlu vd., *İş Hukuku*, 469; Senyen Kaplan, *Bireysel İş Hukuku*, 2. bs, 160.
[119] Alp, "Tele Çalışma (Uzaktan Çalışma)", 807-8.
[120] Ziya Erdem, "Tele çalışma", *İstanbul: Filiz Kitabevi*, 2004, 101; Arzu Kuban, "Yeni İstihdam Türleri Bakımından İşçi Kavramı, İş ve Sosyal Güvenlik Hukukunda İşçi ve İşveren Kavramları ve Ortaya Çıkan Sorunlar", *Prof. Dr. Kemal Oğuzman Anısına, İstanbul Barosu-Galatasaray Üniversitesi, İstanbul*, 1997, 59; Dulay, *Türk İş Hukukunda Evde Çalışma*, 106.
[121] Dulay, *Türk İş Hukukunda Evde Çalışma*, 107.

2.2.5.5. Ürün Arzı ve Hizmet Arzı Esaslı Tele Çalışma

Tele çalışma modelleri, yürütülen ekonomik faaliyetin niteliğine göre sınıflandırılmaktadır. Zira bu nitelik, işin yapısını ve performans değerlendirme metriklerini doğrudan belirleyici niteliktedir. Bu bağlamda, tele çalışma temel olarak "ürün arzı esaslı" ve "hizmet arzı esaslı" olmak üzere ikiye ayrılmaktadır. Ürün arzı esaslı tele çalışma, genellikle somut ve ölçülebilir bir çıktının hedeflendiği işleri kapsamaktadır. Örneğin, telefon aracılığıyla satış yapan bir çalışanın performansı, başarılı görüşme sayısı, bu görüşmelerin satışa dönüştürülme oranı veya belirlenen ciro hedeflerine ulaşma gibi nicel ve somut kriterlere dayanılarak kolayca ölçülebilir[122]. Buna karşılık, hizmet arzı esaslı tele çalışmada odak noktası belirli bir hizmetin sunulmasıdır. Bu hizmetler, sabit bir mekândan (ev, tele merkez vb.) veya mobil olarak sunulabilir, performans değerlendirmesi ise genellikle hizmetin kalitesi gibi daha niteliksel unsurları içerebilir[123].

2.2.6. Tele Çalışmaya İlişkin Hukuki Çerçeve

2.2.6.1. Uluslararası Hukuk Düzenlemeleri

2.2.6.1.1. Uluslararası Çalışma Örgütü Düzenlemeleri

Uluslararası Çalışma Örgütü, evde çalışmanın kendine özgü koşullarını ve işçilerin korunma ihtiyacını dikkate alarak 1996 yılında 177 sayılı Evde Çalışma Sözleşmesi ile 184 sayılı Tavsiye Kararı'nı kabul etmiştir[124]. Bu düzenlemeler, evde çalışmaya ilişkin ilk uluslararası normatif kaynaklar olup eşit muamele, iş sağlığı ve güvenliği, sendikal haklar, ücret, sosyal güvenlik ve denetim gibi temel çalışma haklarını kapsamaktadır[125]. Her ne kadar söz konusu belgeler klasik anlamda ev merkezli üretim

---

[122] Gizem Tan, "Atipik İş Sözleşmelerinden Evde Çalışma ve Tele Çalışma" (Yayınlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi, 2007), 54.
[123] Gizem Tan, "Atipik İş Sözleşmelerinden Evde Çalışma ve Tele Çalışma", 54-55; Murat İkizler, "Türk Hukukunda Esnek Çalışma", *Adalet Yayınevi*, 2012, 191; Kutlu, *İş Hukukunda Tele Çalışma*, 62-63.
[124] Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 156-57; Beyza İnal, "Uzaktan Çalışma" (Başkent Üniversitesi Sosyal Bilimler Enstitüsü, 2021), 31 vd.; Dulay, *Türk İş Hukukunda Evde Çalışma*, 44.
[125] Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 156-57; Kandemir, "Evde Çalışma ve 6098 Sayılı Türk Borçlar Kanunu'nun Evde Hizmet Sözleşmesine İlişkin Hükümleri", 50; Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 563-64.

faaliyetlerini hedef alsa da özellikle bilgi ve iletişim teknolojilerinin gelişimiyle yaygınlaşan tele çalışma uygulamaları açısından da öğretide dolaylı bir uygulama alanı buldukları ifade edilmektedir. Tele çalışma sözleşmesinin, işin ifa edildiği yer konusunda esnek bir çerçeve sunması, ilgili uluslararası belgelerde düzenlenen asgari koruma standartlarının, evde gerçekleştirilen tele çalışma hâllerini de kapsayacak şekilde yorumlanması gerektiği sonucunu doğurmaktadır[126]. Türkiye henüz 177 sayılı Sözleşme'yi onaylamamış olmakla birlikte, iç hukukta yapılan düzenlemelerde Sözleşme'de öngörülen ilkelere büyük ölçüde yer verildiği görülmektedir[127].

2.2.6.1.2. Avrupa Birliği Düzenlemeleri

Avrupa Birliği düzeyinde tele çalışmaya ilişkin hukuki çerçeve, büyük ölçüde sosyal tarafların (işçi ve işveren konfederasyonları) diyalog ve uzlaşısı temelinde şekillenmiştir. Bu yaklaşımın en somut örneği, 2002 yılında Avrupa Birliği sosyal ortakları tarafından imzalanan Tele Çalışma Çerçeve Anlaşması'dır. Anlaşma'nın 2. maddesi çerçevesinde *"tele çalışma, işverene ait işyerinde de gerçekleştirilebilecek bir işin, bilgi teknolojileri kullanılarak ve düzenli bir biçimde işyeri dışında ifa edildiği bir iş organizasyonu"* olarak düzenlenmiştir. Anlaşma çerçevesinde tele çalışma, evde çalışmadan farklı olarak düzenlenmiş olup, işin fiziksel olarak işyeri sınırlarında gerçekleştirilebilme imkânına sahip olmasına rağmen, bilgi teknolojileri aracılığıyla sürekli olarak işyeri dışında organize edilmesi ve ifa edilmesi temeline dayanmaktadır[128].

Avrupa Tele Çalışma Çerçeve Anlaşması, iş organizasyonunun modernleştirilmesi ve esnek çalışma düzenlemelerinin yaygınlaştırılması amacıyla işçi ve işveren temsilcileri tarafından kabul edilmiş olup, tele çalışmanın gönüllülük esasına dayalı niteliğinden başlayarak, eşitlik ilkesinin korunması, veri koruma yükümlülükleri, iş

---

[126] Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 7; Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 50; Kutlu, *İş Hukukunda Tele Çalışma*, 102-3.

[127] Şanlı, "İş Hukukunda Uzaktan Çalışma", 22; Günay, *Türk Hukukunda ve Karşılaştırmalı Hukukta Evde Çalışma*, 390.

[128] Çerçeve Anlaşması, tele çalışmanın hem işyeri fiziki sınırları dışında hem de işverenin işyerinde icra edilebilir nitelikte olmasını bir gereklilik olarak vurgulamaktadır. Türk hukukunda ise bu şart yer almaz; işin yalnızca işyeri dışında, bilgi teknolojileri aracılığıyla yürütülmesi yeterlidir. Ancak her iki yasal çerçevede de çalışanın işyeriyle düzenli bağını sürdürmesinin, tele çalışmanın verimliliği açısından ortak bir unsur olduğu kabul edilmektedir. Bknz. Çelik vd., *İş Hukuku Dersleri*, 218; Aydın, *Bireysel İş Hukuku*, 125.

sağlığı ve güvenliği, ekipman temini, çalışma koşulları, toplu haklara erişim ile eğitim ve mesleki gelişim olanaklarına eşit katılım gibi çeşitli yönlerini düzenlemektedir. Çerçeve Anlaşma ülkemiz tarafından henüz onaylanmamış olsa da Anlaşma'nın hükümleri doğrultusunda yasal düzenlemelerin hayata geçirilmesi, işçilerin etkin bir şekilde korunması açısından büyük önem taşımaktadır.

Tele çalışmanın özellikle pandemi sonrası dönemde yaygınlaşarak sınır ötesi bir boyut kazanması, sosyal güvenlik sistemlerinin koordinasyonu gibi spesifik hukuki sorunları da beraberinde getirmiştir. Bu soruna çözüm bulmak amacıyla Avrupa Birliği, 883/2004 sayılı Tüzük uyarınca Sürekli Sınır Ötesi Tele Çalışma Durumlarında Uygulanmasına İlişkin Çerçeve Anlaşma'yı yürürlüğe koymuştur[129]. Anlaşma, çalışanların sosyal güvenlik haklarını korumayı ve yasal belirsizlikleri gidermeyi amaçlamaktadır. Anlaşma, işverenin bulunduğu ülkeden farklı bir ülkede tele çalışma yapılması durumunda hangi ülke mevzuatının uygulanacağına dair net kurallar getirmektedir. Buna göre, çalışma süresinin %50'sinden azının sınır ötesi tele çalışmaya ayrılması hâlinde işverenin bulunduğu ülke mevzuatının uygulanmasını öngörmektedir. Azami üç yıl geçerli olabilen istisnalara başvuru yoluyla olanak tanıyan anlaşma, imzacı devletler arasında sosyal güvenlik koordinasyonunu ve bireylerin haklarının sürekliliğini sağlamayı hedeflemektedir[130].

---

[129] Avrupa Birliği Sosyal Güvenlik Sistemlerinin Koordinasyonuna İlişkin 883/2004 sayılı Avrupa Parlamentosu ve Konseyi Tüzüğü'nün 16. maddesinin birinci fıkrası, sosyal güvenlik sistemlerine ilişkin genel kurallardan sapmaya imkân tanıyan istisnai bir düzenleme niteliğindedir. Bu hüküm uyarınca, bir veya birden fazla üye devletin yetkili makamları, belirli bir kişinin özel durumunu göz önünde bulundurarak ve kişinin yararına olmak kaydıyla, Tüzüğün 11. ila 15. maddeleri arasında yer alan temel düzenlemelerden farklı bir uygulamayı kararlaştırabilir. Anılan maddelerde, bir kişinin sadece tek bir üye devletin sosyal güvenlik mevzuatına tabi olması gerektiği (madde 11), birden fazla ülkede çalışanlar için geçerli kurallar (madde 13) ve kamu görevlileri, denizciler gibi özel meslek gruplarına özgü hükümler düzenlenmektedir. Özellikle sürekli sınır ötesi tele çalışma gibi, bir çalışanın işverenin bulunduğu ülkeden farklı bir ülkeden uzun süreli ve düzenli olarak çalıştığı durumlarda, bu tür istisnai uygulamalar büyük önem taşımaktadır. Zira mevcut düzenlemeler, klasik iş modelleri temel alınarak oluşturulduğundan, tele çalışmanın sınır ötesi boyutlarını karşılamakta yetersiz kalabilmektedir. Bu bağlamda, 16(1) maddesine dayanılarak Avrupa Birliği nezdinde yapılan Çerçeve Anlaşma, sürekli sınır ötesi tele çalışmanın sosyal güvenlik bakımından hangi ülke mevzuatına tabi olacağına ilişkin yeknesak ve esnek bir uygulama zemini oluşturmayı amaçlamaktadır. Bknz. European Parliament and Council, "Regulation (EC) No 883/2004 of 29 April 2004 on the Coordination of Social Security Systems", Official Journal of the European Union, 30 Nisan 2004, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0883R(01); European Commission, *Practical Guide: The Applicable Legislation in the EU, EEA and in Switzerland* (Directorate-General for Employment, Social Affairs and Inclusion, 2022), https://webgate.ec.europa.eu/circabc-ewpp/d/d/workspace/SpacesStore/49cd18c1-5478-4e15-98dc-c7aa6f01a823/file.bin.

[130] European Commission, *Framework Agreement on the Application of Article 16(1) of Regulation (EC) No 883/2004 in Cases of Habitual Cross-Border Telework* (European Commission, 2023),

2.2.6.2. Tele Çalışmaya İlişkin Ulusal Düzenlemeler

Türk İş Hukuku'nda tele çalışmaya ilişkin düzenlemeler, özellikle 2016 yılında 4857 sayılı İş Kanunu'nda yapılan değişikliklerle birlikte yasal bir çerçeveye kavuşmuştur. Bu düzenlemeyle kanun koyucu hem geleneksel evde çalışmayı hem de teknoloji odaklı tele çalışma modelini "uzaktan çalışma" başlığı altında tek bir çatı altında toplamıştır. Bu yasal reformun temelini İş Kanunu'nun 14. maddesi oluştururken, uygulamanın usul ve esaslarını belirleme görevi ise Çalışma ve Sosyal Güvenlik Bakanlığı tarafından çıkarılan Uzaktan Çalışma Yönetmeliği'ne bırakılmıştır. Dolayısıyla günümüzde tele çalışma ilişkilerine uygulanacak temel hukuki kaynakları, İş Kanunu'nun anılan madde hükmü ve bu maddeye dayanarak hazırlanan Yönetmelik oluşturmaktadır.

Tele çalışma sözleşmelerine uygulanacak hukuk kurallarının hiyerarşisinde, birincil kaynak 4857 sayılı İş Kanunu hükümleridir. Kanun'da özel bir düzenleme bulunmayan hâllerde ise genel kanun niteliğindeki 6098 sayılı Türk Borçlar Kanunu'nun ilgili hükümleri tamamlayıcı olarak devreye girecektir[131]. Her ne kadar İş Kanunu'nun 4. maddesi, bazı faaliyetleri kendi kapsamı dışında tutarak doğrudan Türk Borçlar Kanunu'na tabi kılsa da bilgi ve iletişim teknolojileri kullanılarak yürütülen tele çalışma bu istisnalar kapsamında değerlendirilmeyecektir[132].

Mevcut yasal düzenlemenin yapısı, öğretide önemli eleştirilere konu olmaktadır. Tele çalışmanın, İş Kanunu'nun "çağrı üzerine çalışma" gibi farklı bir atipik çalışma türünü düzenleyen 14. maddesi altında ele alınması, bu eleştirilerin temelini oluşturmaktadır. Zira tele çalışma, mekânsal farklılıkları ve iş görme ediminin teknolojiyle ifası gibi kendine özgü dinamikleriyle diğer çalışma modellerinden belirgin biçimde ayrılırken, mevcut düzenlemenin bu özgün yapıyı tam olarak karşılayamadığı ve hukuki bir boşluk yarattığı ileri sürülmektedir.[133].

---

https://socialsecurity.belgium.be/sites/default/files/content/docs/en/international/framework_agreement_on_cross-border_telework.pdf.

[131] Süzek ve Başterzi, *İş Hukuku*, 291; Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 162-64.

[132] Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 162-64.

[133] Öğretideki eleştiriler için bknz. Ergüneş Emrağ, "4857 Sayılı İş Kanunun Değişik 14. Maddesi Işığında Tele Çalışma", 1420; Alp, "Tele Çalışma (Uzaktan Çalışma)", 826-27; Alp, "Tele Çalışma (Uzaktan Çalışma)", 827; Kutlu, *İş Hukukunda Tele Çalışma*, 113.

İş Kanunu'nun işaret ettiği bu çerçevenin usul ve esasları, Uzaktan Çalışma Yönetmeliği ile detaylandırılmıştır. Yönetmelik, öncelikle iş sözleşmesinin yazılı şekilde yapılmasını ve sözleşmede işin tanımı, süresi, yeri, ücret, ekipman ve iletişim kuralları gibi temel unsurların yer almasını zorunlu kılmaktadır. Çalışma mekânına, malzeme teminine ve üretim maliyetlerine ilişkin giderlerin karşılanma usulünün taraflarca birlikte belirleneceği düzenlenmektedir. Ayrıca, çalışma sürelerinin sözleşmede belirtilmesi ve fazla çalışmanın işçinin kabulüne bağlanması gibi konuları netleştirmektedir[134]. Yönetmelik aynı zamanda, mevcut bir iş sözleşmesinin uzaktan çalışmaya dönüştürülmesi için işçinin yazılı talepte bulunması ve işverenin bu talebi 30 gün içinde yanıtlaması gibi uzaktan çalışmaya geçiş süreçlerini de ayrıntılı olarak düzenlemektedir[135].

Tele çalışmaya doğrudan odaklanmasa da kapsayıcı nitelikte olan bir diğer ulusal düzenleme, Ekranlı Araçlarla Çalışmalarda Sağlık ve Güvenlik Önlemleri Hakkında Yönetmeliktir[136]. Bu Yönetmelik, ekranlı araçlarla yürütülen çalışmalarda asgari sağlık ve güvenlik önlemlerini belirlemeyi amaçlamakta olup, 6331 sayılı İş Sağlığı ve Güvenliği Kanunu'na dayanılarak hazırlanmıştır. Söz konusu düzenleme, işverenlerin çalışanların sağlık ve güvenliğini korumak amacıyla almaları gereken önlemleri ayrıntılı şekilde ortaya koymaktadır. Yönetmelik kapsamında, işverenin risk değerlendirmesi yapma, çalışanları bilgilendirme ve eğitme, uygun ekipman sağlama ve çalışma ortamını ergonomik ve güvenli hâle getirme yükümlülükleri açıkça düzenlenmiştir. Ayrıca, göz sağlığı kontrolleri, çalışma sürelerinin planlanması ve mola aralıkları gibi hususlara özel önem verilmektedir. Bu kapsamda hem teknik hem de organizasyonel tedbirler aracılığıyla iş ilişkisi kapsamında iş sağlığı ve güvenliğinin sağlanması, dolayısıyla çalışanların korunması ve iş verimliliğinin artırılması hedeflenmektedir.

---

[134] Süzek ve Başterzi, *İş Hukuku*, 285-86.
[135] Ömer Ekmekçi ve Esra Yiğit, Bireysel İş Hukuku Dersleri, 6. bs (Onikilevha, 2024), 89-92.
[136] Ekranlı Araçlarla Çalışmalarda Sağlık ve Güvenlik Önlemleri Hakkında Yönetmelik, R.G. 23.12.2013, Sayı: 28861.

2.2.7. Tele Çalışmada Tarafların Hak ve Yükümlülükleri

Tele çalışma ilişkisi, taraflara hem klasik iş sözleşmesinden kaynaklanan temel hak ve borçları yükler hem de bu çalışma biçiminin kendine özgü yapısından doğan yeni hukuki dinamikleri beraberinde getirir. Bu kapsamda işçinin sadakat ve işverenin talimatlarına uyma borcuna karşılık, işverenin de ücret ödeme, eşit davranma ve işçiyi gözetme gibi temel yükümlülükleri prensipte devam etmekle beraber[137] öğretide, uzaktan çalışmaya ilişkin düzenlemelerin özellikle eşit davranma ve iş sağlığı güvenliği borçlarını öne çıkardığı, bular dışındaki işveren yükümlülüklerinde kayda değer bir değişiklik yaratmadığı ifade edilmektedir[138]. Ancak bu yaklaşım, tele çalışmanın iş ilişkisine getirdiği niteliksel dönüşümü tam olarak yansıtmamaktadır. Her ne kadar kanuni düzenlemeler mevcut borçların içeriğini detaylı olarak yeniden şekillendirmese de tele çalışmanın kendine özgü yapısı bu borçların kapsamını ve uygulanma biçimini değiştirmektedir. Özellikle işverenin, işçinin çalışma ortamı üzerindeki doğrudan denetim imkânının azalması ve buna karşılık dijital gözetim araçlarının kullanımının artması, işverenin gözetme borcu ile kişisel verileri koruma yükümlülüğünü niceliksel değil, niteliksel olarak dönüştürmektedir. Dolayısıyla, geleneksel işveren yükümlülüklerinin bu yeni bağlamda nasıl yorumlanması gerektiğinin incelenmesi önem arz etmektedir. Bu çerçevede, takip eden bölümlerde tarafların hak ve borçları, tele çalışmanın değiştirdiği bu dinamikler göz önünde bulundurularak etraflıca ele alınacaktır.

2.2.7.1. İşçinin Yükümlülükleri

Tele çalışma ilişkisinde de işçinin, iş sözleşmesinden doğan iş görme, işverenin talimatlarına uyma, sadakat ve rekabet etmeme gibi temel borçları, genel hükümler çerçevesinde geçerliliğini korumaktadır. Mevzuatımızda, Uzaktan Çalışma Yönetmeliği'nin veri korumaya ilişkin 11. maddesinin 3. fıkrası dışında, tele çalışanın bu sorumluluklarına özgü özel bir düzenleme bulunmamaktadır[139]. Ancak bu durum, söz konusu borçların klasik iş ilişkisindekiyle birebir aynı şekilde uygulandığı anlamına gelmemektedir. Tele çalışmanın mekândan ve doğrudan denetimden

---

[137] Senyen Kaplan, *Bireysel İş Hukuku*, 2. bs, 161; Kutlu, *İş Hukukunda Tele Çalışma*, 304.
[138] Mollamahmutoğlu vd., İş Hukuku, 471.
[139] Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 97-155; Kutlu, *İş Hukukunda Tele Çalışma*, 303-4.

bağımsız yapısı, bu temel yükümlülüklerin içeriğini ve uygulanma biçimini niteliksel olarak dönüştürmektedir. Bu nedenle, söz konusu borçların tele çalışmanın kendine özgü dinamikleri içinde nasıl yorumlanması gerektiğinin incelenmesi önem taşımaktadır.

2.2.7.1.1. İş Görme Borcu

Tele çalışma ilişkisinde de işçinin, işini özenle ve bizzat yerine getirme şeklindeki temel iş görme borcu geçerliliğini korumaktadır[140]. Ancak, işin fiziki olarak işyeri sınırları dışında ve doğrudan denetimden uzakta yapılması, bu borcun kapsamının ve sınırlarının belirsizliğe yer bırakmayacak şekilde tanımlanmasını zorunlu kılmaktadır. Bu bağlamda, Uzaktan Çalışma Yönetmeliği, işçinin sorumluluklarının netleştirilmesi ve ispat kolaylığı sağlanması amacıyla, yerine getirilecek görevlerin kapsamının iş sözleşmesinde açıkça tanımlanmasını şart koşmaktadır. Benzer şekilde Yönetmelik, işveren tarafından sağlanan araç ve malzemelerin kullanım, bakım ve onarımına ilişkin esasların da çalışana net bir şekilde bildirilmesini zorunlu tutmaktadır[141].

Uluslararası düzenlemeler de bu yaklaşımı destekler niteliktedir. Her ne kadar Avrupa Tele Çalışma Çerçeve Anlaşması, iş görme borcunun kendisine ilişkin genel kurallar dışında özel bir hüküm getirmese de bu borcun ifasıyla doğrudan bağlantılı olan yükümlülüklere odaklanmaktadır. Anlaşma, tele çalışanın kendisine emanet edilen iş ekipmanlarını dikkatli kullanma, koruma ve interneti yasa dışı amaçlarla kullanmama yükümlülüğünü vurgularken, aynı zamanda işveren tarafından bildirilen veri koruma kurallarına tam uyum göstermesi gerektiğini de açıkça belirmektedir[142]. Dolayısıyla hem ulusal hem de uluslararası düzenlemeler, iş görme borcunun etkin bir şekilde ifasını, görevin kapsamının netleştirilmesi ve işçinin kendisine emanet edilen araçları ve verileri özenle kullanması şartlarına bağlayarak güvence altına almayı amaçlamaktadır.

---

[140] Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 554; Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 97-98; Kara, *Uzaktan Çalışmada İş Sağlığı ve Güvenliğinin Hukuki Boyutu*, 20.
[141] Kutlu, *İş Hukukunda Tele Çalışma*, 304-5; Kara, *Uzaktan Çalışmada İş Sağlığı ve Güvenliğinin Hukuki Boyutu*, 12.
[142] Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 115-16; Erkanlı Başbüyük, "Uzaktan Çalışmanın Bir Türü Olarak Tele Çalışmada İşçinin Dinlenme Hakkı", 666.

2.2.7.1.2. İşverenin Emir ve Talimatlarına Uyma Borcu

Tele çalışmada işçi ile işveren arasındaki hukuki bağımlılığın en temel yansımalarından biri, işçinin, işverenin yönetim hakkı kapsamında verdiği emir ve talimatlara uyma borcudur. Tele çalışma ilişkisi çerçevesinde işverenin yönetim hakkı, çalışanlara hem işin ifasına hem de işyerindeki davranışlara ilişkin talimatlar verme yetkisini içermektedir[143]. Bu kapsamda tele çalışanlar, işverenin verdiği talimatlara dürüstlük kuralları çerçevesinde riayet etmekle yükümlüdürler[144]. Bu yükümlülüğün hukuki dayanağı, 6098 sayılı Türk Borçlar Kanunu'nun 399. ve 400. maddelerinde düzenlenmiş olup, yalnızca Anayasa'ya, iş mevzuatına, toplu iş sözleşmesine ve bireysel iş sözleşmesine aykırı olmayan talimatlar için geçerlilik taşır. İşverenin yönetim hakkı çerçevesindeki talimatlar, bir yandan işin teknik olarak nasıl yürütüleceğini, diğer yandan işçinin davranış standartlarını belirlemeye yöneliktir. Özellikle tele çalışmada, işin kapsamı, süresi, yürütüleceği yer, ücretlendirme esasları ve işveren tarafından sağlanan araçlara ilişkin hükümlerin açıkça iş sözleşmesinde düzenlenmesi hem hukuki belirliliğin sağlanması hem de özel hayat ile iş yaşamı arasındaki dengenin korunması açısından önem arz etmektedir[145].

2.2.7.1.3. Sadakat Borcu

İşçinin iş görme borcunu dürüstlükle yerine getirmesini güvence altına alan sadakat borcu, işverenin meşru menfaatlerini koruma ve ona zarar verebilecek davranışlardan kaçınma yükümlülüğünü ifade etmektedir[146]. 6098 sayılı Türk Borçlar Kanunu'nun 396. maddesine dayanan bu yükümlülük, tele çalışma bağlamında özellikle işverenin sağladığı ekipmanların korunması ve işletme verilerinin gizliliğinin sağlanması açısından önem kazanmaktadır. Tele çalışmada işin fiziki olarak işyeri sınırları dışında

---

[143] Kara, *Uzaktan Çalışmada İş Sağlığı ve Güvenliğinin Hukuki Boyutu*, 22; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 33-34.

[144] Arzu Arslan Ertürk, "Yeni Türk Borçlar Kanununun Genel Hizmet Sözleşmesinin Kurulmasına ve Tarafların Borçlarına İlişkin Esasları", *6098 Sayılı Türk Borçlar Kanunu Hükümlerinin Değerlendirilmesi Sempozyumu, Sempozyum No. 3, Prof. Dr. Cevdet Yavuz'a Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 2011, 549; Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 158.

[145] Kutlu, *İş Hukukunda Tele Çalışma*, 315-18; Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 33-47.

[146] Gülsevil Alpagut, "İçinin Sadakat Borcu ve Türk Borçlar Kanunu ile Getirilen Düzenlemeler", *Sicil İş Hukuku Dergisi*, sy 25 (2012): 24; Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 108.

yürütülmesi, işverenin denetim yetkisini sınırladığından, sadakat borcunun kapsamı sözleşmelerle açıkça belirlenmeli; getirilen kurallar ise dürüstlük ilkesine ve kişilik haklarına uygun olmalıdır[147].

Tele çalışmada işverenin bilgi sistemlerine dışarıdan erişim sağlanması, işletme verilerinin gizliliği ve güvenliği açısından önemli riskler doğurmaktadır[148]. Özellikle evden çalışma modelinde, verilerin işverenin kontrolü dışındaki ortamlarda işlenmesi, siber saldırılara açık bir yapı oluşturmaktadır. Bu nedenle hem teknik hem de organizasyonel güvenlik önlemleri alınması zorunludur. Avrupa Birliği düzenlemeleri ve mukayeseli hukuk bağlamında ele alındığında işveren; veri koruma politikalarını belirlemek, gerekli önlemleri almak ve tele çalışanı bilgilendirmekle yükümlüdür. Tele çalışanın da bu kurallara uyması ve verilerin korunmasına ilişkin özen yükümlülüğünü yerine getirmesi beklenmektedir[149]. Uzaktan Çalışma Yönetmeliği'nde de bu husus düzenlenmiş, 11. maddenin üçüncü fıkrasında "*Verilerin korunması amacıyla işveren tarafından belirlenen işletme kurallarına uzaktan çalışanın uyması zorunludur."* şeklinde belirtilmiştir. Düzenleme, işletmeler açısından veri koruma hükümleri içermesi nedeniyle önemli bir adımdır. Ancak, işçinin kişisel verilerinin korunmasına ilişkin özel ve ayrıntılı bir hükme yer verilmemiş olması, bu düzenlemeyi eksik kılmaktadır. Bu durum, özellikle uzaktan çalışma ilişkilerinde kişisel verilerin işlenme riskinin arttığı dikkate alındığında, önemli bir boşluk olarak görülmelidir[150].

- **Rekabet Etmeme Borcu**

İşçinin sadakat borcunun iş sözleşmesi sona erdikten sonraki bir yansıması olan rekabet etmeme borcu, özellikle tele çalışma modelinde işletme sırlarının korunması açısından kritik bir hukuki mekanizma olarak ortaya çıkmaktadır. Tele çalışanın, işverenin dijital sistemlerine sahip olduğu geniş erişim, işverenin müşteri çevresi, ticari sırları veya üretim bilgileri gibi kritik verileri depolama ve daha sonra rakip bir

[147] Dulay, Türk İş Hukukunda Evde Çalışma, 184; Kutlu, İş Hukukunda Tele Çalışma, 318-20.
[148] Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 110-11; Dulay, *Türk İş Hukukunda Evde Çalışma*, 46.
[149] Ayrıntılar için bknz. Kutlu, *İş Hukukunda Tele Çalışma*, 327-36.
[150] Kutlu ve Uçar, "Tarafların Hak ve Borçları Kapsamında Koronavirüs Pandemisinde Uzaktan Çalışma", 289; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 88.

faaliyette kullanma riskini artırmaktadır. Türk Borçlar Kanunu'na göre, işçinin bu tür bilgilere erişimi ve bu bilgileri kullanarak işverene önemli ölçüde zarar verme potansiyeli varsa, taraflar arasında yazılı bir sözleşmeyle rekabet yasağı kararlaştırılabilir[151].

Ancak bu yasak, mutlak ve sınırsız değildir; işçinin ekonomik geleceğini hakkaniyete aykırı şekilde kısıtlayamaz. Bu nedenle rekabet yasağı, süre, yer ve konu bakımından ölçülü olmalı ve genellikle iki yılı aşmamalıdır; hâkimin aşırı nitelikteki sınırlamaları daraltma yetkisi bulunmaktadır. Bu noktada tele çalışma, bu borcun uygulanmasında kendine özgü bir zorluk yaratmaktadır[152]. Genellikle teknik bilgiye sahip olan ve bu nedenle rekabet yasağı şartlarını taşıyan tele çalışanlar için getirilecek yasağın, tele çalışmanın zaman ve mekândan bağımsız doğası gereği özellikle "yer" bakımından sınırlandırılması, önemli bir hukuki belirsizliğe yol açabilmektedir[153].

2.2.7.2. İşverenin Yükümlülükleri

Tele çalışma ilişkisinin karşılıklı niteliği gereği, bir önceki bölümde incelenen işçinin borçlarına, işverenin temel yükümlülükleri karşılık gelmektedir. Tele çalışma, işverenin iş sözleşmesinden doğan temel yükümlülüklerini ortadan kaldırmamakta; aksine, bu çalışma modelinin kendine özgü yapısı, söz konusu yükümlülüklerin kapsamını ve uygulanma biçimini yeniden şekillendirmektedir. Bu çerçevede, ücret ödeme ile işin ifası için gerekli malzeme ve giderleri karşılama gibi temel edim yükümlülükleri geçerliliğini korurken, eşit davranma ilkesi de uzaktan ve ofiste çalışanlar arasında bir ayrım yapılmamasını güvence altına almaktadır. İşverenin en geniş kapsamlı borcu olan işçiyi koruma ve gözetme yükümlülüğü ise, tele çalışmanın getirdiği yeni riskler doğrultusunda bir çatı yükümlülük olarak öne çıkmaktadır. Bu temel borç, fiziksel denetimin azaldığı bu yeni düzende, özellikle iş sağlığı ve güvenliğini sağlama, özel hayatın gizliliğine ve kişisel verilerin korunmasına riayet etme ve dijital çağın bir gereği olarak ulaşılabilir olmama hakkına saygı gösterme gibi

---

[151] Alpagut, "İçinin Sadakat Borcu ve Türk Borçlar Kanunu ile Getirilen Düzenlemeler", 26; Dulay, *Türk İş Hukukunda Evde Çalışma*, 198.
[152] Sarper Süzek, "Yeni Türk Borçlar Kanunu Çerçevesinde İşçinin Rekabet Etmeme Borcu", *Journal of Istanbul University Law Faculty* 72, sy 2 (2014): 460, https://dergipark.org.tr/en/download/article-file/97936.
[153] Kutlu, *İş Hukukunda Tele Çalışma*, 348-56.

alt yükümlülükler aracılığıyla daha teknoloji odaklı ve kapsamlı bir anlam kazanmaktadır. Takip eden bölümlerde, işverenin bu temel ve alt yükümlülükleri, tele çalışma düzenlemeleri ışığında ayrıntılı olarak incelenecektir.

2.2.7.2.1. Ücret Ödeme Yükümlülüğü

İşverenin temel borçlarından olan ücret ödeme yükümlülüğü, tele çalışma özelinde hem 4857 sayılı İş Kanunu'nun 14. maddesi hem de Uzaktan Çalışma Yönetmeliği'nin 5. maddesi tarafından güvence altına alınmıştır. Bu hükümler uyarınca, ücret ve ücretin ödenmesine ilişkin esasların iş sözleşmesinde açıkça düzenlenmesi zorunludur. Ancak bu yasal çerçeveye rağmen, işin niteliği ve denetlenebilirliği, ücretlendirme sisteminin türünü doğrudan etkilemektedir. Özellikle evde tele çalışma modelinde, pek çok ülkede olduğu gibi, performansı ölçmenin daha kolay olduğu gerekçesiyle parça başı çalışma esasına dayalı ücretlendirmenin öne çıktığı görülmektedir. Bu durum, uzaktan çalışanların ücretlerinin, aynı işi fiziki olarak işyerinde yapan emsallerine kıyasla daha düşük seviyelerde kalması riskini beraberinde getirmektedir[154]. Parça başı ücretlendirme sistemi, özellikle veri girişi veya çeviri gibi çıktısı kolayca ölçülebilen işlerde uygulanabilir olsa da çalışanları yeterli bir gelir düzeyine ulaşabilmek adına uzun saatler boyunca yoğun bir şekilde çalışmaya itme potansiyeli taşır. Bu riski bertaraf etmek için, çalışma sürelerinin yazılım sistemleri aracılığıyla güvenilir bir şekilde takip edilebildiği durumlarda, daha adil bir yaklaşım olan "zamana dayalı" ücretlendirme sisteminin tercih edilmesi yerinde olacaktır. Çalışma süresinin takibinin mümkün olmadığı ve parça başı ücretin zorunlu olduğu hâllerde ise, bu sistemin yol açabileceği aşırı çalışma risklerini sınırlandırmak amacıyla teknolojik izleme araçlarından veya bilirkişi incelemelerinden yararlanılması düşünülebilir[155].

[154] Tele çalışmada parça başına ücretin ayrıntıları için bknz. Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)".
[155] Kutlu, *İş Hukukunda Tele Çalışma*, 357-61.

2.2.7.2.2. İşin İfasında Gerekli Malzeme ve Giderlerin Karşılanması Yükümlülüğü

İşverenin tele çalışma ilişkisi kapsamındaki bir diğer yükümlülüğü, işin ifası için gereken ekipman ve giderleri karşılamaktır[156]. Bu yükümlülük, İş Kanunu'nun 14. maddesinde, tele çalışma sözleşmelerinde gerekli malzemelerin sağlanmasına dair düzenlemeler yapılması gerektiği belirtilerek, bu ekipmanların iş sağlığı ve güvenliği açısından önemi vurgulanarak ele alınmıştır. Ancak söz konusu maddede, işverenin ekipman teminine dair açık ve net bir zorunluluğa yer verilmemiştir. Bu yaklaşım, her bir çalışan için ayrı bir çalışma mekânı donatmanın geleneksel işyerine göre daha maliyetli olabilmesinden kaynaklanmaktadır[157]. Buna karşın, Uzaktan Çalışma Yönetmeliği'nde durum daha açık biçimde düzenlenmiştir. Yönetmeliğe göre, "*Uzaktan çalışanların mal ve hizmet üretiminde ihtiyaç duyacağı malzeme ve araçların, iş sözleşmesinde aksi kararlaştırılmadıkça işveren tarafından sağlanması esastır"*. Bu ifade, aksi yönde sözleşmesel bir düzenleme bulunmadığı takdirde işverenin ekipman sağlama yükümlülüğünü net bir şekilde göstermektedir[158].

Uluslararası hukuk açısından ise bu konu, Tele Çalışma Çerçeve Anlaşması'nın 7. maddesinde de ayrıntılı olarak düzenlenmiştir. Anlaşma'nın 7. maddesine göre, tele çalışmaya başlamadan önce iş ekipmanlarıyla ilgili sorumlulukların ve maliyetlerin açık şekilde belirlenmesi gerekmektedir. Genel ilke olarak, düzenli tele çalışmada ihtiyaç duyulan ekipmanın temini, kurulumu ve bakımından işveren sorumludur. Ancak tele çalışanın kendi ekipmanını kullanmayı tercih etmesi hâlinde, işverenin bu yükümlülüğü sona ermektedir. Tele çalışmanın düzenli şekilde yürütülmesi durumunda ise işveren, özellikle iletişim giderleri başta olmak üzere tele çalışmadan doğrudan doğan maliyetleri karşılamak veya tazmin etmekle yükümlüdür. Ayrıca işveren, çalışanlara uygun teknik destek hizmeti sunmakla, çalışan tarafından kullanılan ekipmanın veya verilerin zarar görmesi ya da kaybolması durumunda ulusal

---

[156] Civan, "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)", 554; Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 132-68.
[157] Kara, *Uzaktan Çalışmada İş Sağlığı ve Güvenliğinin Hukuki Boyutu*, 12.
[158] Öğretide işin ifasında gerekli malzeme ve giderlerin karşılanmasının zorunluluğuna ilişkin görüşler için bknz. Kutlu, *İş Hukukunda Tele Çalışma*, 368-74; Kara, *Uzaktan Çalışmada İş Sağlığı ve Güvenliğinin Hukuki Boyutu*, 12.

mevzuat ve toplu iş sözleşmeleri çerçevesinde ortaya çıkan maliyetleri karşılamakla sorumludur.

Tele çalışanların kişisel cihazlarını işin yürütümünde kullanmaları da mümkündür. "Bring Your Own Device" olarak ifade edilen bu yöntem, işverenler tarafından cihaz maliyetlerini azaltmak amacıyla yaygın olarak tercih edilmektedir[159]. Ancak bu uygulama, çalışanlara belirli bir esneklik sağlamakla birlikte, çalışanların ve hatta aile bireylerinin kişisel verilerine işveren tarafından erişim riskini de beraberinde getirmektedir[160]. Ayrıca kişisel cihazların iş amaçlı kullanımı, güncelliğini yitirmiş donanım kullanımı, zayıf şifreleme yöntemleri, güvensiz ağ bağlantıları, kötü amaçlı yazılımlar ve cihazların kaybedilmesi gibi ciddi güvenlik riskleri doğurabilmektedir[161]. Bu nedenle, tele çalışanın kendi cihazını kullanması durumunda dahi işveren, bu risklere karşı tüm idari ve teknik tedbirleri alma yükümlülüğünü taşımaktadır.

2.2.7.2.3. Eşit Davranma Yükümlülüğü

İşverenin tele çalışmada eşit davranma yükümlülüğü, İş Kanunu'nun 14. maddesinin altıncı fıkrasında düzenlenmiştir. Söz konusu hükme göre, işveren, esaslı bir gerekçe bulunmadıkça, iş sözleşmesinin niteliğine dayanarak emsal işçiler arasında ayrımcılık yapamayacak ve çalışanları farklı uygulamalara tabi tutamayacaktır[162]. Avrupa Birliği Tele Çalışma Çerçeve Sözleşmesi'nin 4. maddesi de benzer şekilde, uzaktan çalışan işçilerin, çalışma koşulları açısından, işyerinde fiziken çalışan emsal işçilerle aynı haklardan yararlanmalarını öngörmektedir. Bununla birlikte sözleşme, tele çalışmanın özgün yapısının, taraflara bireysel ve toplu iş sözleşmeleri yoluyla duruma özgü düzenlemeler yapma imkânı tanıdığını da kabul etmektedir[163].

---

[159] Özdemir, "Uzaktan Çalışma Yönetmeliği Karşısında Tele Çalışma", 30-31; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 17.

[160] Isabelle Falque-Pierrotin, Opinion 2/2017 on Data Processing at Work, 17/EN WP 249 (EU Comission Article 29 Data Protection Working Party, 2017), 16-18, https://ec.europa.eu/newsroom/article29/items/610169.

[161] Ayrıca cihaz çalışana ait olsa dahi, işverenin KVKK'nın 12. maddesi gereğince veri güvenliğine ilişkin tedbirleri almakla yükümlü olacağına ilişkin bknz. Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 17.

[162] Süzek ve Başterzi, *İş Hukuku*, 284 vd.; Çelik vd., *İş Hukuku Dersleri*, 223; Mollamahmutoğlu vd., *İş Hukuku*, 469.

[163] Ayrıca Çerçeve Sözleşmenin "işin düzenlenmesi" başlıklı 9. maddesi şu şekilde ifade edilmiştir: *"Tele çalışan kanun, toplu iş sözleşmesi ve işletme kuralları çerçevesinde çalışma sürelerini düzenler.*

İş Kanunu'nun 14. maddesinin altıncı fıkrası, eşit davranma yükümlülüğüne aykırılık teşkil eden farklı işlemleri açıkça yasaklamakla birlikte, bu yasağın ihlali hâlinde doğrudan uygulanacak bir yaptırım mekanizması içermemektedir. Bu nedenle, eşitlik ilkesine aykırı işlemlerin denetiminde ve ihlal hâlinde uygulanacak hukuki yaptırımlar açısından İş Kanunu'nun 5. maddesinde düzenlenen ayrımcılık yasağı hükmünün tamamlayıcı ve destekleyici bir düzenleme olarak devreye gireceği öğretide genel kabul görmektedir[164]. Öğretide hâkim olan görüş, uzaktan çalışan işçiler ile işyerinde fiziken çalışan işçiler arasında, özellikle prim ve ikramiye gibi uygulamalar bakımından farklılık yaratılmaması gerektiğini vurgulamaktadır. Ancak tele çalışmanın özelliğinden kaynaklanan farklı uygulamaların, tek başına eşit davranma ilkesine aykırılık teşkil etmeyeceği de kabul edilmektedir[165]. Ek olarak, sonradan uzaktan çalışmaya geçirilen işçiler bakımından da işverenin eşit işlem yükümlülüğünün devam ettiği ifade edilmektedir[166].

2.2.7.2.4. Koruma ve Gözetme Yükümlülüğü

İşverenin, işçiyi koruma ve gözetme yükümlülüğü, tele çalışma ilişkisinin kendine özgü yapısı nedeniyle geleneksel iş ilişkilerine kıyasla daha karmaşık ve çok boyutlu bir nitelik kazanır. Bu durumun temel nedeni, özellikle evden tele çalışma modelinde,

---

Tele çalışana uygulanacak iş yükü ve değerlendirme ölçütleri, işyerinde çalışan karşılaştırılabilir işçiyle denk olmalıdır." Bu hüküm, tele çalışanın işyerinde çalışan diğer işçilerle eşit şekilde muamele görmesini garanti altına almayı amaçlamakta, ancak bu eşitliğin nasıl sağlanacağı ya da hangi önlemlerin alınması gerektiği konusunda ayrıntı sunmamaktadır Sözleşmenin 10. maddesi, tele çalışanların, işyerinde çalışan emsal işçilerle aynı meslek içi eğitim ve kariyer geliştirme imkanlarına sahip olmaları gerektiğini açıkça hükme bağlamaktadır. Bu düzenleme, tele çalışanların bilgi teknolojileri ve iletişim alanında özel eğitim alarak mesleki gelişimlerinin desteklenmesini amaçlamaktadır. Bununla birlikte, eğitim yükümlülüğü yalnızca tele çalışanla sınırlı kalmamakta, aynı zamanda bu çalışma biçiminin yönetimi ve organizasyonu konusunda tele çalışanın üstleri ve çalışma arkadaşlarının da bilgilendirilmesini içermektedir. Bknz. Aydınöz, "İş Hukukunda Tele (Uzaktan) Çalışma", 118.

[164] Çelik vd., *İş Hukuku Dersleri*, 224; Mollamahmutoğlu vd., *İş Hukuku*, 470; İşverenin işçinin uzaktan çalışmaya geçiş talebi karşısında eşit davranma yükümlülüğüne ilişkin bknz. Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 8; Özdemir, "Uzaktan Çalışma Yönetmeliği Karşısında Tele Çalışma", 19.

[165] Çelik vd., *İş Hukuku Dersleri*, 224; Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 198; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 13.

[166] Daha sonra uzaktan çalışmaya geçirilen işçilerin, eşitlik ilkesi çerçevesinde değerlendirilmesine ilişkin tartışmalar için bknz. Çelik vd., *İş Hukuku Dersleri*, 224; Öner Eyrenci vd., *İş Hukuku*, 10. bs (Beta, 2020), 100; Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 198; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 13; Alp, "Corona Günlerinde Uzaktan (Evden) Çalışma, Telafi Çalışması ve Ücret İndirimi", 830; Ergüneş Emrağ, "4857 Sayılı İş Kanunun Değişik 14. Maddesi Işığında Tele Çalışma", 1429; Özdemir, "Uzaktan Çalışma Yönetmeliği Karşısında Tele Çalışma", 31-32.

işin ifa edildiği mekânın aynı zamanda işçinin özel hayat alanını teşkil etmesi ve bu iki alanın sınırlarının kaçınılmaz olarak iç içe geçmesidir[167]. İşverenin yönetim ve denetim yetkisi bu özel alana sirayet ettiğinde, yalnızca işçinin değil, aynı konutu paylaşan üçüncü kişilerin de konut dokunulmazlığı, özel hayatın gizliliği ve kişisel verilerinin korunması gibi temel haklarına saygı gösterilmesi zorunluluğu doğmaktadır[168]. Bu bağlamda işverenin koruma ve gözetme borcu, salt işçinin fiziksel bütünlüğünü sağlamanın ötesine geçerek; onun kişilik haklarını, mahremiyetini ve dijital ortamdaki veri güvenliğini de kapsayan geniş bir çerçeveye yayılmaktadır. Bu temel borç, kendisini takip eden alt başlıklarda detaylandırılacak olan iş sağlığı ve güvenliğini sağlama, özel hayatın gizliliğine riayet etme, kişisel verileri koruma ve ulaşılabilir olmama hakkına saygı gösterme gibi daha özel yükümlülüklerin çatı kavramı niteliğindedir.

- **İş Sağlığı ve Güvenliğini Sağlama Yükümlülüğü**

Tele çalışanların iş sağlığı ve güvenliğinin sağlanması, işveren açısından hem genel ilkelerin geçerliliğini koruduğu hem de tele çalışmaya özgü farklı yaklaşımların benimsenmesinin gerektiği özel bir alan oluşturmaktadır[169]. Tele çalışma, yapısı itibarıyla geleneksel işyerlerinden farklı riskler ve çalışma koşulları içerdiğinden, işverenlerin sorumlulukları da söz konusu farklılıklara göre şekillenmektedir[170]. Bu kapsamda işverenler, uzaktan çalışmanın niteliğine ve ortaya çıkardığı özel koşullara göre, çalışanları iş sağlığı ve güvenliği konusunda bilgilendirmek, gerekli eğitimleri vermek, sağlık gözetimini yapmak ve sağlanan ekipmanların güvenliğini temin etmek gibi yükümlülükleri İş Kanunu'nun 14. maddesinin 6. fıkrası ve Uzaktan Çalışma Yönetmeliği 12. madde uyarınca yerine getirmek zorundadır[171].

---

[167] Öğretide, kişinin yaşam alanı üç kategoriye ayrılmaktadır: Kamuya açık yaşam alanı, kişinin herkese açık olarak gerçekleştirdiği eylemler ve ilişkileri içerir; özel yaşam alanı, ailesi ve arkadaşları gibi belirli kişilerle paylaşılan yaşam olaylarını kapsar; gizli yaşam alanı ise, kişinin sırlarını sakladığı ve yalnızca kendi rızasıyla belirli kişiler tarafından öğrenilebilen alanı ifade eder. Bu ayrım, özel hayatın gizliliğine yönelik müdahalelerin hukuka uygunluk denetiminde temel bir ölçüt olarak kullanılır. Ayrıntılar için bknz. K. Ahmet Sevimli, *İşçinin Özel Yaşamına Müdahalenin Sınırları* (Legal, 2006), 8; Rümeysa Savran, "İşçinin İşyerinde Elektronik Yöntemlerle İzlenmesi" (Yüksek Lisans Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, 2023), 14.

[168] Çelik vd., *İş Hukuku Dersleri*, 226; Mollamahmutoğlu vd., *İş Hukuku*, 470.

[169] Çelik vd., *İş Hukuku Dersleri*, 225.

[170] Ayrıntılar için bknz. Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 129-41.

[171] Ayrıca, Uluslararası Çalışma Örgütü'nün 177 sayılı Evde Çalışma Sözleşmesi'nin 7. maddesinde, iş sağlığı ve güvenliğine ilişkin ulusal yasa ve yönetmeliklerin, evde çalışmanın kendine özgü nitelikleri

Tele çalışmanın gerçekleştiği ortamın kendine özgü koşulları, iş sağlığı ve güvenliği önlemlerinin daha kapsamlı ve farklı bir yaklaşımla ele alınmasını gerektirmektedir. Bu çerçevede işverenler, tele çalışma alanının havalandırılması, yangın güvenliği, kişisel koruyucu ekipmanların sağlanması ve elektrik hatlarının güvenliğinin sağlanması gibi risk azaltıcı önlemleri almak ve çalışanları olası tehlikelere karşı bilgilendirmekle yükümlüdürler[172]. Ayrıca işverenlerin, geleneksel işyerlerinde yaptıkları denetimlere benzer şekilde, tele çalışma koşullarını düzenli olarak değerlendirmeleri ve gerekli kontrolleri gerçekleştirmeleri gerekmektedir[173]. Ancak bu denetimler, çalışanın özel hayatının gizliliği ve kişilik haklarını ihlal etmeyecek şekilde, her bir kontrolden önce çalışana önceden bildirimde bulunularak ve açık rızası alınarak yapılmalıdır[174].

Alınan bu önlemlerin ve yapılan kontrollerin etkinliğinin denetlenmesi amacıyla, tele çalışma alanının müfettişler tarafından incelenmesi gerekliliği ortaya çıkabilmektedir. Ancak bu incelemelerin yapılabilmesi için çalışanın açık rızası gerekmektedir. Çalışanın rızasının alınamadığı durumlarda denetimler çevrim içi yöntemlerle yapılmalıdır. Böylelikle, tele çalışma koşullarında da iş sağlığı ve güvenliği etkin bir şekilde sağlanmış olacaktır[175].

Tele çalışanları ilgilendiren bir diğer önemli düzenleme ise Ekranlı Araçlarla Çalışma Yönetmeliği'dir. Yönetmeliğin 6. maddesine göre işverenler, ekranlı araçlarla çalışmanın doğurabileceği riskler hakkında çalışanları bilgilendirmek ve bu riskleri azaltıcı önlemler konusunda eğitim vermekle yükümlüdürler[176].

---

dikkate alınarak bu çalışma biçimine uygulanacağı hükme bağlanmıştır. Aynı maddede, sağlık ve güvenlik gerekçeleriyle evde çalışmada belirli iş türlerinin ve bazı maddelerin kullanımının yasaklanabileceği koşulların da belirlenmesi öngörülmüştür. Bknz. "Convention C177 - Home Work Convention, 1996 (No. 177)".

[172] Brecht, Hans-Theo: Heimarbeitsgesetz, München 1977, §16 Rn. 3,4; Aktaran: Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 162.

[173] Çelik vd., *İş Hukuku Dersleri*, 226 vd.; Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 131; Kara, *Uzaktan Çalışmada İş Sağlığı ve Güvenliğinin Hukuki Boyutu*, 85.

[174] Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 168; Kutlu, *İş Hukukunda Tele Çalışma*, 403; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 26-27.

[175] Çelik vd., *İş Hukuku Dersleri*, 226 vd.; Senyen Kaplan, *Bireysel İş Hukuku*, 2. bs, 163.

[176] Gaye Baycık vd., "Platform Çalışanlarını Yasal Güvenceye Kavuşturmak: Sorunlar ve Çözüm Önerileri", *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi*, sy 1 (2021): 1693.

Uluslararası hukukta tele çalışanların iş sağlığı ve güvenliği, temel olarak Tele Çalışma Çerçeve Anlaşması'nın 8. maddesi ekseninde düzenlenmektedir. Anılan madde, işverene 89/391 sayılı Direktif başta olmak üzere ilgili tüm mevzuata uygun olarak tele çalışanların sağlığını ve güvenliğini sağlama yükümlülüğü getirmekte ; buna ek olarak, geçerli sağlık ve güvenlik politikaları hakkında çalışanları bilgilendirme sorumluluğu da yüklemektedir[177]. Bu yükümlülüklerin takibi ve doğrulanması amacıyla Anlaşma, işverene tele çalışma alanına erişim hakkı tanımaktadır. Ancak bu hakkın, özellikle işin çalışanın konutunda ifa edildiği durumlarda kullanılabilmesi, çalışanın önceden bilgilendirilmesi ve rızasının alınması şartına bağlanmıştır. İşverenin denetim hakkına bir denge unsuru olarak, tele çalışana da kendi çalışma ortamının denetlenmesini talep etme imkânı verilmiştir[178].

Çerçeve Anlaşma'nın 9. maddesi ile getirilen önemli bir yükümlülük ise tele çalışanların sosyalleşme ihtiyacının karşılanmasına yöneliktir. Bu hükme göre işverenler, tele çalışanların iş ortamından ve çalışma arkadaşlarından izole olmalarını engelleyecek gerekli tedbirleri almakla yükümlüdür. Tele çalışmanın, çalışanları fiziksel olarak iş ortamından uzaklaştırması nedeniyle, ruh sağlığı üzerinde olumsuz etkiler oluşturma riski söz konusudur. Dolayısıyla, işverenlerin, çalışanların ruh sağlığına yönelik ortaya çıkan söz konusu riski iş sağlığı ve güvenliği kapsamında değerlendirmeleri önem arz etmektedir[179].

Bu bağlamda kanaatimizce hibrit çalışma modellerinin uygulanması, işçinin hem uzaktan hem de fiziki olarak işyerinde çalışmasına olanak tanıyarak bahsedilen dezavantajların azaltılmasına katkıda bulunacaktır. İşverenlerin düzenli aralıklarla tele çalışanların iş arkadaşlarıyla bir araya gelmesini sağlaması ve şirket bilgilerine erişimlerini kolaylaştırması, çalışanların işyerinden fiziksel uzaklığının sosyal ilişkilerini ve kurumsal bağlarını olumsuz yönde etkilemesini önlemek açısından son derece önemlidir.

---

[177] Council of the European Communities, Council Directive 89/391/EEC of 12 June 1989 on the Introduction of Measures to Encourage Improvements in the Safety and Health of Workers at Work (İşyerinde İşçilerin Sağlık ve Güvenliğinin Geliştirilmesine İlişkin Önlemlerin Uygulanmasına Dair 12 Haziran 1989 Tarihli 89/391/AET Sayılı Konsey Direktifi), Official Journal of the European Communities, L 183 (29 Haziran 1989)): 1–8.
[178] Çelik vd., *İş Hukuku Dersleri*, 226.
[179] Dulay Yangın, "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi", 165.

- **Özel Hayatın Gizliliğini Sağlama Yükümlülüğü**

Tele çalışma ilişkisinde işverenin tele çalışan üzerinde doğrudan denetim yapma imkânı olmamakta bilgi ve iletişim teknolojileri vasıtasıyla denetimi gerçekleştirmektedir[180]. Hukukumuzda tele çalışanın denetlenmesine ilişkin özel bir düzenleme bulunmayıp Uzaktan Çalışma Yönetmeliği'nin 12. maddesinde *"işverenin uzaktan çalışan işçiyi izleme yöntemlerinin yapılacak iş ile orantılılık ölçüsünde belirleneceği ve işçiye bildirileceği; işverenin izleme sürecinin sürekli nitelik taşımayıp, belirli bir zaman aralığıyla sınırlı olması gerektiği"* düzenlenmiş, ancak bu düzenlemeye Yönetmeliğin yürürlüğe giren nihai metninde yer verilmemiştir[181].

Tele Çalışma Çerçeve Anlaşması'nın 6. maddesinde, işverenin uzaktan çalışanların mahremiyetine saygı gösterme yükümlülüğü açıkça düzenlenmiştir. Anlaşma'ya göre;

> İşveren, uzaktan çalışanların mahremiyetine saygı göstermekle yükümlüdür. Herhangi bir izleme sistemi uygulanacaksa, bu sistem amacına orantılı olmalı ve Görüntü Ekranlı Araçlarla İlgili 90/270 sayılı Direktif'e uygun şekilde hayata geçirilmelidir.

Hukukumuzda tele çalışma özelinde özel hayatın gizliliğine yönelik doğrudan bir yasal düzenleme bulunmamakla birlikte, Anayasa, Türk Medeni Kanunu ve İş Kanunu çerçevesinde kişiliğin korunmasına ilişkin hükümler ve temel ilkeler bu alanda da uygulama alanı bulmaktadır[182]. Ancak kanaatimizce, teknolojinin hızla gelişmesiyle birlikte denetim faaliyetlerinin daha yoğun ve çeşitlenmiş biçimlerde gerçekleştirilmesi, uzaktan çalışma bağlamında özel hayatın gizliliğini daha da kırılgan hâle getirmektedir. Bu nedenle, uzaktan çalışma ilişkilerine özgü olarak özel hayatın gizliliğini güvence altına alacak açık ve kapsamlı bir düzenlemeye ihtiyaç bulunmaktadır.

---

[180] Dilek Dulay Yangın, "Bilgi ve İletişim Teknolojilerinde Yaşanan Gelişimin İş Hukuku Üzerindeki Etkileri: Tele Çalışmaya İlişkin Tespit ve Öneriler", *İş Hukukunda Genç Yaklaşımlar III içinde. İstanbul: On İki Levha Yayıncılık*, 2018, 249; Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 135-40; Dulay, *Türk İş Hukukunda Evde Çalışma*, 221; Kutlu, *İş Hukukunda Tele Çalışma*, 417.

[181] Dulay Yangın, "Bilgi ve İletişim Teknolojilerinde Yaşanan Gelişimin İş Hukuku Üzerindeki Etkileri: Tele Çalışmaya İlişkin Tespit ve Öneriler", 250; Kutlu, *İş Hukukunda Tele Çalışma*, 421.

[182] Dulay, *Türk İş Hukukunda Evde Çalışma*, 223; Kutlu, *İş Hukukunda Tele Çalışma*, 421.

- **Kişisel Verileri Koruma Yükümlülüğü**

Kişisel verilerin korunması yükümlülüğü, işverenin tele çalışana yönelik koruma ve gözetme borcu çerçevesinde değerlendirilmesi gereken temel yükümlülüklerden biridir. Tele çalışma özelinde kişisel verilerin korunmasına yönelik İş Kanunu'nda özel bir düzenleme bulunmadığından, bu alanda Kişisel Verilerin Korunması Kanunu'nun genel hükümleri uygulama alanı bulmaktadır[183]. Ayrıca Türk Borçlar Kanunu'nun 419. maddesinde, işverenin işçinin kişisel verilerini yalnızca işçinin işe yatkınlığı veya hizmet sözleşmesinin yerine getirilmesiyle doğrudan ilgili ve gerekli olduğu ölçüde kullanabileceği belirtilmekte, özel kanun hükümlerinin saklı olduğu da ifade edilmektedir[184].

Uzaktan Çalışma Yönetmeliği'nin "Verilerin Korunması" kenar başlıklı 11. maddesine göre işveren, uzaktan çalışanları, işyerine ve iş süreçlerine dair verilerin güvenliği ile bu verilerin korunması ve paylaşımına ilişkin yasal düzenlemeler ve işletme politikaları hakkında bilgilendirmekle yükümlüdür[185]. Aynı maddede, işverenin veri güvenliğini sağlamak adına gerekli önlemleri alma sorumluluğu vurgulanmış ve bu kapsamda çalışanlara yönelik aydınlatma ve bilgilendirme yükümlülüğü getirilmiştir. 11. maddenin 2. fıkrasında, korunması gereken verilerin tanımı ve kapsamının sözleşmede açıkça belirtilmesi gerektiği hüküm altına alınarak, hukuki belirsizliklerin önüne geçilmesi amaçlanmıştır. Üçüncü fıkrada ise uzaktan çalışanın, işveren tarafından belirlenen veri koruma kurallarına uymakla yükümlü olduğu açıkça düzenlenmiştir[186].

---

[183] Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 62; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 76-124.

[184] Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 143; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 62.

[185] Öğretide bu husus sadece işletme verilerinin korunmasının düzenlenmesi eleştirilmiştir. İşveren sadece uzaktan çalışanların değil çevresindekilerin de kişisel verilerinin güvenliğini gözetmekle yükümlüdür. Bknz. Çelik vd., *İş Hukuku Dersleri*, 225; Ünal Adınır, "Tele çalışmada verilerin korunması", 971; Özdemir, "Uzaktan Çalışma Yönetmeliği Karşısında Tele Çalışma", 38; Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 18.

[186] Kara, *Uzaktan Çalışmada İş Sağlığı ve Güvenliğinin Hukuki Boyutu*, 41; İnal, "Uzaktan Çalışma", 64-65.

2.2.7.2.5. Ulaşılabilir Olmama Hakkına Uyma Yükümlülüğü

Dijitalleşmenin ve esnek çalışma modellerinin giderek yaygınlaşması, iş ile özel hayat arasındaki sınırların belirsizleşmesine yol açarak "ulaşılabilir olmama hakkı" kavramını gündeme getirmiştir[187]. Ulaşılabilir olmama hakkı, çalışanların çalışma saatleri dışında herhangi bir dijital araç aracılığıyla işle ilgili taleplere yanıt vermeme ve bu nedenle herhangi bir olumsuz yaptırıma maruz kalmadan işten bağlantıyı kesebilme özgürlüğünü ifade etmektedir[188]. Bu hakkın temel amacı, çalışanların fiziksel ve psikolojik sağlığını korumak, iş-yaşam dengesini yeniden tesis etmek ve tükenmişlik ile stres gibi olumsuz etkileri azaltmaktır. Zira sürekli erişilebilir olma beklentisi, çalışanların dinlenme sürelerinde bile işle ilgilenmelerine ve özel hayatlarının geri plana itilmesine neden olabilmektedir[189].

Ulaşılabilir olmama hakkının uygulama biçimleri ülkeden ülkeye farklılık göstermektedir. Örneğin Fransa, Belçika, İtalya ve İspanya gibi ülkeler, doğrudan mevzuat düzenlemeleri ile çalışanları koruyan ve bu hakkın kullanılmasını teşvik eden bir yaklaşım benimsemiştir[190]. Fransa, 2016 yılında bu hakkı yasal düzenlemeye konu eden ilk ülke olarak dikkat çekmektedir. Diğer taraftan Almanya gibi bazı ülkeler ise doğrudan yasallaştırma yerine şirket içi politika ve toplu iş sözleşmeleriyle daha esnek bir düzenleme yöntemini tercih etmektedir[191]. Türkiye'de ise ulaşılabilir olmama hakkını doğrudan tanıyan özel bir düzenleme mevcut değildir. Ancak İş Kanunu ve ilgili yönetmeliklerde yer alan çalışma ve dinlenme sürelerine ilişkin hükümler ile işverenin gözetim borcu gibi genel yükümlülükler, dolaylı olarak çalışanlara bir

---

[187] F. Burcu Savaş Kutsal, İşçinin Ulaşılabilir Olmama Hakkı Güncel Çalışma Koşulları ve Karşılaştırmalı Hukuk Işığında Türk İş Hukuku İçin Tespit ve Öneriler, İş Hukuku Monografileri (Seçkin, 2024), 13-15; Emre Ünal, "İşçinin Ulaşılamama Hakkı" (Yayınlanmamış Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, 2023), 1 vd.; Hüseyin Boz ve Ebru Gözen, İş-Yaşam Dengesi Açısından İşgörenin Ulaşılamama Hakkı (Akademisyen Kitabevi, 2024), v; Ece Aktaş, "Dijital Çalışma Bakımından Ulaşılamama Hakkı", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 1, sy 22 (2025): 6.

[188] Savaş Kutsal, *İşçinin Ulaşılabilir Olmama Hakkı Güncel Çalışma Koşulları ve Karşılaştırmalı Hukuk Işığında Türk İş Hukuku İçin Tespit ve Öneriler*, 23-27; Ünal, "İşçinin Ulaşılamama Hakkı", 9; Aktaş, "Dijital Çalışma Bakımından Ulaşılamama Hakkı", 6.

[189] Ünal, "İşçinin Ulaşılamama Hakkı", 11; Savaş Kutsal, *İşçinin Ulaşılabilir Olmama Hakkı Güncel Çalışma Koşulları ve Karşılaştırmalı Hukuk Işığında Türk İş Hukuku İçin Tespit ve Öneriler*, 27.

[190] Savaş Kutsal, *İşçinin Ulaşılabilir Olmama Hakkı Güncel Çalışma Koşulları ve Karşılaştırmalı Hukuk Işığında Türk İş Hukuku İçin Tespit ve Öneriler*, 72-80; Ünal, "İşçinin Ulaşılamama Hakkı", 62-77.

[191] Savaş Kutsal, *İşçinin Ulaşılabilir Olmama Hakkı Güncel Çalışma Koşulları ve Karşılaştırmalı Hukuk Işığında Türk İş Hukuku İçin Tespit ve Öneriler*, 72-80; Ünal, "İşçinin Ulaşılamama Hakkı", 62-77.

koruma sağlayabilmektedir.[192] Bu bağlamda yargı içtihatlarının gelişmesi ve çalışanların bu konuda bilinçlendirilmesi önem taşımakta, aynı zamanda iş gücü piyasasındaki esnekliği engellemeyen, fakat çalışan haklarını net biçimde koruyan yasal düzenlemelerin faydalı olacağı belirtilmektedir[193].

Ulaşılabilir olmama hakkının ihlali, çalışan açısından çeşitli hukuki sonuçlar doğurabilmektedir. Çalışanlar, çalışma saatleri dışı zamanlarda kendilerinden yapılan iş talepleri nedeniyle fazla çalışma ücreti talep edebilirler. Ayrıca sürekli erişilebilir olmanın neden olduğu stres, tükenmişlik ve benzeri psikososyal riskler, iş kazası ya da meslek hastalığı kapsamına girebilir ve işçilere maddi-manevi tazminat davası açma hakkı tanıyabilir. İşverenlerin, çalışma saatleri dışında gerçekleşen hukuka aykırı iş taleplerini, çalışanın kişiliğini koruma ve gözetme borcu çerçevesinde engellemeleri gerekmektedir. Bununla birlikte, ciddi ve yakın tehlike oluştuğu durumlarda çalışanın çalışmaktan kaçınma hakkı ya da çalışma koşullarının katlanılmaz hâle gelmesi durumunda haklı nedenle iş sözleşmesini feshetme hakkı da mevcuttur. Bu kapsamda, çalışanın çalışma saatleri dışında taleplere verdiği rızanın da işveren baskısı altında verilmiş olabileceği unutulmamalı ve bu rızalar dikkatle değerlendirilmelidir[194].

Tele çalışma modeline özgü ulaşılabilir olmama hakkının güvence altına alınması, çalışma saatlerinin belirsizleşmesini önleyerek işverenlerin aşırı dijital izleme veya sürekli erişilebilirlik taleplerinin doğurduğu psikososyal riskleri azaltmada ve çalışanların dijital ortamda sağlıklı bir çalışma düzenine sahip olmalarında kritik bir önem taşımaktadır. Bu doğrultuda hazırlanacak bir mevzuat, çalışanların iş-yaşam dengesini kurmalarına katkı sağlamanın yanı sıra, ruhsal sağlıklarının korunması açısından da büyük önem taşımaktadır.

---

[192] Savaş Kutsal, *İşçinin Ulaşılabilir Olmama Hakkı Güncel Çalışma Koşulları ve Karşılaştırmalı Hukuk Işığında Türk İş Hukuku İçin Tespit ve Öneriler*, 88 vd.; Ünal, "İşçinin Ulaşılamama Hakkı", 176; Mehmet Zahid Erer, "Bir İnsan Hakkı Olarak Ulaşılamama Hakk" (Yayınlanmamış Yüksek Lisans Tezi, İstanbul Medeniyet Üniversitesi, 2024), 140.

[193] Savaş Kutsal, *İşçinin Ulaşılabilir Olmama Hakkı Güncel Çalışma Koşulları ve Karşılaştırmalı Hukuk Işığında Türk İş Hukuku İçin Tespit ve Öneriler*, 110 vd.

[194] Ünal, "İşçinin Ulaşılamama Hakkı", 122 vd.; Aktaş, "Dijital Çalışma Bakımından Ulaşılamama Hakkı", 30 vd.

2.2.7.3. Tele Çalışmanın Şekil Şartlarına İlişkin Yükümlülükler

Tele çalışma ilişkisinin kendine özgü yapısı ve taraflar arasındaki hukuki güvenliğin sağlanması ihtiyacı, bu ilişkinin kuruluşunu ve içeriğini düzenleyen özel şekil şartlarının getirilmesini gerekli kılmıştır. Nitekim kanun koyucu, uzaktan çalışmaya ilişkin birtakım özel şekil şartları belirlemiştir. İş Kanunu'nun 14. maddesinin 5. fıkrasında ve Uzaktan Çalışma Yönetmeliği 5. maddesi 2. fıkrasında, uzaktan çalışma sözleşmelerinde bulunması gereken unsurlar açıkça sıralanmıştır. Buna göre, sözleşmede *"işin tanımı, yapılma şekli, işin süresi ve yeri, ücret ve ücretin ödenmesine ilişkin hususlar, işveren tarafından sağlanan ekipman ve bunların korunmasına ilişkin yükümlülükler, işverenin işçiyle iletişim kurması ile genel ve özel çalışma şartlarına ilişkin hükümler"* gibi hususların belirtilmesi zorunludur. Ayrıca hem Kanun hem de Yönetmelik gereğince uzaktan çalışmaya ilişkin iş sözleşmelerin yazılı şekilde yapılması zorunludur[195].

[195] Süzek ve Başterzi, *İş Hukuku*, 284-85; Şakar ve Erkan Şahin, "Esnek Çalışma Modellerinden Uzaktan Çalışma ve Uzaktan Çalışanların Sigortalılığı", 253; Erkanlı Başbüyük, "Uzaktan Çalışmanın Bir Türü Olarak Tele Çalışmada İşçinin Dinlenme Hakkı", 659.

BÖLÜM III

TELE ÇALIŞMADA İZLEME VE GÖZETLEME

3.1. Çalışma Yaşamında İzleme ve Gözetleme Uygulamalarının Tarihi Gelişimi

İş ilişkisinde izleme ve gözetleme uygulamalarının oldukça eski bir geçmişi vardır. Yüzyıllardır iş ilişkisinde çalışanların izlenmesi ve gözetlenmesi söz konusudur[196]. Kayıtlara geçen ilk örneklerden biri 1900'lü yılların başında Henry Ford'un fabrikalarında üretim verimliliğinin artırılması amacıyla işçilerin çalışma süreçlerinin kronometreyle ölçülmesidir. Ford, yalnızca iş süreçlerini denetlemekle yetinmemiş, aynı zamanda özel dedektifler aracılığıyla işçilerin özel hayatlarını da izleyerek bütüncül bir kontrol mekanizması kurmuştur[197]. 20. yüzyılın sonlarından itibaren bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişmelerle izleme ve gözetleme boyut değiştirerek günümüzdeki karmaşık ve yaygın yapısına evrilmiştir. Ancak, bilgi ve iletişim teknolojilerindeki ilerlemeler ve bu teknolojilerin azalan maliyetleri, 21. yüzyıl işyerlerinde izleme ve gözetim uygulamalarının türünde erişilebilirliğinde ve yoğunluğunda önemli bir dönüşüm yaratmıştır[198]. Bu dönüşümü tetikleyen başlıca faktörler arasında; çok kaynaklı büyük veri kümelerinin oluşturulabilmesi, metin, ses ve video gibi yapılandırılmamış verilerin analiz edilebilmesi ve tahmine dayalı analitik modellerin kullanımının yaygınlaşması sayılabilecektir. Ayrıca, giyilebilir teknolojilerin gelişmesi, akıllı telefonların günlük yaşamın ayrılmaz bir parçası olması ve sosyal medya platformlarının kullanımının sürekli artması işverenlerin çalışanları izleme ve gözetleme kapasitelerini daha önce hiç olmadığı ölçüde arttırmıştır[199]. İş

---

[196] Peter Jeffrey Holland vd., "Electronic Monitoring and Surveillance in the Workplace: The Effects on Trust in Management, and the Moderating Role of Occupational Type", Personnel Review 44, sy 1 (2015): 161.

[197] Harvey L. Fiser ve Patrick D. Hopkins, "Getting Inside the Employee's Head: Neuroscience, Negligent Employment Liability, and the Push and Pull for the New Technology", *Boston University Journal of Science and Technology Law* 23, sy 1 (2017): 48-49.

[198] Holland vd., "Electronic Monitoring and Surveillance in the Workplace", 161.

[199] Yeliz Bozkurt Gümrükçüoğlu, "İşçinin Sosyal Medya Kullanımının İş Hukukundaki Etkileri", *PressAcademia Procedia* 7, sy 1 (2018): 372; Selen Uncular, "Teknolojinin Etkisiyle Dönüşen İş İlişkisinde Giriş Kontrol Sistemleri, Yer Belirleme Sistemleri ve Sosyal Medya Vasıtasıyla İzleme", *Çalışma ve Toplum* 3, sy 66 (2020): 1674.

hukukunun temelinde yatan işverenin en yüksek verimi alma, çalışanların ise örgütlenerek güç kazanma ve insan onuruna yaraşır koşullar elde etme mücadelesi, dijitalleşme ile farklı bir boyut kazanmıştır. Verim, zaman ve maliyet açısından işveren lehine sonuçlarına karşılık, dijital izleme ve gözetleme uygulamaları işçi aleyhine olumsuz etkilere yol açmaktadır. Zira dijitalleşme, izleme ve gözetleme araçlarının türlerini çeşitlendirip kapsam alanını genişletirken çalışan üzerinde bir nevi dijital "panoptikon"[200] etkisi doğurmaktadır. Yapay zekâ sistemleri ise dijital izleme ve gözetlemeyi "algoritmik izleme ya da gözetleme" olarak adlandırabileceğimiz yeni bir seviyeye taşımıştır[201]. Bir yandan işlenen veri miktarı ve hızı artarken, diğer yandan maliyet bakımından önemli bir azalmaya yol açan yapay zekâ destekli izleme ve gözetleme uygulamaları, işverene eş zamanlı, sürekli ve görünmez bir denetim imkânı sağlamaktadır. Ancak bunun çalışanın temel haklarına etkisi dikkate alınmamaktadır.

Dijital çağdaki izleme ve gözetlemenin en belirgin farkı, teknolojinin günlük yaşamımıza entegrasyonu neticesinde çoğu bireyin ürettiği veri miktarının ve bu verilerin izlenebilirliğinin farkında olmamasıdır. Çalışma yaşamı bakımından da aynı durum söz konusudur. CCTV kameralarının varlığı genellikle görsel olarak kaydedildiğimize dair bizi uyarırken, telefonlar, akıllı saatler, GPS sistemleri ve sosyal medya platformları gibi teknolojiler aracılığıyla üretilen veri miktarı çok daha fazladır ve genellikle fark edilmez[202]. Bu cihazlar, her hareketimiz, davranışımız ve biyometrik verimiz hakkında şirketlere sürekli bilgi iletmektedir. Örneğin, Apple'ın "sık kullanılan konumlar" özelliği milyonlarca kullanıcının konumunu takip etmiş; Google, arama sorgularını kullanarak grip salgınlarını tahmin edebilmiş ve Twitter verileri, salgınların resmi sağlık izleme sistemlerinden daha hızlı öngörülmesini sağlamıştır. Benzer şekilde, Jawbone gibi giyilebilir fitness takip cihazlarının, bir depremin merkez

---

[200] Michel Foucault, *Hapishanenin Doğuşu*, 8., çev. Mehmet Ali Kılıçbay (İmge Kitabevi Yayınları, 2019), Panoptikon, ilk olarak 18. yüzyıl düşünürü Jeremy Bentham tarafından tasarlanan, merkezdeki bir gözetleme kulesinden tüm mahpusların görülebildiği ancak mahpusların kendilerini gözetleyeni göremediği bir hapishane modelidir. Bu mimari yapı, sürekli gözetlenme ihtimali nedeniyle bireylerin kendi kendilerini disipline etmelerini ve denetlemelerini sağlar. Kavram, Michel Foucault tarafından modern toplumlardaki iktidar, disiplin ve gözetim mekanizmalarını analiz etmek için güçlü bir metafor olarak kullanılmıştır. Ayrıntılı bilgi için bknz.

[201] Başak Ozan Özparlak, Büyük Veri Çağında Yapay Zeka Sistemlerinin Çalışma İlişkilerinde Kullanımı: Hukuki Bir Değerlendirme (Onikilevha Yayıncılık, 2021), 189.

[202] Javier Sánchez-Monedero ve Lina Dencik, "The Datafication of The Workplace", Cardiff University, datajusticeproject. net, 2019, 15, https://orca.cardiff.ac.uk/id/eprint/125552/1/Report-The-datafication-of-the-workplace.pdf.

üssünü belirlemede geleneksel raporlama sistemlerinden daha etkili olduğu görülmüştür[203].

Günümüzde işverenler tarafından yürütülen izleme ve gözetim faaliyetleri, büyük ölçüde bilgi ve iletişim teknolojilerine dayanmaktadır. Bilgisayarlar, şirket telefonları, güvenlik kameraları, çalışanlara verilen giyilebilir teknolojik cihazlar ve işyerine giriş-çıkışı kontrol eden erişim kartları gibi çeşitli araçlar yaygın olarak kullanılmaktadır. Bu faaliyetler fiziksel araçlarla sınırlı kalmamakta; çevrim içi izleme teknikleri, işçilerin gözetiminde giderek daha merkezi bir rol üstlenmektedir. Nitekim yapılan araştırmalar, işverenlerin %74 gibi yüksek bir oranının çalışanlarını denetlemek için çevrim içi izleme ve gözetim araçlarına başvurduğunu ortaya koymaktadır. Çevrim içi yöntemler arasında özellikle çalışanların ekranlarının gerçek zamanlı takibi (%59) ve ziyaret ettikleri web sitelerinin geçmişinin incelenmesi (%62) gibi uygulamalar öne çıkmaktadır. Ayrıca belirtelim ki, bu uygulamalar dijital ortamla sınırlı kalmayıp, fiziksel ofislerde de hâla yaygın şekilde kullanılmaktadır. Nitekim işverenlerin %75'i kamera (%69) ve biyometrik erişim kontrolü (%58,3) gibi yöntemlerle çalışanları fiziksel olarak izlemektedir. Ayrıca işverenlerin %67'si yüz tanıma ve parmak izi gibi biyometrik verileri toplarken, %61'i ise çalışanların verimliliklerini ölçmek üzere yapay zekâ destekli analiz sistemlerini kullanmaktadır[204].

İzleme ve gözetleme uygulamalarının bu tarihsel evrimi, özellikle günümüzde yaygınlaşan uzaktan çalışma modeliyle birlikte daha karmaşık bir boyut kazanmıştır. Zira çalışanların fiziksel olarak işyerinde bulunmadıkları tele çalışma ortamları, işverenler için farklı denetim ve kontrol ihtiyacını doğurmuştur. Bu ihtiyaç da Henry Ford'un fabrikada uyguladığı doğrudan denetim mekanizmalarından, günümüzün sofistike dijital izleme teknolojilerine kadar uzanan bir evrimi tetiklemiştir. Çalışanların artık işyeri içinde olduğu gibi işyeri dışında da izleme ve gözetim uygulamaları ile takibi mümkündür. Böylece işverenin denetim yetkisi fiziksel olarak işyeri sınırlarının dışında kullanılabilir hâle gelmiştir. Hatta bu denetim kimi hâllerde çalışanın özel hayat alanı olan evine kadar uzanabilmektedir. Ancak bu durum işverenin yönetim hakkı ve denetim yetkisinin sınırları ile çalışanın özel hayatın

[203] Fiser ve Hopkins, "Getting Inside the Employee's Head", 69-70.
[204] ExpressVPN, "Workplace Surveillance Trends in the U.S. 2025", ExpressVPN Blog, 06 Şubat 2025, https://www.expressvpn.com/blog/workplace-surveillance-trends-us/.

gizliliği, konut dokunulmazlığı ve kişisel verilerinin korunması hakkı arasında hassas dengenin kurulması zorunluluğu doğurmaktadır.

Mobil cihazların ve sosyal medyanın yaygınlaşması, izleme ve gözetlemeyi hem daha kolay hem de daha yaygın hâle getirerek işverenlerin çalışanları üzerindeki denetim gücünü ve kontrol olanaklarını önemli ölçüde artırmaktadır. Bu teknolojik kapasite, bir yandan işverenlere iş süreçlerini yönetme, verimliliği artırma ve güvenliği sağlama gibi meşru gerekçeler sunmaktadır. Örneğin, Uber'in sürücü güvenliğini artırmak amacıyla sürüş verilerini analiz etmesi, bu yaklaşımın performansı izleme ve güvenlik tedbirlerini geliştirme açısından ne denli etkili olabileceğini göstermektedir. Diğer yandan, işverenlerin çalışanların davranışları hakkında bu denli detaylı ve gerçek zamanlı bilgiye sahip olması, ne kadar bilginin meşru sayılacağı ve denetimin sınırlarının nerede çizileceği gibi temel hukuki soruları da beraberinde getirmektedir[205].

Aşağıda ayrıntılı olarak ele alınan izleme ve gözetleme yöntemleri, coğrafi olarak dağınık bir iş gücünü yönetme ve performansı uzaktan değerlendirme çabasındaki işverenlere benzeri görülmemiş imkânlar sunmaktadır. Ancak aynı zamanda, bu tarihsel kontrol arayışının çalışanın özel hayat alanına taşınması riskini de beraberinde getirmektedir. Dolayısıyla, izleme ve gözetlemenin teknolojik kapasitesindeki bu artış, tele çalışma özelinde çalışanların temel hak ve özgürlükleri ile işverenin meşru menfaatleri arasında kurulması gereken hassas dengeyi daha da önemli hâle getirmiştir.

3.2. Kavramsal Çerçeve ve Terminoloji Tartışması

İş ilişkilerinde çalışanların faaliyetlerinin performansını, verimliliğini ya da davranışlarını denetim amacıyla işverenlerce kullanılan uygulama ve araçlar, Öğretide sıklıkla "izleme" ve "gözetleme" veya "gözetim" kavramlarıyla ifade edilmektedir[206].

---

[205] Fiser ve Hopkins, "Getting Inside the Employee's Head", 69-70.

[206] Ayrıca, öğretide kimi zaman bu kavramlara ek olarak "denetim" ifadesinin de benzer bağlamlarda tercih edilmektedir. Bknz. Zeki Okur, *İş Hukuku'nda Elektronik Gözetleme* (Legal Yayıncılık, 2011), 22-23. Ek olarak belirtmek gerekir ki, elektronik araçlarla gerçekleştirilen uygulamaları kapsamak üzere öğretide her iki kavramı da içeren "elektronik izleme ve gözetleme" (Electronic Monitoring and

Bu kavramlar, uluslararası raporlarda ve öğretide kimi zaman birbirlerinin yerine kullanılırken, kimi zaman da anlam ve kapsam bakımından birbirinden ayrılarak farklı terminolojik tercihlerle ele alınmaktadır[207]. Ancak belirtelim ki, bu konuda terim birliği sağlanamamış özellikle hukuk öğretisinde iki kavram arasında net bir ayrıma genel olarak yer verilememiştir.

İki kavram arasında ayrım yapılan çalışmalarda ise izleme, belirli bir amaca bağlı olmaksızın bireyler, sistemler veya süreçler hakkındaki bilgilerin otomatik yollarla ve sistematik bir şekilde toplanmasını ifade eden daha genel bir faaliyet olarak ele alınmaktayken, buna karşılık gözetleme, belirli bir otoritenin denetim ve kontrol amacıyla bireyler üzerinde kurduğu, daha müdahaleci ve hedefe yönelik bir ilişkiyi tanımlayacak şekilde ele alınmaktadır[208]. Bu çerçevede gözetleme, kişilerin davranışları, durumları ve hareketlerinin yakından takip edilmesini ve elde edilen bilgilerin davranışları yönlendirmek amacıyla kullanılmasını da ifade etmektedir[209]. Nitekim Eurofound tarafından hazırlanan bir raporda da gözetim teriminin, iş ile ilgili faaliyetlerin ötesine geçerek hem iş hem de iş dışı alanları kapsayan daha müdahaleci teknolojilerle ilişkili olduğu ve kamuoyunda daha olumsuz bir çağrışım yarattığı belirtilmektedir[210]. Öğretide öne sürülen bir görüşe göre ise, "izleme" kavramının iş görme edimiyle doğrudan ilişkili, meşru bir amaca yönelik, orantılı ve ölçülü yöntemleri ifade etmesi gerekirken; "gözetleme" ise bu niteliklerin bulunmadığı, daha

---

Surveillance) terimi de yaygın şekilde kullanılmaktadır. Bknz. Holland vd., "Electronic Monitoring and Surveillance in the Workplace", 161-75.

[207] Ball, *Electronic Monitoring and Surveillance in the Workplace*.

[208] Gözde Yılmaz, "Elektronik Performans İzleme Sistemlerinin Çalışanlar ve İşletmeler Üzerindeki Etkileri", *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi* 4, sy 7 (2005): 3; Zeynep Ceren Nurata, "Hukuksal, Örgütsel ve Etik Bir Sorun Olarak İşyerinde Elektronik Gözetim", *Gazi İktisat ve İşletme Dergisi* 7, sy 3 (2021): 215. İzleme kavramının belirli bir zaman dilimi boyunca bir durumun nasıl değiştiğini veya geliştiğini anlamak amacıyla dikkatli ve sistematik bir şekilde gözlemleme süreci olarak tanımlanmasına ilişkin bknz. İlkay Savcı, "İşyerlerinde Elektronik Denetim ve Gözetim", içinde *Küreselleşme Emek Süreçleri ve Yapısal Uyum*, ed. Ahmet Alpay Dikmen (İmaj Yayıncılık, 2002), 335. Nihan Aydın, "Çalışma Yaşamında Özgürlük Sorunu: Gözetim ve Mahremiyetin Yeni Sınırları" (Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi, 2011), 9; Savran, "İşçinin İşyerinde Elektronik Yöntemlerle İzlenmesi", 56; Michele Molè ve Aida Ponce Del Castillo, "Worker Monitoring Vs Worker Surveillance: The Need for a Legal Differentiation", içinde *Artificial intelligence, labour and society*, ed. Aida Ponce Del Castillo (European Trade Union Institute, 2024), 157-72, https://www.etui.org/publications/artificial-intelligence-labour-and-society. Kamu Hukuku bağlamında kullanımına ilişkin bknz. "Surveillance", Cornell Law School: Legal Information Institute, erişim 12 Şubat 2025, https://www.law.cornell.edu/wex/surveillance.

[209] Hazan Dicle Özer, "Mobese İzleme ve Kayıtları: Gözetim Toplumu Bağlamında Bir Değerlendirme", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 24, sy 1 (2022): 462, 1.

[210] Sara Riso, *Working Conditions - Employee Monitoring and Surveillance: The Challenges of Digitalisation* (European Foundation for the Improvement of Living and Working Conditions (Eurofound), 2020), 7.

müdahaleci, gizli ve yoğun yöntemlerle yapılan uygulamalara işaret etmektedir. Bu görüşe göre, izleme ve gözetleme arasında bir derecelendirme söz konusudur ve hukuka aykırı nitelikteki izleme faaliyetleri "gözetleme" olarak adlandırılmalıdır[211] . Ancak kanaatimizce bu türden bir ayrımın yapılması, kavramların öğretideki ve uygulamadaki kullanımını değiştirmeyeceği gibi, geçmiş araştırmaların değerlendirilmesinde karışıklıklara ve hatalı sonuçlara yol açma riskini de beraberinde getirecektir. Dolayısıyla, bu iki kavramın hukuki açıdan ayrıştırılmamasının daha uygun olacağını düşünmekteyiz.

Çalışanların denetlenmesi olgusunu ele alan akademik disiplinler, konuya farklı teorik açılardan yaklaştıkları için terminoloji tercihlerinde de ayrışmaktadır; bu doğrultuda bazı alanlar ağırlıklı olarak gözetim kavramını kullanırken, diğerleri izleme terimine yoğunlaşmaktadır[212]. Örneğin, örgüt sosyolojisi ve istihdam ilişkileri alanındaki araştırmacılar genellikle "gözetim" terimini tercih etmekte, gözetimi salt teknik bir kontrol mekanizması olarak görmek yerine, örgütsel güç ilişkileri, yönetim politikaları, çalışan direnişi ve anlam üretimi süreçlerinin bütünleşik bir parçası olarak ele almaktadırlar. Bu bağlamda gözetim uygulamalarının yönetsel meşruiyeti, politik boyutları ve çalışanlar üzerindeki etkileri sorgulanmaktadır[213]. Diğer taraftan mesleki psikoloji ve örgütsel davranış disiplini, ağırlıklı olarak "izleme" kavramına yoğunlaşmaktadır. Bu perspektif, izlemeyi sosyal veya politik bir olgu olmaktan ziyade, teknik ve işlevsel yönleri ön planda tutan, performans ve verimlilik artışı hedefleyen bir araç olarak görmektedir. Bu alandaki çalışmalar, izleme yöntemlerinin

---

[211] Ayrıntılar için bknz. Molè ve Ponce Del Castillo, "Worker Monitoring Vs Worker Surveillance", 157-72.

[212] Kirstie Ball, "Workplace Surveillance: An Overview", *Labor History* 51, sy 1 (2010): 88; Ball, *Electronic Monitoring and Surveillance in the Workplace*.

[213] Graham Sewell ve James R. Barker, "Coercion Versus Care: Using Irony to Make Sense of Organizational Surveillance", *Academy of Management Review* 31, sy 4 (2006): 934-61; G. Sewell ve J. Barker, "Performance Measurement as Surveillance: When (If Ever) Does 'Measuring Everything That Moves' Become Oppressive", *Unpublished manuscript, University of Melbourne, Parkville, Australia*, 2008; Kirstie Ball ve T. Margulis, "Monitoring and Surveillance in Call Centres: A Review and Synthesis", *New Technology, Work and Employment* 26, sy 2 (2011): 113-26; François-Xavier De Vaujany vd., "Control and Surveillance in Work Practice: Cultivating Paradox in 'New' Modes of Organizing", *Organization Studies* 42, sy 5 (2021): 675-95; Oliver G. Kayas, "Workplace Surveillance: A Systematic Review, Integrative Framework, and Research Agenda", *Journal of Business Research* 168 (Kasım 2023): 114212. Sosyolog Gary T. Marx, International Encyclopedia of the Social & Behavioral Sciences adlı eserinde gözetlemeyi, "bireylerin, grupların ve bağlamların bilgi elde etmek veya üretmek amacıyla teknik araçlar kullanılarak incelenmesi" olarak tanımlamaktadır. Ayrıntılar için bknz. Gary T. Marx, "Surveillance Studies", içinde *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)*, ed. James D. Wright (Elsevier, 2015), 733-41.

etkinliği ile bunların çalışan davranışları üzerindeki sonuçlarını incelemekte ve iş stresi, motivasyon düşüklüğü ya da sistemin manipülasyonu gibi olası olumsuz etkilere dikkat çekmektedir[214]. Bu çalışma kapsamında incelenen hukuki metin ve öğretide, belirli bir kavramın diğerine kıyasla tutarlı şekilde öne çıktığı ya da kavramlar arasında açık bir terminolojik ayrımın benimsendiği yönünde belirgin bir eğilim tespit edilememiştir[215].

Yukarıda yapılan açıklamalardan da anlaşılacağı üzere, "izleme" ve "gözetleme" kavramları arasındaki terminolojik ayrım, farklı disiplinler ve yaklaşımlar arasında henüz bir netliğe kavuşmamıştır. Öğretide gözlemlenen bu kavramsal geçişkenlik ve terim birliğinin bulunmaması nedeniyle, çalışmamız kapsamında bu iki kavram arasında katı bir ayrıma gidilmemiştir. Bu doğrultuda, metnin bütünlüğü içinde her iki terim de çalışanların denetlenmesine yönelik benzer uygulama ve araçları ifade etmek amacıyla, aralarında belirgin bir hiyerarşi veya anlam farkı gözetilmeksizin birbirlerinin yerine kullanılmıştır.

3.3. Tele Çalışma Sürecinde Kullanılan İzleme ve Gözetleme Yöntemleri

İş ilişkilerinde çalışanların faaliyetlerinin izlenmesi ve gözetlenmesine ilişkin yöntemler, yukarıda açıklandığı üzere uygulama biçimlerine (izleme) ve amaçlarına göre (gözetleme) sınıflandırılmaktadır. İzleme yöntemlerinde faaliyetlerin uygulama biçimi esas alınmakta ve bu kapsamda iki temel izleme yöntemine dikkat çekilmektedir. Bunlardan ilki, çalışanların doğrudan ve geleneksel yollarla gözlem

---

[214] Filiz Demir vd., *Örgutsel Davranış Kavramlar ve Araştırmalar-I*, ed. Bengü Hırlak (Özgür Yayınları, 2023), https://doi.org/10.58830/ozgur.pub79; Rudolf Siegel vd., "The Impact of Electronic Monitoring on Employees' Job Satisfaction, Stress, Performance, and Counterproductive Work Behavior: A Meta-Analysis", *Computers in Human Behavior Reports* 8 (Aralık 2022): 100227.

[215] Bknz. F. Burcu Savaş, "İş Hukukunda 'Siber Gözetim'", Çalışma ve Toplum 3, sy 22 (2009): 97-132; Okur, İş Hukuku'nda Elektronik Gözetleme; Artür Karademir, "İşyerinde İnternetin Özel Amaçla Kullanımı ve İşverence Gözetlenmesi", Terazi Hukuk Dergisi 10, sy 112 (2015): 56-64; Gülsevil Alpagut, "İşyerinde Kamera Gözetlemesi ve AİHM Kararları ile Tespit Edilen Esaslar", Prof. Dr. Savaş Taşkent'e Armağan, İstanbul: On İki Levha Yayıncılık, 2019, 275-313; Canan Erdoğan, Kişilik Hakkı Kapsamında İşçilerin İzlenmesi ve Gözetlenmesi (Yetkin Yayınları, 2017); Yeliz Bozkurt Gümrükçüoğlu, "İşyerinde Elektronik Gözetim Uygulamaları ve İşçinin Kişisel Verilerinin Korunması", II. Kişisel Verilerin Korunması Sempozyumu, 7 Şubat 2019, Kişisel Verilerin Korunması Kurumu, 2019, http://openaccess.ihu.edu.tr/xmlui/handle/20.500.12154/1039; Saime Duygu Kahraman Akgül, "İşçinin İşyerinde İzlenmesi ve Gözetlenmesinin Hukuki Sonuçları" (Yayınlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi Sosyal Bilimler Enstitüsü, 2020); A. Eda Manav Özdemir, "İşçinin İzlenmesi ve Gözetlenmesi", içinde Muhtelif Yönleriyle Kişisel Verilerin Korunması Hukuku, ed. Kemal Şenocak (Yetkin Yayınları, 2022).

altında tutulduğu fiziksel izleme yöntemidir. İkincisi ise teknolojik araçlar yardımıyla yürütülen ve doğrudan gözlem yerine daha dolaylı ancak kapsamlı veri toplama imkânı sağlayan elektronik izleme yöntemidir[216]. Gözetleme yöntemleri ise işverenlerin çalışanlar üzerindeki denetim faaliyetleri, işçinin davranışlarını yönetme, yönlendirme ve kontrol etme hedefleri göz önüne alınarak değerlendirilmektedir. Bu bağlamda, olası riskleri ve ihlalleri önlemek amacıyla yapılan gözetim, mevcut sorunları veya kural ihlallerini belirlemek için gerçekleştirilen tespit amaçlı gözetim, iş süreçlerinin etkinliğini ve sürekliliğini sağlama amacı taşıyan gözetim, üçüncü kişilere yönelik bilgi toplanmasına dayalı dolaylı gözetim, çalışanların performans ve verimliliklerinin değerlendirilmesine yönelik gözetim ile kanuni yükümlülüklerin yerine getirilmesi amacıyla yapılan gözetim türleri ele alınmıştır[217]. Bununla birlikte, gözetleme faaliyetleri farklı kriterler açısından da tasnif edildiğini belirtmek gerekmektedir. Mekânsal kapsam açısından bakıldığında, gözetim faaliyetleri işyeri içinde ya da dışında uygulanabilmektedir. İşyerinin niteliğine göre ise kamuya açık olan işyerlerinde ve kamuya kapalı işyerlerinde gerçekleştirilen gözetim arasında ayrım yapılmaktadır. Denetimin kaynağı açısından ise işten kaynaklanan ve özel nitelikli davranıştan kaynaklanan gözetim ayrımı söz konusudur. Şeffaflık kriterine göre gözetim faaliyetleri, açık ya da gizli yöntemlerle icra edilebilmektedir[218]. Çalışmamız kapsamında öncelikle izleme yöntemleri ayrıntılı olarak ele alınacak ardından amaç odaklı gözetleme yöntemleri incelenecektir.

---

[216] Okur, *İş Hukuku'nda Elektronik Gözetleme*, 26.

[217] Okur, İş Hukuku'nda Elektronik Gözetleme, 35-36, 103; Kahraman Akgül, "İşçinin İşyerinde İzlenmesi ve Gözetlenmesinin Hukuki Sonuçları", 29, 88-89; Orhan Ürüncan Yücel, "İşçilerin Sosyal Medya Paylaşımlarının İşveren Tarafından Denetimi ve İş İlişkisine Etkisi" (Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2018), 62; Savran, "İşçinin İşyerinde Elektronik Yöntemlerle İzlenmesi", 71; Ifeoma Ajunwa, "Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law", Louis ULJ 63, sy 21 (2018): 23; Erdoğan, Kişilik Hakkı Kapsamında İşçilerin İzlenmesi ve Gözetlenmesi, 125; Erkan Erdemir ve İlyas Çeliktaş, "Örgütsel ve Hukuki Açıdan İşyeri İzleme: Karşılaştırmalı Bir İnceleme", Kazancı Hakemli Hukuk Dergisi 19, sy 20 (2006): 88; Mehmet Tekergül, "İşyerinde Elektronik Gözetim Uygulamaları" (Yüksek Lisans Tezi, Kadir Has üniversitesi, 2010), 45.

[218] Ayrıntılı bilgi için bknz. Okur, *İş Hukuku'nda Elektronik Gözetleme*, 26.

3.3.1. Kullanılan Teknolojik Araçlara Göre Sınıflandırma

3.3.1.1. Fiziksel İzleme ve Gözetleme

Fiziksel izleme ve gözetleme, işverenin çalışanın faaliyetlerini doğrudan denetleme yetkisini, genellikle herhangi bir teknolojik araç kullanmaksızın bizzat kendisi veya bir işveren vekili ya da denetçi aracılığıyla gerçekleştirdiği bir yöntemdir[219]. Dijitalleşmenin yaygınlaşmasından önce iş ilişkileri kapsamında izleme ve gözetleme, ağırlıklı olarak fiziksel müdahaleye dayalı yöntemlerle gerçekleştirilmekteydi. Günümüzde ise teknolojik gelişmeler, işverenlerin izleme ve gözetleme yetkisini daha geniş ve sistematik bir şekilde kullanabilmesini mümkün kılmış; bu doğrultuda, çalışanların faaliyetleri yalnızca doğrudan fiziksel olarak değil, aynı zamanda çeşitli dijital araçlar vasıtasıyla sürekli olarak izlenebilir hâle gelmiştir[220].Bu çerçevede, işveren veya vekilleri tarafından sıklıkla başvurulan denetleme yöntemleri arasında; kamera ve mikrofon gibi teknolojik araçlarla yapılan gözetleme ile çalışanın ofisi, dolabı, kişisel eşyaları ve üstünü kapsayan fiziksel aramalar bulunmaktadır[221]. Bu yöntemler içerisinde, tarihsel olarak en yaygın ve sistematik biçimde uygulananlardan biri, üst aramaları ve eşya kontrolleridir[222]. Günümüzde de işverenler tarafından sıkça başvurulan üst ve eşya aramaları, işçinin temel haklarıyla çatışma potansiyeli taşımakta ve uygulamada önemli tartışmalara yol açmaktadır. Bu konuda öğretide iki

---

[219] Okur, İş Hukuku'nda Elektronik Gözetleme, 22; Simon Mark Reilly, "The Use of Electronic Surveillance and Performance Measures in the Workplace: A Qualitative Investigation" (Durham theses, Durham University, 2010), 45, http://etheses.dur.ac.uk/429/.

[220] İşe girişte kart basma, üretim miktarının sayılması veya tartılması, parça başı ücretlendirme gibi uygulamalar, izleme ve gözetlemenin eski biçimlerine örnek teşkil ettiğine ilişkin bknz. Ball, "Workplace Surveillance: An Overview", 89. Fiziksel gözetim (physical surveillance), kimi zaman elektronik gözetim (electronic surveillance) kapsamında da değerlendirilen bir izleme türü olup, bireyin rızası ve bilgisi dışında; optik ya da akustik araçlar kullanılarak bulunduğu yerin, davranışlarının ve konuşmalarının gözlemlenmesi şeklinde tanımlanmaktadır. Bknz. Ergun Özbudun, "Anayasa Hukuku Bakımından Özel Haberleşmenin Gizliliği", *Ankara Üniversitesi Hukuk Fakültesi 50.Yıl Armağanı* 1, sy 50 (1977): 271; Okur, *İş Hukuku'nda Elektronik Gözetleme*, n. 11.

[221] Mark Jeffery, "Information Technology and Workers' Privacy: Introduction Part I: Introduction", *Comparative Labor Law & Policy Journal* 23, sy 2 (2002): 260.

[222] Bu tür aramalarla işverenler genellikle yasa dışı madde kullanımı, hırsızlık veya alkol ya da silah bulundurma gibi durumları tespit etmeyi amaçlamaktadır. Daha az bilinen fiziksel arama türlerinden biri ise "çöp karıştırma" (dumpster diving) olarak adlandırılan, oldukça radikal bir yöntemdir. Bu yöntemde işverenler, çalışanların çöplerini ve geri dönüştürülen malzemelerini fiziksel olarak karıştırarak bilgi aramaktadır. Bknz. Corey A. Ciocchetti, "The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring: The Eavesdropping Employer", *American Business Law Journal* 48, sy 2 (2011): 316-17.

temel yaklaşım dikkat çekmektedir[223]. Birinci görüşe göre, iş sağlığı ve güvenliği ya da işyerinin korunması gibi açık ve meşru gerekçeler bulunmaksızın gerçekleştirilen aramalar, işçinin özel hayatının gizliliği hakkına ağır bir müdahale niteliği taşımaktadır[224]. Diğer görüş ise, üst ve eşya aramalarının meşru kabul edilebilmesi için, işverenin iş sağlığı ve güvenliği veya işyerini koruma amacıyla hareket etmesinin yanında, denetim yetkisini ölçülülük ilkesine uygun biçimde kullanması ve işçinin temel haklarına saygı göstermesi gerektiğini vurgulamaktadır[225]. Uygulamada özellikle üst ve eşya aramalarının hangi koşullar altında hukuka uygun sayılacağına ilişkin temel ilkeler ve ölçülülük kriteri çerçevesindeki hukuki yaklaşımlar bu doğrultuda ele alınmaktadır[226]. Kanaatimizce de işverenin işyerindeki güvenlik endişelerini gidermek amacıyla dahi olsa, herhangi bir somut şüphe olmaksızın genel ve sistematik biçimde yapılan üst ve eşya aramaları, işçinin kişilik haklarına ve özel hayatının gizliliğine yönelik orantısız bir müdahale teşkil etmektedir. Zira bu tür uygulamalar, çalışanın yalnızca fiziksel mahremiyetini değil, aynı zamanda insan onurunu da zedeleme potansiyeli taşımakta ve iş ilişkisi çerçevesinde bulunması gereken güven ortamını ciddi şekilde sarsmaktadır.

Tele çalışma ilişkisinde fiziksel izleme yöntemlerinin uygulanabilirliği, esasen çalışanın özel hayat alanı olan konutunun denetlenmesi gibi istisnai durumlarla sınırlıdır. İşverenin, iş sağlığı ve güvenliği önlemlerine uyulup uyulmadığını denetleme gibi amaçlarla ve yasal sınırlar çerçevesinde çalışanın evine erişimi, çalışanın rızası alınarak ve önceden bildirimde bulunularak mümkün olabilir. Ancak bu denetim, çalışanın anayasal temel hakları olan konut dokunulmazlığı ve özel hayatın gizliliği ile sınırlıdır ve keyfi bir gözetim aracına dönüşemez[227]. Bunun dışında, fiziksel izleme, doğası gereği işveren ile çalışanın aynı fiziksel ortamda bulunduğu geleneksel çalışma biçimlerine özgü bir denetim yöntemi olup, tele çalışma modelinde genel olarak kullanım alanı bulamamaktadır. Ancak, fiziksel izlemenin

---

[223] Yasin Üstün ve Ayşe Günal, "İş İlişkilerinde Bazı Yaygın Uygulamaların Kişisel Verilerin Korunması Kanunu Kapsamında Değerlendirilmesi", *Kişisel Verileri Koruma Dergisi* 2, sy 2 (2020): 64.
[224] Sevimli, *İşçinin Özel Yaşamına Müdahalenin Sınırları*, n. 85.
[225] Şükran Ertürk, *İş İlişkisinde Temel Haklar* (Seçkin, 2002), 126; Seracettin Göktaş, "Türk İş Hukukunda İşverenin İşçinin Özel Yaşamına Saygı Borcu", *Anayasa Yargısı* 38, sy 2 (2021): 25-46; Üstün ve Günal, "İş İlişkilerinde Bazı Yaygın Uygulamaların Kişisel Verilerin Korunması Kanunu Kapsamında Değerlendirilmesi", 64.
[226] Ayrıntılı bilgi için bknz. Sevimli, *İşçinin Özel Yaşamına Müdahalenin Sınırları*, 254-67.
[227] Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 188-89.

sınırlarına ve özellikle bireyin mahremiyetine müdahale potansiyeli taşıyan türlerine (örneğin üst aramaları) ilişkin geliştirilmiş hukuki ilkeler ve tartışmalar, tele çalışma modelinde başvurulan ve benzer temel hak ihlali riskleri barındırabilen elektronik izleme yöntemlerinin hukuka uygunluk denetiminde önemli bir referans ve kıyas noktası sunmaktadır.

3.3.1.2. Elektronik İzleme ve Gözetleme

İşin organizasyonu ve denetimi, insan eliyle ve makinelerle yapıldığında önemli farklılıklar göstermektedir. Bir işveren vekilinin denetimi, doğası gereği sınırlı ve fark edilebilirken; makineler yorulmadan, sürekli izleyip büyük miktarda veri işleyerek çalışanların hak ve özgürlüklerine daha müdahaleci, tehditkâr ve hatta fark edilmeksizin bir şekilde yaklaşmaktadır. Teknolojinin bu dönüşümü, daha önce de belirttiğimiz üzere 21. yüzyıl işyerlerinde izleme ve gözetim uygulamalarının türünde, erişilebilirliğinde ve yoğunluğunda önemli bir değişim yaratmıştır[228].

Teknolojinin hızlı ilerlemesi, çalışanların izlenmesi ve gözetlenmesi yöntemlerinde köklü ve kapsamlı bir dönüşüm yaratmıştır. Günümüzde işverenler, çalışanların performanslarını, davranışlarını ve faaliyetlerini takip etmek amacıyla akıllı cihazlar, dijital uygulamalar ve yazılımlar gibi ileri teknoloji araçlarını yoğun biçimde kullanmaktadır[229]. Bu durum, iş ilişkilerinde geleneksel izleme ve gözetleme yöntemlerinden önemli ölçüde farklılaşan ve çalışanlar üzerinde daha derin ve sürekli bir kontrol imkânı sunan "elektronik izleme ve gözetleme" olarak adlandırılan yeni bir gözetim türünün ortaya çıkmasına yol açmıştır[230].

Elektronik gözetleme, *"elektronik nitelikli yardımcı araçların kullanımı ile işçinin durumu ya da davranış tarzları, yazıları, konuşmaları, hareketleri ile işçinin*

---

[228] Ali Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", *Hukuk ve Adalet Eleştirel Hukuk Dergisi, Legal Yayınevi*, sy Özel Sayı (Eylül 2023): 75.
[229] Erdoğan, *Kişilik Hakkı Kapsamında İşçilerin İzlenmesi ve Gözetlenmesi*, 42.
[230] Ayrıca, öğretide işçilerin faaliyetlerinin izlenmesi bağlamında "siber gözetim" kavramı da kullanılmaktadır. Bknz. Savaş, "İş Hukukunda 'Siber Gözetim'", 97-132; Başka bir terim olan elektronik performans gözetleme kavramının kapsamı, uygulama biçimleri ve çalışanlar üzerindeki etkileri hakkında ayrıntılı bilgi için bknz. Daniel M. Ravid vd., "EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring", Journal of Management 46, sy 1 (2020): 100-126.

bağlantıda bulunduğu objeler ve işçinin çalıştığı işyeri bölümünün izlenmesi ve/veya kayıt altına alınması" olarak tanımlanmıştır[231]. Bu çerçevede, elektronik gözetleme; varlık ve devamlılık takip cihazları, konum takibi, bilgisayar, telefon ve internet kullanımının izlenmesi gibi birbirinden farklı birçok yöntemi kapsamaktadır. Öneri: "Fiziksel mesafenin ve doğrudan gözlemin ortadan kalktığı tele çalışma modelinde işverenler, iş süreçlerini yönetmek ve çalışan faaliyetlerini takip etmek için büyük ölçüde bu elektronik gözetim yöntemlerinden faydalanmaktadır.

3.3.1.3. Varlık ve Devamlılık Takip Sistemleri

Varlık ve devamlılık takip sistemleri, işyerlerinde çalışanların giriş-çıkış kontrollerini yapmak, çalışma saatleri içerisinde görev yerlerinde bulunup bulunmadıklarını denetlemek, işe geç gelme, devamsızlık veya işten erken ayrılma durumlarını izlemek amacıyla kullanılan yöntemlerdir. Teknolojinin gelişmesiyle birlikte bu sistemlerin kullanımı önemli ölçüde yaygınlaşmış ve işverenlerin çalışanları izlemesi daha kolay hâle gelmiştir[232]. Söz konusu sistemler, erişim kartları ve elektronik anahtarlar gibi konvansiyonel yöntemlerin yanı sıra; retina taraması, parmak izi ve yüz tanıma gibi biyometrik doğrulama teknolojilerinden de yararlanmaktadır[233].

Tele çalışma modelinde çalışanların fiziksel işyeriyle doğrudan temasının bulunmaması, varlık ve devamlılık takibinin geleneksel yöntemlerle yürütülmesini güçleştirmekte; bu durum, denetim süreçlerinin dijital araçlar aracılığıyla gerçekleştirilmesini zorunlu kılmaktadır. Bu bağlamda kullanılan dijital katılım ve devam takip sistemleri, yalnızca devamsızlık ya da işe geç kalma gibi temel verileri kaydetmekle sınırlı kalmamakta; aynı zamanda çalışanın görev başında bulunup bulunmadığı, günlük çalışma süresi, iş süreçlerine katılım düzeyi ile verimlilik, görev temposu ve iş disiplini gibi performans göstergelerini de algoritmik analiz yöntemleriyle izleme ve değerlendirme olanağı sunmaktadır[234]. Bu sistemler, böylece

---

[231] Okur, *İş Hukuku'nda Elektronik Gözetleme*, 201.
[232] Falque-Pierrotin, Opinion 2/2017 on Data Processing at Work, 18.
[233] A. Eda Manav, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 19, sy 2 (2015): 121; Mustafa Alp ve Sevil Doğan, "Giyilebilir Teknolojiler ve İş İlişkisine Etkileri", *Çalışma ve Toplum Dergisi* 4, sy 71 (2021): 2610; Okur, *İş Hukuku'nda Elektronik Gözetleme*, 117-19.
[234] Örneğin, çalışan devamsızlıklarını değerlendirmek amacıyla kullanılan "Bradford Faktörü" adlı formül, devamsızlıkların sıklığı ile her bir devamsızlık döneminin gün sayısını çarparak bir skor

işverenin tele çalışma modelinde dahi çalışan performansını sistematik biçimde takip edebilmesine imkân tanımaktadır[235].

3.3.1.4. Görüntü Kayıt Sistemleri ile Çalışan İzleme ve Gözetleme Uygulamaları

Görüntü kayıt sistemleri ile çalışan izleme ve gözetleme uygulamaları, işverenlerin çalışanları denetlemek amacıyla sıklıkla kullandıkları yöntemlerden biridir[236]. Öğretide, bu uygulama *"her türlü teknik araçla işçinin aktivitelerine ilişkin görüntü ve bilgilerin elde edilmesi"* şeklinde tanımlanmıştır[237]. İşverenler, işyerine giriş ve çıkışın kontrolü, üretimin işleyişinin ve verimliliğin sağlanması, işin teknik işleyişinin gözetlenmesi, işyerinde üçüncü kişilerin suç işlemesinin önlenmesi gibi çeşitli nedenlerle bu yönteme başvurabilmektedir[238].

Tele çalışanlar açısından kullanılan en yaygın yöntem ise, genellikle çalışanın kullandığı bilgisayara entegre olan veya harici olarak bağlanan bilgisayar kamerası (webcam) aracılığıyla gözetimdir[239]. Tele çalışanın bilgisayar kamerasıyla denetlenmesi; ya gerçek zamanlı olarak takip edilmesi ya da görüntülerinin sürekli veya periyodik olarak kaydedilmesi yoluyla gerçekleşmektedir. Bu yöntemde işveren, tele çalışanın sadece iş performansını ve çalışma süreçlerini değil, aynı zamanda çalıştığı fiziksel ortamı da bilgisayar kamerasıyla doğrudan gözlemleyerek kayıt altına alma imkânına kavuşmaktadır[240]. İzleme teknolojileri zaman içerisinde önemli bir dönüşüm geçirerek farklı güvenlik ve mahremiyet düzeyleri sunan sistemler hâlini almıştır. İlk nesil sistemlerden biri olan dijital video kaydediciler (digital video

---

üretmektedir. Elde edilen puan ne kadar yüksekse, ilgili devamsızlığın işyeri düzeni ve verimliliği üzerindeki olumsuz etkisi de o ölçüde artmaktadır. Bknz. Ciocchetti, "The Eavesdropping Employer", 304-6.

[235] Bu uygulamlardan biri olan DigiAtt isimli mobil ve web uygulaması, çalışanların giriş ve çıkış saatlerini, gecikme veya erken ayrılma durumlarını otomatik olarak kaydetmek amacıyla geliştirilmiştir. Bknz. Bohol Island State University – Candijay Campus, Cogtong, Candijay, Bohol vd., "Digital Attendance and Accomplishment Report Monitoring System (DIGIATT)", International Multidisciplinary Research Journal 3, sy 2 (2021): 123-33.

[236] Savran, "İşçinin İşyerinde Elektronik Yöntemlerle İzlenmesi", 97.

[237] Okur, *İş Hukuku'nda Elektronik Gözetleme*, 119.

[238] Okur, *İş Hukuku'nda Elektronik Gözetleme*, 129-36.

[239] Kahraman Akgül, "İşçinin İşyerinde İzlenmesi ve Gözetlenmesinin Hukuki Sonuçları", 57-58; Yonca Dursun, *Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Korunması* (Seçkin, 2021), 98; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 164.

[240] "What Is Webcam Monitoring?", Monitask, erişim 22 Şubat 2025, https://www.monitask.com/en/business-glossary/webcam-monitoring.

recorder) işyerlerinde çalışanlara ait görüntü kayıtlarını yerel olarak depolamakla birlikte, şifreleme ve güvenlik önlemleri açısından yetersiz olmaları nedeniyle yetkisiz erişim riskine açık sistemlerdir. Bu cihazlarda veri güvenliğine ilişkin eksiklikler, çalışanların kişisel verilerinin korunması açısından ciddi tehditler oluşturmaktadır. Buna karşılık, ikinci nesil sistemler olan ağ video kaydetme (network video recorder) teknolojileri, kamera kayıtlarını ağ üzerinden şifreli biçimde ileterek ve uzaktan erişim imkânı sunarak veri güvenliğini artırmakta; ancak internet bağlantısına dayalı yapıları nedeniyle siber saldırılara karşı daha hassas hâle gelmektedir. Bu nedenle NVR sistemlerinde çok faktörlü kimlik doğrulama, güçlü şifreleme ve güvenlik duvarları gibi ileri düzey önlemler alınması zorunludur. En gelişmiş izleme biçimini temsil eden akıllı video kaydetme (intelligent video recorder) sistemleri ise yapay zekâ destekli analiz teknikleriyle yalnızca görüntüleri depolamakla kalmayıp, çalışan davranışlarına dair anlamlı veri çıktıları da üretebilmektedir. IVR sistemleri, bulut tabanlı depolama ve analiz altyapısı sayesinde daha kapsamlı bir izleme kapasitesi sunsa da bu durum yüksek hacimli kişisel veri işlemeyi beraberinde getirdiğinden, veri koruma hukukuna uyum açısından şifreleme, anonimleştirme ve yurt dışına veri aktarımında özel hukuki değerlendirmeleri gerektiren ek güvenlik önlemlerini zorunlu kılmaktadır[241]. Bu doğrultuda kullanılan sistemler, teknolojik gelişmelere paralel olarak önemli bir dönüşüm geçirmiş ve geçirmeyi sürdürmektedir.

3.3.1.5. Dijital Konum Belirleme Sistemleri

İşverenlerin çalışanları gözetleme yöntemleri arasında, özellikle tele veya sahada çalışan personel açısından önem taşıyan uygulamalardan biri de konum takibidir. İşçinin konum takibi, günümüzde yaygın olarak GPS, hücresel ağlar (GSM/UMTS), Wi-Fi, IP adresi, Bluetooth ve RFID gibi çeşitli teknolojik araçlar kullanılarak gerçekleştirilmektedir[242]. Bu takip, genellikle işçinin kullandığı araçlara veya

---

[241] Ayrıntılı bilgi için bknz. "What Is a PVR?", EasyTechJunkie, erişim 22 Şubat 2025, https://www.easytechjunkie.com/what-is-a-pvr.htm; "NVR vs. DVR: Understanding the Key Differences | Blog Ajax", Ajax Systems, 30 Eylül 2024, https://ajax.systems/blog/nvr-vs-dvr-key-differences/; "What to Look for in a Video Surveillance Management System", Spot AI, erişim 22 Şubat 2025, https://www.spot.ai/blog/best-video-surveillance-management.

[242] Okur, *İş Hukuku'nda Elektronik Gözetleme*, 205-6; Dilek Dulay Yangın, "Avrupa İnsan Hakları Mahkemesi'nin İşçilerin Elektronik Konum Belirleme Sistemleri (GPS) İle Takip Edilmesine İlişkin 13 Aralık 2022 Tarihli Gramaxo Kararı Üzerine Değerlendirmeler", *Çalışma ve Toplum* 3, sy 82 (2024): 875; Alp ve Doğan, "Giyilebilir Teknolojiler ve İş İlişkisine Etkileri", 2602; Savran, "İşçinin İşyerinde Elektronik Yöntemlerle İzlenmesi", 91-95.

kendisine tahsis edilen telefonlara entegre edilen yazılımlar aracılığıyla yapılmaktadır[243]. İşverenler bu yöntemlerle çalışanların bulundukları konumu gerçek zamanlı olarak izleyerek, sahada bulunan işçilerin güzergâhlarını, çalışma alanlarını ve faaliyetlerini takip edebilmektedirler[244].

İşçinin konum takibinde tercih edilen yöntemlerden GPS sistemleri ve hücresel ağlar, özellikle görev alanlarının kontrolü ve güzergâhların belirlenmesinde öne çıkarken, Wi-Fi ve IP adresleri aracılığıyla yapılan izlemeler çevrim içi faaliyetlerini ve bulundukları fiziksel ortamları tespit etmek amacıyla kullanılmaktadır. Ayrıca RFID ve Bluetooth gibi teknolojiler de genellikle işyerleri içinde çalışanların hareketlerini ve erişim yetkilerini denetlemek için kullanılmaktadır[245].

İşverenler tarafından gerçekleştirilen konum takibinin uygulamada en yaygın şekli, çalışanların kullandıkları araçların takip edilmesidir. İşverenler, bu araçların konum verilerini birçok farklı amaçla kullanmaktadır. Bunlar arasında; satış ve dağıtım rotalarının etkin bir şekilde planlanması, çalışanların görevlerini verimli ve zamanında yerine getirmelerinin sağlanması, çalışma saatlerine uyumun denetlenmesi, yakıt tüketimi gibi operasyonel maliyetlerin kontrol altında tutulması ve genel olarak şirket kaynaklarının doğru ve etkin kullanılması sayılabilecektir[246]. Araç takip sistemleri, yalnızca iş aracının konum bilgilerini değil, aynı zamanda aracı kullanan işçiye dair sürücü davranışı gibi çeşitli verileri de işleyebilmektedir[247]. Ayrıca belirtelim ki, araçların içerisine yerleştirilen ve konum takibinin yanı sıra video, ses kaydetme gibi

---

[243] Ajunwa, "Algorithms at Work", 23-24.
[244] Ball, *Electronic Monitoring and Surveillance in the Workplace*, 26.
[245] "How to Track Field Employees to Increase Productivity", BuildOps, erişim 03 Mart 2025, https://buildops.com/resources/how-to-track-field-employees/; "Do Wi-Fi Indoor Positioning Systems Still Make Sense in 2025?", Mapsted Blog, erişim 03 Mart 2025, https://mapsted.com/en-in/blog/wifi-positioning-system-explained; GeoPlugin Team, "IP Tracer: Top Methods and Use Cases - GeoPlugin - Resources", GeoPlugin - Resources -, 05 Kasım 2024, https://www.geoplugin.com/resources/ip-tracer-top-methods-and-use-cases/; Inpixon, "Bluetooth RTLS: BLE Location Tracking & Positioning | Inpixon", erişim 03 Mart 2025, https://www.inpixon.com/technology/standards/bluetooth-low-energy; RFID Construction Worker Tracking: Enhancing Efficiency n' Safety on Site, RFID, 24 Mayıs 2024, https://cpcongroup.com/rfid-construction-worker-tracking/.
[246] Dulay Yangın, "Avrupa İnsan Hakları Mahkemesi'nin İşçilerin Elektronik Konum Belirleme Sistemleri (GPS) İle Takip Edilmesine İlişkin 13 Aralık 2022 Tarihli Gramaxo Kararı Üzerine Değerlendirmeler", 873-902; Uncular, "Giriş Kontrol Sistemleri, Yer Belirleme Sistemleri ve Sosyal Medya Vasıtasıyla İzleme", 1680.
[247] Uncular, "Giriş Kontrol Sistemleri, Yer Belirleme Sistemleri ve Sosyal Medya Vasıtasıyla İzleme", 1680; Ball, Electronic Monitoring and Surveillance in the Workplace, 28; Ifeoma Ajunwa vd., "Limitless Worker Surveillance", California Law Review 105, sy 3 (2017): 743-44.

özellikleri olan cihazlar işçiye dair daha fazla veri toplanmasına olanak tanıyabilmektedir[248].

Tele çalışmada ise dijital konum belirleme uygulamaları, çalışanın işini hangi fiziksel mekândan yürüttüğünü tespit etmek amacıyla yaygın bir şekilde kullanılmaktadır. Özellikle IP adresi, Wi-Fi bağlantı verisi ve GPS gibi teknolojiler aracılığıyla çalışanın evinde mi yoksa farklı bir konumda mı bulunduğu saptanabilmektedir. Bu tür konum verileri, çoğu zaman çalışanın iş görme ediminin ifasında kullandığı dizüstü bilgisayar, tablet veya mobil cihazlar aracılığıyla toplanmaktadır. Aynı amaçlarla kullanılan yeni bazı araçlar da söz konusudur. Örneğin, çalışanın fiziksel konumu giyilebilir cihazlardan (örneğin akıllı saatlerden) elde edilen ivmeölçer ve jiroskop verileriyle gerçek zamanlı hareket tanıma yöntemleri aracılığıyla da tespit edilebilmektedir. Söz konusu teknolojiler; işverene yalnızca çalışanın konumunu takip etme olanağı sunmakla kalmamakta, aynı zamanda uzak bağlantı sistemleri üzerinden toplanan oturum açma saatleri, bağlantı noktaları ve kullanılan ağlar gibi veriler aracılığıyla çalışma saatlerine uyumunu ve sisteme yetkisiz erişimlerini denetleme imkânı da sağlamaktadır[249].

3.3.1.6. Bilgisayar ve Cep Telefonu Kullanımının İzlenmesi ve Gözetlenmesi

Günümüz iş yaşamında bilgisayarlar ve cep telefonları, iletişimden veri işlemeye, belge paylaşımından çevrim içi toplantılara kadar pek çok sürecin yürütüldüğü temel araçlar hâline gelmiştir. Bu cihazların iş süreçlerinde merkezi bir rol üstlenmesi, işverenlerin çalışan faaliyetlerini izlemeye yönelik uygulamalarının da bu araçlar üzerinde giderek yaygınlaşmasına neden olmuştur. İzleme faaliyetleri kimi zaman

---

[248] İşveren, konum belirleme sistemleriyle yapılacak takip hakkında işçiyi açık ve detaylı bir şekilde bilgilendirmelidir. Ayrıca işveren, işçinin iş aracını özel amaçlarla kullanımına izin verdiği durumlarda, iş görme edimi kapsamı dışında herhangi bir izleme ve gözetleme veya veri toplama faaliyeti yürütmemelidir. Çalışma gün ve saatleri dışında konum belirleme sistemi devre dışı bırakılmalıdır. Ayrıntılı bilgi için bknz. Uncular, "Giriş Kontrol Sistemleri, Yer Belirleme Sistemleri ve Sosyal Medya Vasıtasıyla İzleme", 1680-82; Hayrunnisa Özdemir, "İşyerinde İşçilerin İzlenmesi ve İşçinin Kişilik Haklarının Korunması", *Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi* 14, sy 1-2 (2010): 231-70.

[249] Nitekim geliştirilen gerçek zamanlı ve taşınabilir bir Nesnelerin İnterneti (IoT) sistemi, çalışanların duruş ve hareketlerinden topladığı verileri konumsal davranış örüntülerinin analizi için kullanarak çalışanın iş başında olup olmadığını uzaktan tespit etme imkânı sunmaktadır. Ayrıntılı bilgi için bknz. Yongxin Zhang vd., "A Real-Time Portable IoT System for Telework Tracking", *Frontiers in Digital Health* 3 (Haziran 2021): 643042.

doğrudan bu cihazlara entegre edilen yazılımlar aracılığıyla gerçekleştirilmekte, kimi zaman ise söz konusu cihazların bağlı bulunduğu ağların trafik verilerinin analiz edilmesi yoluyla dolaylı olarak yürütülmektedir[250].

Bilindiği üzere, bilgisayar ve cep telefonları özellikle tele çalışma ilişkilerinde işin yürütülmesinde vazgeçilmez araçlar hâline gelmiştir. Bu teknolojik donanımın iş süreçlerinde merkezi bir rol üstlenmesi, işverenin çalışanların dijital faaliyetlerini daha yakından ve sistematik biçimde izleme ihtiyacını da beraberinde getirmiştir. Çalışanların dijital faaliyetleri çeşitli uygulamalar aracılığıyla ayrıntılı biçimde takip edilebilmektedir. Söz konusu uygulamalar; ekran görüntüsü alma, çevrim içi olma sürelerini raporlama, tuş hareketlerini izleme, ekran kaydı oluşturma, arama geçmişini ve tarayıcı verilerini kaydetme, kullanılan uygulamaların ve web sitelerinin analiz edilmesi gibi çok yönlü izleme ve gözetleme imkânları sunmaktadır[251]. Şunu da belirtelim ki bu araçlar, sadece zaman ve görev yönetimini kolaylaştırmakla kalmamakta; aynı zamanda performans değerlendirmesi, güvenlik risklerinin tespiti ve veri sızıntılarının önlenmesi gibi amaçlarla da kullanılmaktadır[252].

Öte yandan, özellikle iş amaçlı akıllı telefon kullanımının yaygınlaşmasıyla birlikte, cep telefonları üzerinden gerçekleştirilen izleme faaliyetleri işverenler açısından giderek daha fazla önem kazanmıştır. Belirtilen amaçla geliştirilen ve kullanılan bazı yazılımlar, işverenlere son derece geniş bir gözetim alanı sunmaktadır. Özellikle son yıllarda geliştirilen yazılımlar aracılığıyla; telefon görüşmelerinin kayıtları, kısa mesajların (hatta bazen silinen mesajların dahi) içerikleri[253], cihazın GPS verileri üzerinden anlık ve geçmişe dönük konum bilgileri ve çalışanın sosyal medya

---

[250] Melanie R Bueckert, "Electronic Employee Monitoring: Potential Reform Options", *Manitoba Law Journal* 6 (2009): 100; Ciocchetti, "The Eavesdropping Employer", 312-14.
[251] Erdoğan, *Kişilik Hakkı Kapsamında İşçilerin İzlenmesi ve Gözetlenmesi*, 80-81; Ivan Manokha, "New Means of Workplace Surveillance", *Monthly Review*, 01 Şubat 2019, 30.
[252] "ActivTrak: Work Wiser with Workforce Analytics & Productivity Insights", ActivTrak, erişim 27 Şubat 2025, https://www.activtrak.com/. Ayrıca, ekranlardaki metinlerin yapay zekâ destekli analizini mümkün kılan optik karakter tanıma (OCR) gibi teknolojiler sayesinde veri güvenliğinin sağlanması amacıyla içerik denetimi de gerçekleştirilebilmektedir. "What Is the Difference between Teramind Starter, Teramind UAM, Teramind DLP and Teramind Enterprise? | Teramind Knowledge Base", erişim 27 Şubat 2025, https://kb.teramind.co/en/articles/8790885-what-is-the-difference-between-teramind-starter-teramind-uam-teramind-dlp-and-teramind-enterprise.
[253] "Track GPS Location Of Any Smartphone | TrackMyFone", erişim 27 Şubat 2025, https://www.trackmyfone.com/gps-tracking.html.

platformlarındaki etkileşimleri gibi çok çeşitli ve oldukça kritik verilere erişim sağlanabilmektedir[254].

İşveren tarafından işçiye sağlanan bilgisayar, telefon vb. teknolojik araçların uygulamaların kullanımının denetlenmesi ve sınırlandırılması, işverenin yönetim hakkı ile işçinin temel hakları arasındaki hassas dengenin gözetlenmesini gerektiren önemli bir konudur. Temel ilke, bu araçların işin görülmesi amacına uygun olarak kullanılması olup bu amaca aykırı kullanımlar işveren tarafından kısıtlanabilir[255]. Ancak günümüz çalışma koşullarında teknolojik araçların kullanımının özel amaçla bütünüyle kural olarak yasaklanması gerçekçi bulunmamakta ve ölçüsüz kabul edilmektedir. Bu nedenle işverenlerin, yıllık yaklaşık 100 saatlik özel internet kullanımına izin vererek, yalnızca verimliliği düşüren veya güvenlik riski taşıyan sitelere erişimi objektif kriterlere dayalı olarak sınırlaması önerilmektedir[256].

3.3.1.7. Elektronik İletişim Uygulamalarının İzlenmesi ve Gözetlenmesi

İşverenler, çalışanların kullandığı çeşitli iletişim uygulamaları üzerinde izleme ve gözetleme yapabilmektedir. Bu tür faaliyetler, genellikle telefon görüşmeleri, e-postalar, kısa mesajlar (SMS) ve WhatsApp, Telegram, Messenger, Zoom gibi internet tabanlı iletişim uygulamaları üzerinden gerçekleştirilmektedir[257]. Kullanılan izleme uygulamaları, çeşitli iletişim verilerinin ayrıntılı takibine olanak tanımaktadır. Örneğin, telefon görüşmelerine ilişkin olarak; yapılan aramaların süresi, çevrilen numaralar ve gelen çağrılar arasındaki zaman aralıkları kaydedilebilmektedir. Yazılı iletişim açısından ise gönderilen ve alınan e-postaların yanı sıra kısa mesaj (Short Message Service - SMS) içerikleri izlenebilmektedir. Benzer şekilde, internet tabanlı uygulamalar üzerinden gerçekleştirilen yazılı mesajlar, sesli ve görüntülü görüşmeler ile çevrim içi toplantı kayıtları da izlenebilir ve kayda alınabilir veri türleri arasında yer almaktadır[258].

---

[254] "Hubstaff Software Features and Capabilities", Hubstaff, erişim 27 Şubat 2025, http://bestnjawnings.com/features.html.
[255] Erdem Özdemir, "İnternet ve İş Sözleşmesi: Yeni Teknolojilerin İş İlişkisine Etkileri Üzerine", *Sicil İş Hukuku Dergisi* Yıl:3, sy 10 (2008): 18.
[256] Özdemir, "İnternet ve İş Sözleşmesi: Yeni Teknolojilerin İş İlişkisine Etkileri Üzerine", 19.
[257] Süzek ve Başterzi, *İş Hukuku*, 30-33; Savran, "İşçinin İşyerinde Elektronik Yöntemlerle İzlenmesi", 136.
[258] Ciocchetti, "The Eavesdropping Employer", 321-22.

İşverenler tarafından benimsenen yaklaşımlar, sadece belirli iletişim faaliyetlerini izlemekle sınırlı kalmamaktadır. Çalışanların kullandıkları tüm bilgi ve iletişim teknolojilerini (bilgisayarlar, telefonlar, yazılımlar, ağ bağlantıları vb.) kapsayan ve bütünleşik bir şekilde çalışan izleme yöntemleri de giderek daha fazla uygulanabilmektedir. Bu tür kapsamlı ya da öğretide bazen "hepsi bir arada" (all-in-one) olarak da adlandırılan izleme sistemleri, fiziki olarak işyerindeki veya uzaktan yürütülen bütün dijital faaliyetlerin tek bir merkezi sistem üzerinden sürekli olarak izlenmesine, kaydedilmesine, takip edilmesine ve derinlemesine analiz edilmesine olanak tanımaktadır[259].

Çalışanların elektronik posta hesaplarının denetlenmesi, işverenin yönetim hakkı kapsamında başvurduğu en yaygın denetim uygulamalarından biridir. İşveren tarafından gerçekleştirilen e-posta denetiminin hukuki meşruiyeti, denetime konu olan hesabın niteliğine göre farklılık göstermektedir. İş amaçlı tahsis edilen kurumsal e-posta hesapları, karine olarak işle ilgili kabul edildiğinden, işverenin yönetim hakkı kapsamında içeriği denetlenebilmektedir[260]. İşyerinde e-posta denetimine ilişkin yaklaşımlar ise öğretide farklılık göstermektedir[261]. Bir görüşe göre, eğer işçinin özel amaçlı e-posta kullanımı açıkça yasaklanmışsa, gönderilen tüm iletilerin işle ilgili olduğu varsayılmalıdır. Bu durumda, yasağa uymayan bir işçinin e-postalarının denetlenmesi özel hayatın gizliliğini ihlal etmez ve işçinin bu yöndeki bir iddiası hakkın kötüye kullanımı olarak kabul edilebilir[262]. Daha sınırlayıcı bir başka yaklaşım ise denetimin, iletinin içeriğinden ziyade gönderici, alıcı, başlık ve zaman gibi dışsal verilerle kısıtlanması gerektiğini savunmaktadır. Bu tür bir denetimin de ancak işin devamlılığının sağlanması veya sistemsel güvenlik tehditleri gibi zorunlu hâllerde ve uluslararası standartlara uygun olarak yapılması gerektiği belirtilmektedir[263]. Genel bir ilke olarak ise, her türlü denetimin şeffaf bir politikaya dayanması, ölçülülük ilkesine riayet edilmesi, işçinin rızasının alınması ve yalnızca işin niteliğinin gerektirdiği

[259] Falque-Pierrotin, Opinion 2/2017 on Data Processing at Work, 13.
[260] Dulay, *Türk İş Hukukunda Evde Çalışma*, 231-32; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 192 vd.
[261] Dulay, *Türk İş Hukukunda Evde Çalışma*, 232; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 192 vd.
[262] Özdemir, "İnternet ve İş Sözleşmesi: Yeni Teknolojilerin İş İlişkisine Etkileri Üzerine", 20; Okur, *İş Hukuku'nda Elektronik Gözetleme*, 141.
[263] Sevimli, *İşçinin Özel Yaşamına Müdahalenin Sınırları*, 238; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 192 vd.

durumlarda başvurulması gerektiği vurgulanmaktadır[264]. Kanaatimizce, bu farklı yaklaşımlar arasında en dengeli ve hukuki geçerliliği en yüksek olan çözüm; şeffaflık, meşru amaç ve ölçülülük ilkelerini birleştiren bütüncül bir modelin benimsenmesidir. İşverenin, denetim yetkisini kullanmadan önce çalışanlarını açık ve net bir politika ile bilgilendirmesi esastır[265]. Mutlak yasaklar, işverene sınırsız bir denetim hakkı tanımaz; ancak işçinin makûl gizlilik beklentisini şekillendiren önemli bir unsurdur. Modern hukuk sistemlerinde temel hak ve özgürlüklere en az müdahale eden yolun seçilmesi gerektiğinden, denetim kademeli bir yaklaşımla ele alınmalıdır. Öncelikle genel ve içeriğe girmeyen yöntemler (dışsal veri kontrolü gibi) tercih edilmeli; yalnızca somut bir şüphe veya hukuki bir zorunluluk hâlinde, amaçla sınırlı ve orantılı olacak şekilde içeriğe yönelik kontrollere başvurulmalıdır. Bu yaklaşım, hem işverenin yönetim hakkı ve meşru menfaatlerini hem de işçinin temel bir insan hakkı olan özel hayatının gizliliğini en adil şekilde koruyacaktır.

Tele çalışma modelinde, yukarıda da belirtilen elektronik iletişim uygulamaları, işin yürütülmesi, ekip içi koordinasyon ve işverenle etkileşim açısından sıklıkla temel araçlar olarak öne çıkmakta, geleneksel işyerindeki yüz yüze iletişimin ikamesi olmaktadır. Söz konusu uygulamaların işveren tarafından denetlenmesi, fiziksel olarak

---

[264] Fuat Bayram, "Borçlar Kanunu Tasarısı Işığında İşverenin, İşçinin Kişiliğini Koruma Borcu", *İş Hukuku ve Sosyal Güvenlik Hukuku Türk Milli Komitesi* 30 (2006): 23-26.

[265] E-postaların denetlenmesinde ilişkin Anayasa Mahkemesi kararları için bknz. E.Ü. [GK], B. No: 2016/13010, 17/9/2020: Bu kararda Anayasa Mahkemesi, işverenin çalışanın kurumsal e-posta hesabını denetlemeden önce, denetlemenin hukuki dayanağı, amaçları, kapsamı, süresi ve sonuçları gibi konularda çalışanı açıkça bilgilendirmesi gerektiğini vurgulamıştır. Bilgilendirme yapılmadığı takdirde, çalışanın özel hayatına saygı ve haberleşme hürriyetinin korunacağına dair makûl bir beklenti içinde olacağının altı çizilmiştir. Derece mahkemelerinin, işverenin bu bilgilendirme yükümlülüğünü yerine getirip getirmediğini tartışmadan, hukuka aykırı olarak elde edilen e-posta içeriklerini delil olarak kabul etmesini hak ihlali olarak değerlendirmiştir. Celal Oraj Altunörgü, B. No: 2018/31036, 12/1/2021: Bu kararda, E.Ü. kararındaki ilkeler tekrar edilmekle birlikte, somut olayda farklı bir sonuca varılmıştır. Başvurucunun imzaladığı iş sözleşmesinde, kurumsal e-postanın sadece iş amaçlı kullanılacağı ve banka yönetimi tarafından haber verilmeksizin denetlenebileceğine dair açık bir düzenleme bulunduğu tespit edilmiştir. Anayasa Mahkemesi, bu sözleşme hükmünü, işverenin denetleme yetkisi ve usulü konusunda çalışana önceden yaptığı açık bir bildirim olarak kabul etmiş ve başvurucunun sözleşmeyi imzalayarak buna rıza gösterdiğini değerlendirmiştir. Bu nedenle, bilgilendirme yükümlülüğünün yerine getirildiği sonucuna vararak hak ihlali olmadığına karar vermiştir. Fırat Gerçek, B. No: 2019/25604, 21/9/2022: Bu başvuruda ise, iş sözleşmesinin feshine başka bir çalışana ait olan ve işveren tarafından verilen cep telefonundaki mesajlaşmaların delil olarak gösterilmesi söz konusudur. Mahkeme, Bölge Adliye Mahkemesi kararında atıf yapılan "İletişim Araçları Politikası" belgesinin, denetleme yetkisini, kullanım sınırlarını ve yaptırımları açıkça düzenleyip düzenlemediğinin ve bu belgenin başvurucuya özel olarak bildirilip bildirilmediğinin tartışılmadığını belirtmiştir. Başvurucuya özel bir bilgilendirme yapıldığına dair bir araştırma yapılmadığı ve bir başkasına ait telefondaki yazışmaların denetlenmesinin başvurucunun makûl beklentisine aykırı olduğu vurgulanarak hak ihlali kararı verilmiştir.

işyerinde bulunmayan tele çalışanlar açısından hem yaygın bir kontrol mekanizması sunmakta hem de konunun hassasiyetini artırmaktadır. Çalışanların genellikle kendi özel hayat alanlarında bu iletişim araçlarını kullanması, iş ve özel nitelikteki iletişimlerin birbirine karışma ihtimalini artırabilmekte, bu da toplanan verilerin kapsamı ve niteliği itibarıyla özel hayatın gizliliği ile haberleşme hürriyeti bakımından önemli hukuki sorunları gündeme getirebilmektedir. Tüm bu nedenlerle, tele çalışma modelinde kullanılan ve pek çok iletişim aracını barındıran uygulamaların denetlenmesi, işverenler için özel hayatın gizliliği ve kişisel verilerin korunması hukuku kapsamında ciddi sorumluluklar doğurmaktadır.

3.3.1.8. Sosyal Medya Hesaplarının ve Aktivitelerinin İzlenmesi ve Gözetlenmesi

Günümüzde sosyal medyanın hem bireysel hem de toplumsal düzeyde artan etkisi, çalışma yaşamına da yansımıştır. Özellikle dijital mecraların işyeri sınırlarını belirsizleştirmesi, işverenlerin çalışanların sosyal medya kullanımını denetleme yönündeki eğilimlerini güçlendirmiştir[266]. Çalışanların kişisel sosyal medya paylaşımlarının işletmenin marka değeri ve müşteri ilişkileri üzerindeki olası etkileri de bu denetim pratiklerine dayanak oluşturan başlıca gerekçeler arasında yer almaktadır[267]. Öte yandan, teknolojinin gelişimine paralel olarak internetin işyerlerinde yaygınlaşması, iş süreçlerini kolaylaştırmakla birlikte çeşitli hukuki uyuşmazlıklara da zemin hazırlamaktadır. Çalışma saatleri içerisinde sosyal medya ve diğer dijital mecraların verimsiz biçimde kullanılması; gizli bilgilerin ifşası, ticari sırların açığa çıkması ya da kurumsal itibarın zedelenmesi gibi riskleri beraberinde getirmektedir[268]. Zira sosyal medya hesaplarının yaygınlaşması ve dijital izleme teknolojilerindeki hızlı gelişmeler, işverenlere çalışanları hakkında çok daha geniş kapsamlı ve detaylı verilere ulaşma imkânı sağlamıştır. Bu bağlamda işverenler artık sadece çalışanların iş saatleri içinde gerçekleştirdikleri faaliyetleri değil, aynı zamanda

[266] Yücel, "İşçilerin Sosyal Medya Paylaşımlarının İşveren Tarafından Denetimi ve İş İlişkisine Etkisi", 21-22.
[267] Nihat Seyhun Alp, "İş Hukukunda İşçilerin Sosyal Medya Kullanımına İlişkin İşyeri İç Yönetmelikleri/Rehberler", Anadolu Üniversitesi Hukuk Fakültesi Dergisi 11, sy 1 (2025): 58, 1.
[268] Savaş, "İş Hukukunda 'Siber Gözetim'", 97; Yusuf Yiğit, "Yargı Kararları Işığında İşçinin Sosyal Medya Paylaşımı Nedeniyle İş Sözleşmesinin İşverence Feshinin Koşulları", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 26, sy 2 (2024): 982-83.

sosyal çevreleri, görüşleri, inançları, ilgi alanları, konum bilgileri ve davranışları gibi özel hayatlarına dair ayrıntılı bilgilere de erişebilmektedir[269].

Fiziksel olarak işyeri sınırlarının dışında bulunan tele çalışanların sosyal medya platformlarında gerçekleştirdikleri paylaşımlar, beğeniler, yorumlar ve etkileşimler; işverenlerce yalnızca bireysel ifade biçimleri olarak değil, aynı zamanda iş performansı, kurumsal sadakat ya da temsil yeterliliği gibi unsurlar açısından da dolaylı şekilde değerlendirilebilmektedir. Sosyal medya platformları, bu bağlamda sadece kişisel bir iletişim alanı olmaktan çıkmakta; aynı zamanda çalışanların profesyonel kimliklerinin ve kurumla olan bağlarının dışa yansıdığı bir alana dönüşmektedir. Bu eğilim, özellikle tele çalışanların dijital davranışlarının iş ilişkisi bağlamında daha sık izlenmesine ve yorumlanmasına yol açmaktadır.

3.3.1.9. Yeni Nesil İzleme ve Teknolojileri

Günümüzde, bilgi ve iletişim teknolojilerindeki gelişmeler, işverenlerin çalışanları izleme ve gözetleme uygulamalarını yaygınlaştırmakla kalmayıp daha sofistike hâle getirmektedir[270]. Yapay zekâ, nesnelerin interneti, giyilebilir teknolojiler ve nöroteknoloji gibi yenilikler, çalışanların performansını ve güvenliğini daha ayrıntılı biçimde değerlendirme imkânı sunmaktadır. Mevcut teknolojiler, konum, hareket ve biyometrik verileri sürekli olarak kaydederek işverenlere ayrıntılı bilgi sağlamaktadır. Gelecekte ise bu teknolojilerin gelişmesiyle birlikte insan faaliyetlerinin yalnızca izlenmesi değil, doğrudan uzaktan kontrol edilmesi dahi mümkün olabilecektir. Örneğin, dijital kameralar olayların nesnel olarak analiz edilmesini sağlarken, biyometrik verileri izleyebilen giyilebilir cihazlar ve mikroskobik sensörler (nöral tozlar) sayesinde çalışanların sağlık durumları veya stres seviyeleri gerçek zamanlı izlenmesine ve duruma göre önlem alınmasına imkân tanımaktadır[271]. Bu çerçevede,

---

[269] Yiğit, "Yargı Kararları Işığında İşçinin Sosyal Medya Paylaşımı Nedeniyle İş Sözleşmesinin İşverence Feshinin Koşulları", 989; Falque-Pierrotin, Opinion 2/2017 on Data Processing at Work, 12.
[270] İlke Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, Birinci baskı (Adalet Yayınevi, 2016), 1; Sencer Metin Ses ve Refik Korkusuz, "İş İlişkisinde Kişisel Verilerin Yapay Zeka Destekli Sistemler Yardımıyla İşlenmesi", *Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi* 6, sy 2 Prof. Dr. Mustafa Avcı'ya Armağan (2025): 1004, 2 Prof. Dr. Mustafa Avcı'ya Armağan; Dulay Yangın, "Avrupa İnsan Hakları Mahkemesi'nin İşçilerin Elektronik Konum Belirleme Sistemleri (GPS) İle Takip Edilmesine İlişkin 13 Aralık 2022 Tarihli Gramaxo Kararı Üzerine Değerlendirmeler", 874-75; Alp ve Doğan, "Giyilebilir Teknolojiler ve İş İlişkisine Etkileri", 2600.
[271] Fiser ve Hopkins, "Getting Inside the Employee's Head", 70-75.

geleneksel performans değerlendirme yöntemlerinin ötesine geçilerek, yeni nesil teknolojilere dayanan izleme araçları, çalışanların faaliyetlerini ve performansını değerlendirmede giderek daha merkezi bir rol oynamaktadır[272]. Aşağıda günümüz iş dünyasında kullanılmaya başlanan bu ileri düzey izleme araçları ayrıntılı olarak ele alınacaktır.

3.3.1.9.1. Nesnelerin İnterneti

Nesnelerin interneti (Internet of Things - IoT), fiziksel nesnelerin sensörler, yazılımlar ve diğer dijital bileşenlerle donatılarak, internet üzerinden veri toplamasını, iletmesini ve diğer cihaz ya da sistemlerle etkileşime girmesini sağlayan bir teknolojik altyapıdır[273]. Bu altyapı, insanlar, nesneler ve dijital sistemler arasında sürekli ve dinamik bir bilgi alışverişi ortamı oluşturmaktadır[274]. IoT'nin etki alanı, akıllı şehirlerden tarıma, lojistikten sağlık hizmetlerine kadar çok geniş bir yelpazeyi kapsamaktadır. Örneğin, üretim tesislerindeki makineler, IoT sensörleri aracılığıyla kendi bakım ihtiyaçlarını öngörerek verimliliği artırırken; tedarik zincirlerinde ise ürünlerin ve taşıma araçlarının anlık takibiyle lojistik süreçler optimize edilmektedir[275]. Bu geniş uygulama alanları içinde, iş ilişkileri bağlamında IoT'nin uygulama alanları özellikle giyilebilir teknolojiler aracılığıyla genişlemektedir[276].

---

[272] Fiser ve Hopkins, "Getting Inside the Employee's Head", 52.
[273] Alp ve Doğan, "Giyilebilir Teknolojiler ve İş İlişkisine Etkileri", 2601-2; Ozan Özparlak, *Büyük Veri Çağında Yapay Zeka Sistemlerinin Çalışma İlişkilerinde Kullanımı: Hukuki Bir Değerlendirme*, 67-68.
[274] Keyur K Patel vd., "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", International Journal of Engineering Science and Computing 6, sy 5 (2016): 6122-26; Technology Innovators, Internet of Things (IoT) in Logistics: Real-Time Tracking and Asset Management, 19 Mayıs 2023, https://www.technology-innovators.com/internet-of-things-iot-in-logistics-real-time-tracking-and-asset-management/; Opsiocloud, Internet of Things Supply Chain & Logistics Optimization, 26 Şubat 2025, https://opsiocloud.com/iot-supply-chain-logistics/.
[275] Technology Innovators, Internet of Things (IoT) in Logistics.
[276] Patel vd., "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", 6125; Dr. Heidrich Vicci, "The Impact of IoT on the Modern World A Review and Evaluation Study", SSRN Electronic Journal, 2024, 8, https://www.ssrn.com/abstract=4818308; Kunal Yogen Sevak ve Babu George, "The Evolution of Internet of Things (IoT) Research in Business Management: A Systematic Review of the Literature", Journal of Internet and Digital Economics 4, sy 3 (2024): 245-46.

3.3.1.9.2. Giyilebilir Teknolojiler

Giyilebilir teknolojiler[277], vücuda kolayca takılabilen bilgisayarlar, yazılımlar, elektronik cihazlar ve sensörleri içeren giysiler veya aksesuarlar olarak tanımlanmaktadır[278]. Bu kapsamda akıllı bileklikler, kulaklıklar, gözlükler, sensör entegreli iş eldivenleri, sağlık verilerini izleyen akıllı saatler ve yaka kartları gibi birçok cihaz örnek olarak gösterilebilir[279]. Bu teknolojiler aracılığıyla, işçilerin fiziksel konumları, hareketleri (örneğin, belirli bir görevi tamamlama süresi veya adedi), ergonomik duruşları ve hatta kalp atış hızı, stres seviyesi, vücut sıcaklığı gibi çeşitli fizyolojik verileri anlık veya periyodik olarak elde edilebilmektedir. Ayrıca, bu cihazlar sadece çalışana odaklanmakla kalmayıp, çalışma ortamındaki sıcaklık, nem, hava kalitesi ve potansiyel tehlike yaratabilecek gaz yoğunluğu gibi çevresel koşullara ilişkin verilerin toplanmasına ve analiz edilmesine de olanak tanımaktadır[280]. Bunlara ek olarak, iş kazalarını ve meslek hastalıklarını önlemeye yönelik olarak geliştirilen dış iskelet sistemleri (exo-iskeletler) [281], akıllı yelekler, kasklar ve sağlık verilerini ölçemeye yönelik uygulamalar gibi koruyucu nitelikteki giyilebilir teknolojiler,

---

[277] Bu alan "Giyilebilir Nesnelerin İnterneti (Wearable Internet of Things-WIoT)" olarak da adlandırılabilmektedir. Bknz. Irene Ioannidou ve Nicolas Sklavos, "On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications", Cryptography 5, sy 4 (2021): 5-7.

[278] Riso, *Working Conditions*, 5; Byungjoo Choi vd., "What Drives Construction Workers' Acceptance of Wearable Technologies in the Workplace?: Indoor Localization and Wearable Health Devices for Occupational Safety and Health", *Automation in Construction* 84 (2017): 31.

[279] Şirketler, çalışan verimliliğini denetlemek için çeşitli giyilebilir teknolojiler kullanmaktadır. Örneğin Amazon, çalışanlarını el hareketlerini izleyen bilekliklerle yönlendirerek verimliliği artırmaktadır. ViSafe programı ise kas hareketlerini analiz ederek ergonomi ve güvenlik odaklı raporlar sunar. Hatta bu teknoloji, Transport for London (TfL) tarafından acil müdahale personelinin performansını değerlendirmek amacıyla kullanılmaktadır. Benzer bir başka teknoloji de Kinetic firmasının REFLEX cihazıdır. Bu cihaz, tehlikeli vücut pozisyonlarını tespit ettiğinde kullanıcıyı titreşimle uyarır. Ayrıca topladığı verileri, hem bireysel hem de kurumsal güvenlik hedeflerine katkı sağlayacak şekilde analiz panellerinde sunar. Bknz. Sánchez-Monedero ve Dencik, "The Datafication of The Workplace", 23-24. Çalışan verimliliğini teknolojiyle izleme uygulamalarının çarpıcı bir örneğini Tesco sunmaktadır. Şirket, İrlanda'daki bir dağıtım merkezinde Motorola bileklik terminalleri kullanarak çalışanların görev hızlarını ve hareketlerini anlık olarak izlemiştir. Bu sistemde denetim o kadar ileri bir seviyededir ki, düşük performans gösterenler uyarılmakla kalmamış, tuvalet molaları bile verimlilik puanlamasına dâhil edilmiştir. Bu tür doğrudan performans takibinin ötesinde, geleceğin teknolojileri iş süreçlerini yeniden şekillendirmeyi vaat etmektedir. Bu doğrultuda, Google Glass gibi artırılmış gerçeklik cihazlarının süreçleri optimize etmesi, Microsoft'un geliştirdiği projeksiyon tabanlı cihazların ise iş akışlarına esneklik ve hız kazandırması beklenmektedir. Ajunwa, "Algorithms at Work", 41-42.

[280] Patel vd., "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", 6124-25.

[281] Exo-iskeletlerin tanımları gereği giyilebilir teknolojiler (wearables) kategorisine dâhil edilmediği yönünde görüşler bulunmaktadır. Bu görüşe göre, exo-iskeletler esas olarak fiziksel güç gerektiren işlerde kullanıcıya destek sağlamak amacıyla kullanılmaktadır. Bknz. Esra Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, Güncellenmiş 2. Baskı (On İki Levha Yayıncılık, 2023), 354-55.

çalışma yaşamında gittikçe yaygınlaşmaktadır[282]. Böylelikle bu tür teknolojiler, envanter yönetimi ve işlem takibinden mesleki yaralanmaların önlenmesine kadar hem çalışan performansının artırılması hem de iş sağlığı ve güvenliği uygulamalarının geliştirilmesi gibi birçok farklı görevde etkin biçimde kullanılabilmektedir[283]. Ayrıca, kurumsal sağlık stratejileri çerçevesinde, çalışanların sağlıklı yaşam tarzı davranışları geliştirmeleri, adım sayar ve aktivite takip cihazları gibi teknolojik araçların teşvikiyle desteklenmektedir[284]. Bununla birlikte, deri altına yerleştirilen mikroçipler gibi işçinin konumundan fizyolojik verilerine kadar ayrıntılı biçimde izlenmesine olanak tanıyan uygulamalar da söz konusudur[285].

Giyilebilir teknolojilerin sunduğu potansiyel faydaların yanı sıra, özellikle çalışan mahremiyeti ve veri güvenliği açısından ciddi riskler ve sakıncalar da bulunmaktadır. Bu teknolojiler, kullanıldıkları süre boyunca çalışanın hareketleri, fizyolojik durumu ve hatta bazen çevresi hakkında sürekli ve detaylı veri toplama kapasitesine sahiptir. Toplanan veriler, çoğu zaman özel nitelikli kişisel veri kategorisine girmekte ve düzenli olarak işlenip analiz edilebilmektedir. Böylece, işverene, çalışanını geleneksel yöntemlerle mümkün olmayan bir derinlikte ve süreklilikte izleme olanağı tanımaktadır[286]. Bu tür verilerin, çalışanın performansı, sağlık durumu ya da işe uygunluğu gibi önemli karar süreçlerinde kullanılması, çalışan üzerinde doğrudan baskı yaratmakta; stres, kaygı ve çeşitli duygusal tepkilere neden olabilmektedir[287].

Giyilebilir teknolojiler; çalışanın anlık konumu, fiziksel hareketleri, aktivite düzeyleri ve dinlenme süreleri gibi verileri gerçek zamanlı toplayabilme yeteneğiyle, doğası

---

[282] Alp ve Doğan, "Giyilebilir Teknolojiler ve İş İlişkisine Etkileri", 2625; Ajunwa, "Algorithms at Work", 34-42.
[283] Choi vd., "Construction Workers and Wearables", 31; Ajunwa, "Algorithms at Work", 36. Bu teknolojilere iyi bir örnek, perakende sektöründe kullanılan RetailNext programıdır. Bu program, Bluetooth düşük enerji sinyalleri aracılığıyla çalışanların ve müşterilerin mağaza içi hareketlerini izleyerek performans verileri üretmektedir. Aynı zamanda RFID çipleri kullanarak çalışanların konumunu ve güvenlik durumunu anlık olarak denetlemektedir. Benzer bir teknoloji, İspanyol Tagingenieros şirketi tarafından iş güvenliği amacıyla kullanılmaktadır. Şirket, RFID çipleri sayesinde işçilerin tehlikeli alanlara koruyucu ekipmanla girip girmedileri takip etmektedir. Bknz. Sánchez-Monedero ve Dencik, "The Datafication of The Workplace", 23-24.
[284] Ball, *Electronic Monitoring and Surveillance in the Workplace*, 25; Ajunwa, "Algorithms at Work", 37-38.
[285] Alp ve Doğan, "Giyilebilir Teknolojiler ve İş İlişkisine Etkileri", 2625; Ravid vd., "EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring", 2.
[286] Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 353-55.
[287] Ball, *Electronic Monitoring and Surveillance in the Workplace*, 69.

gereği müdahaleci bir takip aracı olarak değerlendirilebilir[288]. Bu durum, toplanan verilerin ne zaman, nasıl ve kimlerle paylaşıldığı konusunda genellikle yeterli bilgiye sahip olmayan çalışanlar aleyhine önemli bir mahremiyet riski ve bilgi asimetrisi yaratmaktadır[289]. Mahremiyete ilişkin bu endişeler, cihazların ve yazılımların barındırdığı somut güvenlik zafiyetleri ile daha da derinleşmektedir. Nitekim, ampirik çalışmalar bu teknolojilerin çok katmanlı riskler içerdiğini göstermektedir. Bir yandan, birçok fitness uygulamasının asgari güvenlik standartlarını karşılamadığı ve kullanıcı verilerini çok sayıda üçüncü tarafla paylaştığı belirlenmiştir. Diğer yandan, giyilebilir teknolojilerin ivmeölçer gibi sensörlerinden elde edilen verilerle anonim hâl getirilen kullanıcıların kimliğinin tespit edilebildiği kanıtlanmıştır. Bununla birlikte, cihazlardaki Bluetooth bağlantılarının, siber saldırganlar tarafından kolayca manipüle edilebildiği tespit edilmiştir. Örneğin saldırganlar, tekrar oynatma (replay), kaba kuvvet (brute-force) ve "Ortadaki Adam" (Man-in-the-Middle) gibi siber saldırılarla iletişimi gizlice dinleyebilmekte, şifreleri zorla kırabilmekte veya eski veri paketlerini yeniden göndererek sistemi yanıltabilmektedir[290]. Bu nedenle işveren giyilebilir teknolojilerin kullanımında aşağıda belirtilen teknik tedbirleri çok sıkı bir şekilde uygulamalıdır[291].

3.3.1.9.3. Nöroteknoloji Temelli İzleme ve Gözetleme

Nöroteknoloji, sinir sistemi ile teknolojinin etkileşimine odaklanan, özellikle beyin aktivitelerinin izlenmesi, analiz edilmesi ve yönlendirilmesi gibi potansiyeller

---

[288] Alp ve Doğan, "Giyilebilir Teknolojiler ve İş İlişkisine Etkileri", 2614.
[289] Ioannidou ve Sklavos, "On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications", 1.
[290] Ioannidou ve Sklavos, "On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications", 5; Hossein Fereidooni vd., "Fitness trackers: fit for health but unfit for security and privacy", *2017 IEEE/ACM international conference on connected health: Applications, systems and Engineering technologies (CHASE)*, IEEE, 2017, 24, https://ieeexplore.ieee.org/abstract/document/8010569/; Eric Clausing ve M. Schiefer, "Internet of Things Security Evaluation of 7 Fitness Trackers on Android and the Apple Watch", *AV TEST, Germany*, sy 1-21 (2016): 20; Qiaoyang Zhang ve Zhiyao Liang, "Security Analysis of Bluetooth Low Energy Based Smart Wristbands", *2017 2nd International Conference on Frontiers of Sensors Technologies (ICFST)*, IEEE, 2017, 421-25, https://ieeexplore.ieee.org/abstract/document/8210548/; Rohit Goyal vd., "Mind the Tracker You Wear: A Security Analysis of Wearable Health Trackers", *Proceedings of the 31st Annual ACM Symposium on Applied Computing* (New York, NY, USA), SAC '16, Association for Computing Machinery, 04 Nisan 2016, 131–136; J. J. Ho vd., "A Snapshot of Data Sharing by Select Health and Fitness Apps", conference paper presented de In Proceedings of the Seminar on Privacy Implications of Consumer Generated and Controlled Health Data, Washington, DC, USA, *Federal Trade Commission, Washington*, 07 Mayıs 2014.
[291] Bknz. Bölüm 4.5.1.

barındıran disiplinler arası bir alandır[292]. İş ilişkilerinde nöroteknoloji uygulamaları ise, çalışanların performans düzeylerini ölçme, dikkat dağılımını belirleme ve üretkenliklerini değerlendirme amacıyla kullanılabildiği gibi, işe alım süreçlerinde, terfi değerlendirmelerinde veya işten çıkarma kararlarında da etkili bir ölçüt olarak kullanılabilmektedir[293]. Bu kapsamda geliştirilen sistemlerin çeşitli kullanım alanları söz konusudur. Örneğin, çalışanların beyin dalgalarından elde edilen verileri kullanarak eğitim süreçleri kişiselleştirilmekte; EEG sensörleriyle[294] donatılmış giyilebilir teknolojiler ve göz hareketi izleyen cihazlar aracılığıyla da yorgunluk gibi riskli durumlar erken aşamada tespit edilmektedir. Ayrıca, beyin-bilgisayar ara yüzü (BCI) çipleri ve beyin aktivitelerini algılayabilen kablosuz kulaklıklar gibi ileri teknolojiler, çalışanların zihinsel durumlarını izleyerek üretkenlik artırımı ve sağlık takibi amacıyla kullanılabilecek yeni olanaklar sunmaktadır[295].

---

[292] Aliyu Aminu Ahmed ve Rukayya Aminu Muhammed, "Accessibility, Use and Effectiveness of Neurotechnology Devices for Improved Productivity in Workplace", International Journal of Scientific and Research Publications (IJSRP) 11, sy 10 (2021): 16.

[293] Anna Wexler ve Peter B. Reiner, "Oversight of Direct-to-Consumer Neurotechnologies", *Science* 363, sy 6424 (2019): 234-35; Ekaterina Muhl ve Roberto Andorno, "Neurosurveillance in the Workplace: Do Employers Have the Right to Monitor Employees' Minds?", *Frontiers in Human Dynamics* 5 (2023): 8.

[294] Çalışanların beyin aktivitelerini izlemenin en pratik yollarından biri, EEG (Elektroensefalografi) sensörleriyle donatılmış kafa bantları veya kulak içi cihazlardır. Bu giyilebilir teknolojiler, ham beyin dalgalarını toplamakta, sinyal kirliliğini temizlemekte ve özel algoritmalarla analiz etmektedir. Bu süreç sonunda, çalışanın konsantrasyon seviyesi, duygusal durumu ve zihinsel yorgunluğu gibi değerli bilgilere ulaşılmaktadır. Bknz. Ekaterina Muhl, "The Challenge of Wearable Neurodevices for Workplace Monitoring: An EU Legal Perspective", *Frontiers in Human Dynamics* 6 (Ekim 2024): 2, https://www.frontiersin.orghttps://www.frontiersin.org/journals/human-dynamics/articles/10.3389/fhumd.2024.1473893/full.

[295] İşyerinde nöroteknoloji uygulamaları kapsamında dikkat çeken yenilikçiler arasında İsrail merkezli InnerEye ve Silikon Vadisi'nde faaliyet gösteren Emotiv şirketi öne çıkmaktadır. InnerEye, çalışanlara âdeta "süper insan" yetenekleri kazandırmayı amaçlarken; Emotiv, beyin izleme teknolojilerini, uzaktan çalışanlar dâhil olmak üzere ofis ortamına taşımaktadır. Emotiv'in EEG sensörlü kulaklıkları, çalışanların stres ve dikkat düzeylerini beyin dalgaları üzerinden izlemeye imkân sağlamakta ve işyerinde performans takibi için kullanılmaktadır. Emotiv ayrıca, 2018 yılında SAP SE ile gerçekleştirdiği iş birliğiyle, Focus UX sistemi aracılığıyla çalışanların beyin verilerinden yararlanarak işyeri öğrenme ve gelişim süreçlerini kişiselleştirmeyi hedeflemiştir. İşyerinde kullanılan diğer nöroteknolojik araçlar arasında, Wenco International Mining Systems tarafından geliştirilen ve EEG sensörleriyle donatılmış bir yorgunluk izleme bandı olan SmartCap de yer almaktadır. SmartCap, çalışanların tehlikeli düzeyde uykulu hale gelmeleri durumunda Bluetooth aracılığıyla veri ileterek gerekli uyarıları sağlamakta ve özellikle madencilik ile taşımacılık gibi gece vardiyalarının ve uzun çalışma saatlerinin yaygın olduğu sektörlerde kullanılmaktadır. Buna ek olarak, göz kapağı hareketlerini takip ederek yorgunluk tespiti yapan Optalert gözlükleri de, çalışan sağlığını korumaya yönelik bir diğer örnek olarak işyerinde uygulamaya konulmuştur. Son dönemde, nöroteknoloji alanında daha ileri adımlar atan girişimler de dikkat çekmektedir. 2024 yılında teknoloji milyarderi Elon Musk'ın kurucusu olduğu Neuralink şirketi, Telepathy adı verilen beyin-bilgisayar ara yüzü (BCI) çipini ilk kez bir insana başarıyla yerleştirmiştir. Bu çerçevede, Apple da beyin dalgalarını izleyebilen yeni nesil kablosuz kulaklıklar geliştirmektedir. Apple'ın bu teknolojisi, kullanıcıların beyin aktivitelerini algılayarak stres, dikkat gibi zihinsel durumları belirlemeye yönelik veriler toplamayı hedeflemektedir. Söz konusu cihazlar, doğrudan işyeri performans takibi, çalışan sağlığının izlenmesi ve üretkenlik artırımı gibi alanlarda potansiyel kullanım imkânı sunmaktadır. Bknz. Jeremy Ben Merkelson vd.,

Dünya genelinde birçok şirket, çalışanların yorgunluk düzeylerini izlemek, dikkatlerini takip etmek, iş güvenliğini sağlamak, stresi azaltmak ve verimliliği artırarak daha uyumlu bir çalışma ortamı oluşturmak amacıyla; beyin aktivitelerini veya vücuttaki kasların birleşim noktalarındaki elektriksel hareketleri anlık ve grafiksel olarak ölçebilen giyilebilir cihazlar kullanmaya başlamıştır. Bu bağlamda sinirsel ara yüzler; saatler, kulaklıklar, baretler, şapkalar ve sanal gerçeklik gözlükleri gibi gündelik kullanım araçlarına entegre edilerek çalışma hayatında yaygın bir biçimde kullanılmaya başlanmıştır[296].

Nöroteknoloji, çalışanların zihinsel süreçlerine ilişkin kapsamlı ve ayrıntılı bilgiler sunabilmekte; kişinin bilişsel kapasitesi, konsantrasyon seviyesi, stres düzeyi ve nörolojik açıdan risk teşkil edebilecek eğilimleri gibi çeşitli parametreleri açığa çıkarabilmektedir[297]. Bunun yanı sıra, işverenlerin çalışanlara ait rastlantısal nitelikteki verilere (örneğin erken bilişsel gerileme belirtilerinin tespit edilmesine) erişim sağlamaları da mümkün olabilmektedir[298]. Bu veriler ise iş güvenliği senaryolarında anlık geri bildirimle kullanıma aktarılabilmektedir. Nöroteknolojinin çalışanların anlık zihinsel durumları hakkında sağladığı geribildirimler sayesinde, kişilerin kendi performanslarını daha etkin şekilde yönetmeleri ve iş güvenliğini artırmaları da mümkün hâle gelmektedir[299]. Özellikle dikkat eksikliği veya yorgunluk gibi durumların iş kazalarına yol açabileceği yüksek riskli mesleklerde, EEG tabanlı nöroteknolojilerin kullanılması, önleyici bir güvenlik önlemi olarak

---

"Neurotechnology Works Its Way Forward", *Seattle University Law Review Online* 48, sy 57 (2025): 60; Evan Ackerman ve Eliza Strickland, "Neurotechnology and Emotional AI Are Creating a New Kind of Line Manager", IEEE Spectrum, 19 Kasım 2022, https://www.bps.org.uk/psychologist/neurotechnology-and-emotional-ai-are-creating-new-kind-line-manager; "Neurotechnology is becoming widespread in workplaces - and our brain data needs to be protected", Healthworld, 2024, https://health.economictimes.indiatimes.com/news/health-it/neurotechnology-is-becoming-widespread-in-workplaces-and-our-brain-data-needs-to-be-protected/112652528.

[296] Nita A. Farahany, "Neurotech at Work", Harvard Business Review, Mart 2023, https://hbr.org/2023/03/neurotech-at-work.

[297] Microsoft'un yaptığı bir araştırmaya göre, art arda yapılan sanal toplantılar çalışanlarda bilişsel yorgunluğa yol açmaktadır. Şirket, bu soruna yönelik olarak Teams platformuna "Together Mode" gibi özellikler eklemiş ve toplantı aralarında verilen molaların stresi azalttığını göstermiştir. Bu uygulamalar, nöroteknolojinin iş yerindeki artan rolüne örnek teşkil etmektedir. Ayrıntılı bilgi için bknz. Muhl ve Andorno, "Neurosurveillance in the Workplace", 1-9.

[298] Nita A. Farahany, "Neurotech at Work".

[299] Arnaud Devigne, "How Neurotechnologies Can Shape The Future Of Work", Forbes, 2024, https://www.forbes.com/councils/forbesbusinesscouncil/2024/09/20/how-neurotechnologies-can-shape-the-future-of-work/; Muhl ve Andorno, "Neurosurveillance in the Workplace", 2.

değerlendirilebilmektedir[300]. Örneğin, büyük araçları kullanan sürücülerin yorgunluk ve uyku hâli gibi risklerini tespit ederek kazaların önüne geçilmesi sağlanabilmektedir[301].

Yakın gelecekte bazı sektörlerde belirtilen nöroteknolojik geri bildirim sistemlerinin artık yasal bir zorunluluk hâline gelmesi de muhtemeldir. Örneğin, madencilik, ağır taşımacılık ve havacılıkta vardiya düzenlemeleri ile iş sağlığı ve güvenliği açısından yorgunluk izleme sensörlerinin kullanımını zorunlu tutulabilecektir. Nitekim günümüzde de bazı ülkelerde, yüksek risk taşıyan işkollarında stres ve yorgunluk izleme teknolojilerinin kullanımı zorunlu tutulmakta; ayrıca, bazı endüstriyel tesislerde üretim süreçlerinin optimizasyonu amacıyla stres seviyelerini ölçen sensör sistemlerinin aktif olarak uygulandığı görülmektedir. Özellikle Çin'de, yüksek risk taşıyan işkollarında stres ve yorgunluk izleme teknolojileri aktif olarak kullanılmaktadır. Örneğin, hızlı tren sürücülerinin yorgunluk düzeylerini tespit ederek güvenliği artırmak amacıyla EEG başlıkları takmaları zorunlu tutulurken; Hangzhou Zhongheng Elektrik fabrikası gibi endüstriyel tesislerde ise çalışanların stres seviyeleri sensörlerle izlenerek hem olası psikolojik sorunların erken tespiti hedeflenmekte hem de üretim süreçleri optimize edilmektedir. Bu tür uygulamaların devlet fabrikaları ve okullar gibi farklı kurumsal ortamlara da yaygınlaştığı belirtilmektedir[302].

Nöroteknolojilerin iş ilişkilerinde kullanımına yönelik giderek artan ilgi, çalışanların zihinsel mahremiyetinin korunması, nöroveriler temelinde ortaya çıkabilecek ayrımcılık riskleri (nörodiskriminasyon) ve iş güvencesinin zayıflaması gibi önemli etik ve hukuki sorunları da beraberinde getirmektedir[303]. Günümüzde nöroteknoloji şirketlerinin büyük bölümünün, gerekli veri güvenliği standartlarına ve şeffaf bir gizlilik politikasına sahip olmadığı, ayrıca ticari kaygılarla bu konulardaki tartışmaları

---

[300] Muhl, "The Challenge of Wearable Neurodevices for Workplace Monitoring", 5.
[301] Bu tür durumlarda kamu güvenliği, bireyin zihinsel mahremiyet hakkına göre öncelikli bir değer olarak değerlendirilebilmektedir. Nita A. Farahany, "Neurotech at Work"; Zihinsel mahremiyet hakkına ilişkin yeni düzenlemler için bknz. Jeremy Ben Merkelson vd., "Neurotechnology In The Workplace: A Futuristic Reality", *Mealey's Data Privacy Report (LexisNexis)* 9, sy 6 (2023): 20.
[302] Ayrıntılı bilgi için bknz. Erica Harper, The Evolving Neurotechnology Landscape: Examining the Role and Importance of Human Rights in Regulation (The Geneva Academy of International Humanitarian Law and Human Rights, 2023), 7, https://www.geneva-academy.ch/joomlatools-files/docman-files/The%20Evolving%20Neurotechnology%20Landscape.pdf; "China Claims It's Scanning Workers' Brainwaves to Increase Efficiency and Profits", VICE, 01 Mayıs 2018, https://www.vice.com/en/article/china-brain-wave-hats-helmets-productivity/.
[303] Muhl ve Andorno, "Neurosurveillance in the Workplace", 7-9.

ön plana çıkarmaktan kaçındığı görülmektedir. Diğer yandan kullanıcılar (iş ilişkisi bağlamında işverenler) ise çoğu durumda kişisel beyin verilerinin hangi amaçlarla kullanılacağını tam olarak kavrayamadan kullanıcı sözleşmelerini onaylamaktadır[304].

İşverenlerin, iş ilişkisi kapsamında bu şirketlerden temin ettikleri teknolojik cihazlar aracılığıyla çalışanlara ait verileri işlemesi ise, kişisel veri güvenliği ve mahremiyet açısından ciddi riskler doğurmaktadır. Nöroteknolojik araçlarla toplanan beyin verileri istisnai bir nitelik taşımaktadır. Zira bu veriler, düşünceler, duygular ve karar verme süreçlerine ilişkin son derece kritik kişisel bilgileri açığa çıkarabilmektedir[305]. Nitekim beyin verilerini toplayan cihazlar çoğu zaman "sağlık" veya "kişisel gelişim" amacıyla pazarlansa da pratikte kullanıcının kişilik özellikleri, bireysel iradesi, değer yargıları, sosyal tutumları ve karar alma mekanizmaları hakkında derinlemesine çıkarımlar sunabilmektedir[306]. Elde edilen veriler aracılığıyla bireylerin duygusal durumları, uyarılma seviyeleri ve dikkat düzeyleri görünür kılınmaktadır[307]. Özellikle "sinirsel veri" olarak nitelendirilen bilgiler, söz konusu teknolojileri hem veri koruma hukuku hem de etik açıdan son derece kritik bir konuma taşımaktadır[308]. Zira bu veriler, bireyin kimliğinin belirlenmesine olanak tanıdığı için kişisel veri niteliğine sahip olup sağlık durumuna, biyometrik ve nörolojik özelliklere dair hassas bilgiler içermesi nedeniyle Genel Veri Koruma Tüzüğü'nün 9. maddesi kapsamında özel nitelikli veri olarak değerlendirilmektedir[309].

---

[304] Nicole Minielly vd., "Privacy Challenges to the Democratization of Brain Data", iScience 23, sy 6 (2020): 3.
[305] Minielly vd., "Privacy Challenges to the Democratization of Brain Data", 1.
[306] Minielly vd., "Privacy Challenges to the Democratization of Brain Data", 1.
[307] Kişinin siyasal eğilimi, uykusuzluğunun ne kadar ciddi olduğu ya da birine gerçekten âşık mı yoksa sadece geçici bir istek mi duyduğu gibi bilgiler de bu şekilde analiz edilebilmektedir. Ayrıca zaman içinde beyin işlevlerindeki değişimler izlenerek alzheimer, şizofreni veya demans gibi hastalıkların erken belirtileri fark edilebilmektedir. Epilepsi hastaları içinse, nöbet başlamadan önce uyarı alınması mümkün olmaktadır. Sporcular için geliştirilen akıllı kasklarla da beyin sarsıntıları meydana geldiği anda teşhis edilebilecektir. Bknz. Nita A. Farahany, "Neurotech at Work".
[308] Stephanie Naufel ve Eran Klein, "Brain–Computer Interface (BCI) Researcher Perspectives on Neural Data Ownership and Privacy", Journal of Neural Engineering 17, sy 1 (2020): 2. Ayrıca, söz konusu teknolojilerin etik tartışmaları yalnızca veri mahremiyeti ekseninde yürümemektedir. Beyin uyarımı gibi müdahaleci uygulamalar, bireylerin davranışlarını veya kişilik özelliklerini değiştirme riski taşıdığından, bireysel özerkliğin korunması ilkesini de ön plana çıkarmaktadır. Bu teknolojilerin hem veri toplama hem de uyaran gönderme kapasitesi, hukuki ve etik çerçevenin bütüncül bir yaklaşımla ele alınmasını zorunlu kılmaktadır. Bknz. Kate S. Gaudry vd., "Projections and the Potential Societal Impact of the Future of Neurotechnologies", Frontiers in Neuroscience 15 (Kasım 2021): 1, https://www.frontiersin.orghttps://www.frontiersin.org/journals/neuroscience/articles/10.3389/fnins.2021.658930/full; Kişisel Verileri Koruma Kurumu, 6698 sayılı Kanunda Yer Alan Temel Kavramlar (Kişisel Verileri Koruma Kurumu, 2020).
[309] Beyin verilerinin kavramsal çerçevesine ilişkin öğretideki tartışmalar için bknz Muhl, "The Challenge of Wearable Neurodevices for Workplace Monitoring", 5-6.

Nöroteknoloji uygulamalarıyla elde edilen beyin verilerinin işlenmesi, sadece başlangıçtaki kullanım amaçlarıyla sınırlı kalmayıp, bireyler hakkında daha kapsamlı ve öngörülmesi güç bilgilerin ortaya çıkarılması riskini de beraberinde getirmektedir[310]. Öğretide, doğrudan elde edilen bu tür beyin verileri birincil veriler (first-order data) olarak adlandırılmaktadır. Bu verilerin, farklı kaynaklarla birleştirilerek çalışanların gelecekteki performansları, bilişsel kapasiteleri ve davranışsal eğilimleri hakkında öngörülerde bulunulmasına imkân sağlamakta ve bu şekilde elde edilen bilgiler ise "ikincil çıkarımlar" (second-order inferences) olarak adlandırılmaktadır[311]. İkincil çıkarımların işlenmesi ise bireylerin farkında olmadan çok daha kapsamlı profillerin oluşturulmasına zemin hazırlamakta ve kişilik haklarının ihlal edilmesi riskini arttırmaktadır.

Birleşik Krallık'ın bağımsız veri düzenleyici kurumu olan Information Commissioner's Office (ICO) 2023 tarihli raporunda 2028 sonuna kadar güvenlik, çalışan sağlığı ve işe alım gibi nedenlerle iş ilişkileri kapsamında bedene doğrudan müdahale etmeyen nöroteknolojilerin kullanımında önemli bir artış yaşanacağını öngörmüştür[312]. İş ilişkilerindeki güç dengesizliği ve beyin verilerinin hassas doğası nedeniyle, söz konusu teknolojilerin kullanımına ilişkin açık, adil ve etkin bir hukuki düzenlemenin oluşturulması gerekliliği kaçınılmaz hâle gelmiştir[313]. Aksi takdirde, çalışanların rızası dışında hassas sağlık verilerinin ifşa olması, toplanan ham nöroverilerden hareketle ikincil çıkarımlar yapılarak bireylerin profillenmesi ve bu temelde nöro-ayrımcılık gibi yeni nesil hak ihlallerinin ortaya çıkması kaçınılmaz olacaktır.

3.3.1.9.4. Yapay Zekâ Destekli İzleme ve Gözetleme Sistemleri

Yapay zekâ sistemleri, büyük veri kümelerini karmaşık algoritmalar aracılığıyla işleyerek[314], izleme, gözetleme ve karar alma süreçlerinde giderek daha yaygın

[310] Minielly vd., "Privacy Challenges to the Democratization of Brain Data", 1.
[311] Muhl, "The Challenge of Wearable Neurodevices for Workplace Monitoring", 2.
[312] ICO, ICO Tech Futures: Neurotechnology (Information Commissioner's Office, 2023), 14, https://ico.org.uk/media/about-the-ico/research-and-reports/ico-tech-futures-neurotechnology-0-1.pdf.
[313] Merkelson vd., "Neurotechnology Works Its Way Forward", 61.
[314] Erdem Büyüksağiş, "Yapay Zeka Karşısında Kişisel Verilerin Korunması ve Revizyon İhtiyacı", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 18, sy 2 (2021): 529-30, 2.

biçimde kullanılmaktadır. Bununla birlikte, kişisel verilerin korunması, özel hayatın gizliliği ve ayrımcılık yasağı gibi temel hak ve özgürlükler bakımından ciddi riskler doğurmaktadır[315]. Özellikle algoritmaların karar alma süreçlerinde şeffaf olmaması (diğer bir ifadeyle "kara kutu" etkisi)[316] ve bu algoritmaların, ayrımcı sonuçlar doğurabilmesi, söz konusu teknolojilerin hem etik hem de hukuki denetime tabi tutulmasını ve insan hakları ile uyumlu şekilde kullanılmasını zorunlu kılmaktadır[317].

Yapay zekâ, çalışanlar açısından insan kapasitesini artırma, yaratıcılığı destekleme, yeterince temsil edilmeyen grupların iş gücüne katılımını teşvik etme ve ekonomik, sosyal ve çevresel eşitsizlikleri azaltma potansiyeline sahiptir. Bununla birlikte, yapay zekâ sistemleri aynı zamanda otoriter denetim mekanizmalarını güçlendirme riski taşımakta; izleme, puanlama, teşvik ve yaptırımlar aracılığıyla çalışanlar üzerinde baskı kurabilmektedir. Yapay zekâ destekli izleme araçları tarafından toplanan verilerin, başlangıçtaki kullanım amacının ötesinde ve beklenmedik şekillerde manipüle edilerek ikincil çıkarımlar için kullanılması da mümkündür. Ayrıca, bu tür sistemlerin tarafsızlık iddiasına karşın, mevcut ön yargıları yeniden üretebilme ve ayrımcılığı derinleştirme potansiyelleri bulunmaktadır[318].

---

[315] Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 50-51; Ömer Faruk Ereken, "Yapay Zeka Tabanlı Personel Seçim Sistemi Uygulaması" (Yayınlanmış Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, 2021), iv; K. Dündar ve A.C. Ağaçkayak, "Yapay Zeka ve Makine Öğrenmesi İle İnsan İlişkileri Analizi", içinde Mühendislikte Yenilikçi Yaklaşımlar-2, 1. (Eğitim Yayinevi, 2024), 128; Uğur Karaboğa, "İşe Alım Süreçlerinde Yapay Zeka Teknolojilerinin Kullanımı" (Yüksek Lisans Tezi, İstanbul Medipol Üniversitesi Sosyal Bilimler Enstitüsü, 2020), 32-33; Hoofnagle vd., "The European Union General Data Protection Regulation: What It Is and What It Means", 469.

[316] Kara kutu (black box) kavramı, bir sistemin iç işleyişinin dışarıdan görülemediği, yalnızca girdiler ve çıktılar üzerinden değerlendirilebildiği durumları tanımlar. Bu kavram, özellikle yapay zekâ sistemlerinde, algoritmanın hangi verilerle nasıl bir sonuca ulaştığının kullanıcılar ya da denetçiler tarafından anlaşılmasının mümkün olmadığı durumları ifade etmek için kullanılmaktadır. Kullanılan algoritmalar, bazı durumlarda kişisel verilerin nasıl işlediği açık biçimde izlenebilirken, bazı durumlarda ise karar alma süreci dışarıdan gözlemlenemeyen ve iç işleyişi anlaşılamayan bir "kara kutu" niteliği taşıyabilmektedir. Özellikle yüksek hacimli veri setlerinin güçlü işlem kapasitesine sahip sistemler tarafından analiz edilmesiyle ortaya çıkan çıktılar, teknik olarak hesaplanabilir olsa da; bu çıktıların nasıl üretildiği, süreçlerin karmaşıklığı nedeniyle insanlar tarafından pratikte takip edilemez ve açıklanamaz hale gelmektedir. Bknz. Osman Gazi Güçlütürk, "Türk Hukukunda Makine Öğrenmesine Dayalı Yapay Zekada Verinin Hukuka Uygun Şekilde Kullanılması" (Doktora Tezi, Galatasaray Üniversitesi, 2021), 38.

[317] Yiliyaer Abudureyimu ve Yucel Ogurlur, "Yapay Zekâ Uygulamalarının Kişisel Verilerin Korumasına Dair Doğurabileceği Sorunlar ve Çözüm Önerileri", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi 20, sy 41 (2021): 766; Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 86.

[318] Yeliz Bozkurt Gümrükçüoğlu ve Gülnihal Ahter Yakacak, "Yapay Zekânın İşe Alım Süreçlerinde Kullanımı ve Algoritmik Ayrımcılık", *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 72, sy 4 (2024): 1701 vd.; Antonio Aloisi ve Elena Gramano, "Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context", *Special Issue of Comparative Labor Law & Policy Journal* 41, sy 1 (2019): 119-20.

İş ilişkilerinde yapay zekâ teknolojileri, işe alım süreçlerinde adayların özgeçmişleri ile sosyal medya profillerinin taranmasından[319]; video mülakatlarda jest, mimik ve ses tonu gibi ifadelerin analizine kadar uzanan uygulamalarıyla[320] başlayarak, iş ilişkisinin tüm yaşam döngüsünü kapsayan bir etki alanı yaratmaktadır. İş ilişkisi kurulduktan sonra ise, çalışan performansının değerlendirilmesi, iş organizasyonunun şekillendirilmesi ve hatta iş sözleşmesinin sona erdirilmesi gibi süreçlerde bu sistemlerin kullanımı giderek artmaktadır[321].

Günümüzde yapay zekâ destekli algoritmalar, risk analizi, mesleki eğitim ve kariyer gelişimi, iş sağlığı ve güvenliği, performans değerlendirmesi, iş organizasyonu ve çalışma süreçlerinin yönetimi gibi birçok alanda işverenlerin en önemli yardımcı araçlarından biri hâline gelmiştir[322]. Mobil cihazlar, giyilebilir teknolojiler ya da işletme donanımlarına gömülü sistemler aracılığıyla toplanan veriler, yapay zekâ algoritmalarıyla analiz edilerek çalışanların fiziksel ve psikolojik durumlarına ilişkin değerlendirmelerde kullanılmaktadır. Tele çalışanlar açısından ise ekran kayıtları, internet kullanımı ve zaman yönetimi analizleri gibi izleme araçlarıyla entegre edilerek daha detaylı bir denetim altyapısı oluşturulabilmektedir[323]. Böylelikle elde edilen verilerin derinlemesine incelenmesiyle çalışanların performansına dair ayrıntılı çıkarımlar yapılabilmekte, çalışan hakkında daha kapsamlı ve isabetli değerlendirmeler mümkün hâle gelmektedir.

Yapay zekâ algoritmaları, yalnızca çalışma performansına ilişkin verilerle sınırlı kalmayıp, müşteri geri bildirimleri gibi dolaylı izleme verilerini de analiz ederek çok boyutlu performans değerlendirmelerini mümkün kılmaktadır[324]. Bu analizlerin, iş

---

[319] Bozkurt Gümrükçüoğlu ve Yakacak, "Yapay Zekânın İşe Alım Süreçlerinde Kullanımı ve Algoritmik Ayrımcılık", 1711-12; Yiğitcan Çankaya, *Yapay Zekanın İş İlişkisine Etkileri* (On İki Levha Yayıncılık, 2024), 170-73; Ezgi Sima Çelik, "İşe Alımda Adayın Kişisel Veri Güvenliği: Yapay Zeka Destekli Video Mülakat Uygulamaları", *Kişisel Verileri Koruma Dergisi* 6, sy 1 (2024): 1, 1.

[320] Bozkurt Gümrükçüoğlu ve Yakacak, "Yapay Zekânın İşe Alım Süreçlerinde Kullanımı ve Algoritmik Ayrımcılık", 1715-17; Selma Kılıç Kırılmaz ve Çağdaş Ateş, "İşe Alımlarda Yapay Zekâ Kullanımı: Kavramsal Bir Değerlendirme", *Journal of Business and Trade* 2, sy 1 (2021): 46; Çelik, "İşe Alımda Adayın Kişisel Veri Güvenliği", 1-13; Ses ve Korkusuz, "İş İlişkisinde Kişisel Verilerin Yapay Zeka Destekli Sistemler Yardımıyla İşlenmesi", 91.

[321] Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 52-62.

[322] Lisa Kresge, Data and Algorithms in the Workplace: A Primer on New Technologies, t.y., 22-42.

[323] Adam Campbell, "Security and Privacy Analysis of Employee Monitoring Applications" (Master Thesis, University of Waterloo, 2023), 32-35, http://hdl.handle.net/10012/19724.

[324] Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 59; Tüketici kaynaklı derecelendirme sistemleri, online yemek siparişlerinde "hız-kurye-lezzet" kategorilerinde

gücü piyasasına dair büyük veri (big data) kümeleriyle birleştirilmesi sonucunda, çalışanların ücretlendirilmesi, eğitim ihtiyaçları, pozisyon uygunlukları ve hatta işten çıkarma gibi kritik kararlar için destek mekanizmaları oluşturulmaktadır[325].

Yapay zekâ teknolojilerinin, fiziksel, sosyal ve ekonomik parametreleri yüksek doğrulukla analiz edebilmesi, yalnızca mevcut performansın değil, gelecekteki potansiyelin de öngörülmesine olanak tanımaktadır. Bu çerçevede, terfi süreçleri, performans değerlendirmesi, ücretin belirlenmesi[326], kariyer gelişimi ve kişiye özel eğitim programlarının planlanması gibi kritik insan kaynakları kararlarında daha veri temelli bir yaklaşım benimsenebilmektedir [327]. Ayrıca, çalışanlara anlık geri bildirim sunulması sayesinde kişiselleştirilmiş mesleki gelişim stratejileri geliştirilebilmekte; tahmine dayalı analiz yöntemleri (predictive analytics) aracılığıyla da işten ayrılma eğilimleri gibi stratejik öneme sahip olgular önceden tespit edilerek önleyici politikalar oluşturulabilmektedir[328].

İş ilişkilerinde yapay zekâ kullanımının sağladığı avantajların yanında belirli kısıtlılıkları ve riskleri de söz konusudur. Yapay zekâ ile yapılan değerlendirmelerin

---

yıldızlı puanlama ile yaygınlaşırken, restoranlarda da tabletler aracılığıyla uygulanmaktadır. Ziosk gibi şirketler, Olive Garden ve Applebee's gibi restoran zincirleri için tabletler üretmekte, Chili's ise 823 restoranına 45.000'den fazla tablet yerleştirerek müşterilerden memnuniyet anketleri doldurmalarını istemektedir. Bu anketler, çalışanların performans değerlendirmelerine katkı sağlamaktadır. E. Sipahi Döngül ve E. Artantaş, "Örgütlerde Algoritmik Yönetim Uygulamaları", içinde Sosyal Beşeri ve İdari Bilimler Alanında Uluslararasi Araştırmalar XI (Egitim Yaymevi, 2022), 143.

[325] Ozan Özparlak, Büyük Veri Çağında Yapay Zeka Sistemlerinin Çalışma İlişkilerinde Kullanımı: Hukuki Bir Değerlendirme, 179; Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 58; G Madhumita vd., "AI-powered Performance Management: Driving Employee Success and Organizational Growth", 2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST), Nisan 2024, 209, https://ieeexplore.ieee.org/document/10578371.

[326] Ücretin belirlenmesinde yapay zekâ kullanıma ilişkin ayrıntılı bilgi için bknz. Kuldeep Sharma vd., "A Method Leveraging AI to Forecast Employee Performance during Work Hours and Propose Appropriate Salary Adjustments", 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Mayıs 2024, 1-6, https://ieeexplore.ieee.org/document/10601739.

[327] Örneğin, yapılan bir çalışmada, çalışan performansı; yaş, eğitim, iş stresi ve iş-yaşam dengesi gibi değişkenler kullanılarak, insan müdahalesini en aza indiren bir makine öğrenmesi modeliyle objektif olarak değerlendirilmiştir. Modelin başarısı doğruluk (accuracy), kesinlik (precision), duyarlılık (recall) ve F1 skoru gibi metriklerle doğrulanmış, böylece değerlendirme sürecinin kişisel ve kurumsal ön yargılardan arındırılması hedeflenmiştir. Ayrıntılı bilgi için bknz. Zannatul Nayem ve Md. Aftab Uddin, "Unbiased employee performance evaluation using machine learning", *Journal of Open Innovation: Technology, Market, and Complexity* 10, sy 1 (2024): 100243.

[328] Stebin George vd., "Predicting Employee Attrition Using Machine Learning Algorithms", *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, Aralık 2022, 700-705, https://ieeexplore.ieee.org/document/10074131.

yalnızca nicel ölçütlere indirgenmesi, insan emeğinin deneyim, sezgi, empati ve takım çalışması gibi niteliksel boyutlarının göz ardı edilmesi riskini beraberinde getirmektedir. Ayrıca bu durum, söz konusu sistemlerin karmaşık ve duygusal yoğunluğu yüksek işlerde yetersiz kalmasına neden olabilmektedir[329]. Bu kapsamda çalışanların kapsamlı şekilde gözetlenmesi ve analiz edilmesi, işletmesel hedeflere ulaşmayı kolaylaştırsa da çalışanların özel hayatın gizliliği, kişisel verilerin korunması ve insan onuruna saygı gibi temel haklarını ihlal riski taşımaktadır[330].

Yapay zekâ destekli otomatik karar verme sistemlerinin şeffaflık ve insan müdahalesinden yoksun olması, haksız işten çıkarmalar[331] ve kişisel veri ihlalleri[332] gibi ciddi hukuki sorunlara yol açabilmektedir. Ayrıca belirtelim ki, yapay zekânın yüksek analiz gücü sayesinde mevcut verilerden ikincil çıkarımlar üretilebilmesi yeni

[329] Scott Nicholas Pletcher, "Practical and Ethical Perspectives on AI-Based Employee Performance Evaluation", OSF Preprints, OSF Preprints, Center for Open Science, 28 Nisan 2023, 8-9, 29yej, https://ideas.repec.org//p/osf/osfxxx/29yej.html.

[330] Madhumita vd., "AI-powered Performance Management", 209.

[331] Örneğin, Amazon'un kullandığı otomatik veri analiz sistemleri, çalışan performansını sürekli izleyip değerlendirmekte ve üretkenlik seviyelerine göre işten çıkarmalar yapılmasına yol açmaktadır. Bu sistemde, çalışanlar "time off task" (TOT) adı verilen bir metriğe göre değerlendirilmektedir. Eğer bir çalışanın TOT süresi sık sık yüksek seviyelere ulaşırsa, uyarılar yapılmakta, hatta otomatik olarak işten çıkarma işlemleri devreye sokulmaktadır. Baltimore'daki bir dağıtım merkezinde her yıl yalnızca düşük üretkenlik nedeniyle personelin yüzde 10'undan fazlasının işine son verilmesi, bu sistemlerin iş gücü üzerindeki etkisini açıkça ortaya koymaktadır. Bu uygulama, Amazon'un Kuzey Amerika genelinde 125.000'den fazla tam zamanlı çalışanı bulunan 75'ten fazla dağıtım merkezine yayıldığında, yapay zekânın izleme kapasitesinin binlerce çalışanın işini kaybetmesine neden olabileceği bir tablo ortaya çıkmaktadır. Performansı objektif verilerle ölçmeyi amaçlayan bu sistemler, aynı zamanda çalışanlar üzerinde yoğun baskı yaratmakta ve bu durum etik ve hukuki soruları gündeme getirmektedir. Bknz. Colin Lecher, "How Amazon Automatically Tracks and Fires Warehouse Workers for 'Productivity'", The Verge, 25 Nisan 2019, https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations.

[332] Hollanda Uber'de çalışan üç sürücü, geçmişte iyi performans göstermelerine rağmen Uber'in otomatik karar mekanizması tarafından "dolandırıcılık" gerekçesiyle işten çıkarılmıştır. Şirket, sürücülerden birinin çok sayıda yolculuğu iptal ettiği ve bu iptallerde sahtecilik yaptığı iddiasında bulunmuş; diğer iki sürücüyü ise sahte hesaplarla yüksek ücretli yolculuklar gerçekleştirmekle suçlamıştır. Uber, karar sürecinin algoritmalarla yürütüldüğünü kabul etmiş, ancak sürece ilişkin kullanılan kriterler ve bu kriterlerin ağırlıkları gibi detayları ticari sır gerekçesiyle sağlamayı reddetmiştir. Sürücüler, GDPR'nin 15/1-h maddesine dayanarak, otomatik karar alma sürecinin altında yatan mantık, kullanılan faktörler ve bu kararın kendileri üzerindeki etkilerini öğrenmek istemiştir. Ancak Uber, bu talepleri geri çevirmiştir. Bunun üzerine sürücüler, Uber'in otomatik karar alma sisteminin GDPR'nin 22. ve 15/1-h maddeleri kapsamındaki haklarını ihlal ettiği gerekçesiyle hukuki yollara başvurmuşlardır. Mahkeme, Uber'in GDPR'nin bilgi sağlama yükümlülüğünü yerine getirmediğine ve karar sürecinde anlamlı bir insan müdahalesinin bulunmadığına karar vermiştir. Bu nedenle Mahkeme, Uber'in sürücülere sürece dair daha fazla bilgi sağlamasına ve idari para cezası ödemesine hükmetmiştir. ECLI:NL:GHAMS:2023:793, 200.295.742/01 (Amsterdam Bölge Mahkemesi 05 Ekim 2023), https://5b88ae42-7f11-4060-85ff-4724bbfed648.usrfiles.com/ugd/5b88ae_9f6a8251f07b4789852d1fdc171b9475.pdf.

sorunlar doğurmaktadır[333]. Örneğin, görünüşte zararsız performans metrikleri, algoritmalar tarafından işçinin sağlık durumu, sendikal aidiyeti ya da psikolojik profili gibi hassas nitelikte verilere dönüştürülebilmekte ve bu durum işçinin kişisel verilerinin hukuka aykırı olarak işlenmesine neden olabilmektedir. İşçilerin temel haklarının korunabilmesi için yapay zekânın karar alma süreçlerine etik ve şeffaf denetim mekanizmalarının entegre edilmesi gerekmektedir[334]. Bu yaklaşım hem performansın doğru ölçülmesini hem de çalışanlar arasında daha adil ve hukuka uygun bir değerlendirme yapılmasını sağlayacaktır.

Tele çalışma bağlamında yapay zekâ destekli izleme ve gözetleme uygulamaları ise fiziksel mekândan bağımsız çalışanların dijital ortamda sürekli denetimini mümkün kılarak işverenlerin kontrol yetkisini yeniden tanımlamaktadır. Ekran süresi, tuş vuruşları, çevrim içi etkinlikler ve görev tamamlama süreleri gibi davranışsal verilerin toplanarak algoritmalar aracılığıyla analiz edilmesine dayanmaktadır. Bu teknolojiler aracılığıyla yalnızca üretkenlik düzeyleri değil, aynı zamanda dikkat dağınıklığı, motivasyon eksikliği ya da işten ayrılma eğilimleri gibi öngörüsel veriler de değerlendirilebilmektedir[335]. Ancak, çalışanların çevrim içi faaliyetlerinin bu denli ayrıntılı şekilde izlenmesi, özel hayatın gizliliği ve kişisel verilerin korunması bakımından ciddi riskler barındırmakta; uzaktan çalışmanın sunduğu özerklik olanaklarını görünmez, fakat sürekli bir dijital denetim rejimiyle sınırlandırmaktadır. Bu nedenle, tele çalışma ilişkilerinde kullanılan yapay zekâ destekli izleme ve gözetleme araçlarının, yalnızca verimlilik ve iş süreçlerinin optimizasyonuna katkısı açısından değil, aynı zamanda çalışanların kişisel verilerinin korunması, özel hayatın

[333] Güçlütürk, "Türk Hukukunda Makine Öğrenmesine Dayalı Yapay Zekada Verinin Hukuka Uygun Şekilde Kullanılması", 95; Murat Volkan Dülger, "Yapay Zeka Teknolojileri ve Veri Koruma Hukuku (Artificial Intelligence Technologies and Data Protection Law)", SSRN Scholarly Paper no. 3792333, Rochester, NY, 24 Şubat 2021, 3-4, https://papers.ssrn.com/abstract=3792333; Ses ve Korkusuz, "İş İlişkisinde Kişisel Verilerin Yapay Zeka Destekli Sistemler Yardımıyla İşlenmesi", 1029; Başak Ozan Özparlak ve Müge Çetin, "ChatGPT ve Üretici Yapay Zekâ Modellerinde Mahremiyet ve Güvenliğin Hukuki Boyutu", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 29, sy 2 (2023): 1021, 2.

[334] Angelica Salvi del Pero vd., Using Artificial Intelligence in the Workplace: What Are the Main Ethical Risks? (OECD, 2022), 31, https://www.oecd-ilibrary.org/social-issues-migration-health/using-artificial-intelligence-in-the-workplace_840a2d9f-en.

[335] Antonio Aloisi ve Valerio De Stefano, "Essential Jobs, Remote Work and Digital Surveillance: Addressing the COVID-19 Pandemic Panopticon", International Labour Review 161, sy 2 (2022): 296-99.

gizliliği ve temel hak ve özgürlükleri üzerindeki etkileri bakımından da çok boyutlu ve bütüncül bir hukuki değerlendirmeye tabi tutulması gerekmektedir[336].

3.3.2. Amaçlarına Göre Sınıflandırma

3.3.2.1. Tespit Amaçlı İzleme ve Gözetleme

Tespit amaçlı izleme ve gözetleme; işverenin, işçinin iş ilişkisi kapsamında gerçekleştirdiği belirli bir hukuka aykırı ya da sözleşmeye aykırı davranışına ilişkin somut ve ciddi şüphelerin varlığı durumunda başvurduğu, hedef odaklı bir kontrol yöntemidir. Genel ve sürekli nitelikteki izleme ve gözetleme uygulamalarından farklı biçimde, bu yöntem yalnızca belirli bir ihlal şüphesinin varlığı durumunda uygulanabilmektedir. Yöntemin temel amacı ise şüphe duyulan kusurlu davranışın somut şekilde tespit edilmesi ve ilgili ihlalin açık ve tartışmaya mahal vermeyecek biçimde ortaya konulmasıdır. Bu yöntemin uygulanabilmesi için soyut kuşkular yeterli olmayıp, belirli bir olaya veya delile dayanan ciddi bir şüphenin varlığı aranmaktadır[337].

İşverenin haklı fesih nedenlerini ispat etmesi amacıyla veya işçinin iş ilişkisi kapsamında hırsızlık, veri sızdırma gibi suç teşkil eden fiillerde bulunduğu şüphesi doğduğunda, tespit amaçlı gözetleme yöntemi vasıtasıyla elde ettiği bulgular kritik önem taşımaktadır. Çalışanın işletmeye ait gizli belgeleri üçüncü şahıslara aktardığına dair somut şüphelerin bulunması hâlinde, çalışanın elektronik posta trafiğinin veya bilgisayar kullanımının tespit amaçlı izleme ve gözetleme yöntemleriyle denetlenmesi ve elde edilen verilerin olası bir uyuşmazlıkta mahkemeye delil olarak sunulması bu gözetim türüne örnek olarak verilebilecektir[338].

3.3.2.2. Önleme Amaçlı İzleme ve Gözetleme

Önleme amaçlı izleme ve gözetleme, işçilerin gelecekte ortaya çıkabilecek sözleşmeye aykırı veya hukuka aykırı davranışlarını önceden engellemek amaçlamaktadır. Bu

---

[336] Aloisi ve De Stefano, "Essential Jobs, Remote Work and Digital Surveillance", 300-303.
[337] Okur, *İş Hukuku'nda Elektronik Gözetleme*, 25.
[338] Savaş, "İş Hukukunda 'Siber Gözetim'", 119-20.

yaklaşımda işverenin temel hedefi; çalışanlarda sürekli izlendiği ve davranışlarının kontrol altında tutulduğu yönünde bir farkındalık oluşturarak, onları önleyici biçimde disipline etmektir. Böylece, henüz gerçekleşmemiş ancak gerçekleşme ihtimali bulunan ihlal ve riskler, gözetimin caydırıcı etkisiyle önlenmiş olur. Bu kapsamda uygulanan gözetim, işletmenin faaliyet alanına, çalışma biçimine ve mevcut risk seviyesine bağlı olarak yoğunluk ve kapsam açısından farklılık gösterebilmektedir[339].

Tele çalışmada, işverenlerin başvurdukları izleme ve gözetim faaliyetleri genellikle önleyici bir nitelik taşımaktadır. Örneğin, işverenlerin, çalışanların çalışma saatleri içerisinde işle ilgili olmayan web sitelerine erişimini engelleyen ve bu erişim denemelerini raporlayan yazılımlar kullanması, doğrudan bir veri takibi ve gözetleme uygulamasıdır. Özellikle verilerin fiziksel olarak işyeri sınırları dışına taşındığı tele çalışma modelinde veri güvenliği kritik önem taşıdığından, bu gözetim daha da önem kazanmaktadır. Çalışanların kullandıkları bilgisayarlarda veri sızıntılarını engellemek amacıyla belirli dosyalara erişim yetkilerinin sınırlandırılması veya hassas belgelerin kopyalanmasının otomatik olarak engellenmesi de bu tür önleyici faaliyetler arasında yer almaktadır. Bu sistemler, bir engelleme yaparken aynı zamanda kimin, ne zaman, hangi veriye erişmeye çalıştığını da kaydetmektedir. Böylelikle, henüz gerçekleşmemiş ancak gerçekleşmesi durumunda hukuki veya ekonomik zarar doğurabilecek eylemlerin önüne geçilmesi hedeflenmektedir.

3.3.2.3. İşin İşleyişini Takip Etme Amacıyla İzleme ve Gözetleme

İş süreçlerinin etkinliğini, sürekliliğini ve kalitesini sağlamaya odaklanan ve bu yönüyle çalışanların kişisel davranışlarını doğrudan hedef almayan özel bir gözetim türü de "işin işleyişini takip etme amacıyla gözetleme" olarak tanımlanabilir. Bu yaklaşımda temel amaç; işçinin bireysel davranışlarını izlemek veya kişisel performansına dair sürekli bir veri akışı sağlamak değildir. Aksine, işletmenin faaliyet gösterdiği alanda kullanılan makine, araç-gereç ve işin işleyişinin doğru ve kesintisiz biçimde işlemesini güvence altına almaktır. Dolayısıyla, bu tür gözetim faaliyetleri yalnızca çalışanın görev kapsamında makinelerle ya da iş süreçleriyle etkileşimde bulunduğu anlarda devreye girmektedir. Bu nedenle işçiye yönelik gözetim; süre ve

[339] Okur, *İş Hukuku'nda Elektronik Gözetleme*, 26.

kapsam bakımından sınırlı, rastlantısal ve dolaylıdır[340]. Tele çalışma modelinde ise ekran aktivitesini sürekli kaydetmek yerine yalnızca teknik bir sorun çıktığında veya iş süreçlerinin aksadığının tespitinde bilgisayar sisteminin durumunu kontrol etmek ya da fiziksel üretim hattında çalışan makinelerin performansını ölçen sensörlerin yalnızca arıza durumunda çalışanı gözlem altına alması, işin yürütülmesine yönelik gözetimin tipik örnekleri arasında yer almaktadır.

3.3.2.4. Dolaylı İzleme ve Gözetleme

Dolaylı izleme ve gözetleme kavramı (refractive monitorin gand surveillance), çalışanların doğrudan gözlem altında tutulmadığı ancak üçüncü kişiler üzerinden veya dolaylı yöntemlerle takip edilerek kontrol edilmesi olarak ifade etmektedir. Bu gözetim biçiminin temel özelliği; belirli bir gruba yönelik olarak toplanan bilgilerin, doğrudan gözetim altında olmayan başka grupların davranışlarını yönetme, yönlendirme veya değerlendirme amacıyla kullanılabilmesidir. Çok katmanlı ve etkileşimli bir yapı sunan bu yöntem, doğrudan temas kurulamayan gruplar üzerinde dolaylı araçlarla denetim sağlamaya olanak tanımaktadır[341].

Bu tür çok boyutlu gözetim uygulamaları perakende sektöründe sıklıkla kullanılmaktadır. Örneğin, müşterilerin alışveriş tercihleri, ürün değerlendirmeleri veya mağaza içi davranışlarının analiz edilmesi yoluyla elde edilen dolaylı veriler, satış elemanlarının performans değerlendirmesi ve çalışma süreçlerinin denetlenmesi için kullanılabilmektedir[342]. Çalışanların birey olarak değil, öncelikli olarak performans skorlarına indirgenen dijital profiller şeklinde var oldukları platform çalışmalarında, gözetim genellikle müşteri geri bildirimlerine dayalı olarak atanan toplu performans puanları ya da sıralamalar aracılığıyla gerçekleştirilmektedir. Bu sayede müşteriler ve çalışanlar aynı dijital zeminde buluşturulmaktadır[343].

---

[340] Okur, İş Hukuku'nda Elektronik Gözetleme, 26.
[341] Karen Levy ve Solon Barocas, "Privacy at the Margins| Refractive Surveillance: Monitoring Customers to Manage Workers", *International Journal of Communication* 12 (2018): 1166-88.
[342] "People Counting | Occupancy | Retail Analytics | RetailNext", erişim 16 Şubat 2025, https://retailnext.net/.
[343] Manokha, "New Means of Workplace Surveillance", 35.

Benzer bir biçimde, eğitim sektörü de dolaylı gözetim uygulamalarının yaygınlaştığı alanlardan biridir. Öğretmen ve akademisyenlerin performans değerlendirmeleri doğrudan kendilerinin değil, öğrencilerin başarı durumları, davranış biçimleri veya memnuniyet anketleri gibi dolaylı göstergeler üzerinden gerçekleştirilebilmektedir. Böylece, bir paydaş grubu (örneğin müşteriler, hastalar veya öğrenciler) hakkında çeşitli yöntemlerle toplanan veriler, doğrudan ve sürekli bir gözetime tabi tutulmayan başka bir çalışan grubunun (satış elemanları, sağlık personeli, öğretmenler veya akademisyenler gibi) denetiminde, performansının değerlendirilmesinde ve hatta çalışma biçimlerinin yönlendirilmesinde merkezi bir araç hâline gelmektedir. Dolaylı gözetim, farklı paydaş grupları arasında sürekli bir veri akışı ve geri bildirim döngüsü yaratarak, geleneksel hiyerarşik denetimden farklı, çok katmanlı ve etkileşimli yeni nesil kontrol mekanizmalarının oluşmasına zemin hazırlamaktadır[344]. Tele çalışma modelinde ise özellikle müşteri etkileşiminin yoğun olduğu çağrı merkezi çalışanları ve teknik destek uzmanları gibi çalışanlar için müşteri geri bildirimleri, kullanıcı yorumları veya tamamlanan işlere verilen puanlar gibi üçüncü kişi kaynaklı veriler, dolaylı bir performans gözetimi ve değerlendirme aracı olarak sıkça kullanılmaktadır[345].

3.3.2.5. İşçinin Performansını Ölçmeye Yönelik İzleme ve Gözetleme

İşçilerin izleme ve gözetlemeye tabi tutulmasının en önemli nedenlerinden biri performans ölçümdür. İşverenler, ekonomik menfaatlerini korumak, işletme süreçlerinin etkinliğini artırmak ve çalışan performansını en üst düzeye çıkarmak amacıyla işçilerin faaliyetlerini yakından takip etmekte ve bu doğrultuda çeşitli yöntemlere başvurmaktadır. Çalışanların performans ve verimlilik düzeylerinin sistematik biçimde ölçülmesine yönelik izleme ve gözetleme uygulamalarının ilk kuramsal temelleri, 1911 yılında Frederick W. Taylor tarafından geliştirilen bilimsel yönetim ilkelerine dayanmaktadır. Taylorizm olarak bilinen bu yaklaşım, iş süreçlerinin rasyonelleştirilmesini, işçilerin çalışma temposunun sürekli kontrol

[344] Levy ve Barocas, "Privacy at the Margins| Refractive Surveillance", 1166-88; Sánchez-Monedero ve Dencik, "The Datafication of The Workplace", 17-18.
[345] Amjad Alfaleh vd., "Onsite Versus Remote Working: The Impact on Satisfaction, Productivity, and Performance of Medical Call Center Workers", *INQUIRY: The Journal of Health Care Organization, Provision, and Financing* 58 (Ocak 2021): 1-7, https://journals.sagepub.com/doi/10.1177/00469580211056041.

edilmesini ve gözetim altında tutulmasını sağlamıştır. Taylorist düşüncenin temel varsayımı, işverenlerin ekonomik çıkarlarının maksimize edilmesinin ancak çalışanların faaliyetlerinin sürekli ve ayrıntılı biçimde izlenmesiyle mümkün olduğudur[346].

Bu sistematik ölçüm yaklaşımından önce, kapitalizm öncesi dönemlerdeki izleme ve gözetleme uygulamaları, üretim süreçlerinin genel akışını denetlemekle sınırlı kalmıştır. Örneğin, Orta Çağ Avrupa'sında lonca sistemine bağlı işçiler, çalışma hızlarını büyük ölçüde kendi iradeleriyle belirleyebilmekte ve diledikleri zaman mola verebilmekteydi. Bu dönemde, işverenlerin işçilerin bireysel performanslarını sürekli ve sistematik biçimde ölçmesi söz konusu değildi[347]. Bilimsel yönetim ilkelerinin sanayideki yansımaları ise doğrudan ve fiziksel izleme yöntemleriyle kendini göstermiştir. Örneğin, 1910'lu yıllarda Ford fabrikalarında işçilerin çalışma hızlarının kronometrelerle ölçülmesi veya 1979 yılında sağlık çalışanı Patty Jo Toor'un işvereni tarafından çalışma sırasında attığı adımların mezura kullanılarak fiziksel olarak ölçülmesi gibi uygulamalara rastlanmıştır. Hatta Ford'un denetim anlayışı, fabrika duvarlarının dışına taşarak 1914'te kurduğu Sosyolojik Departman ile işçilerin özel hayatlarını da kapsamıştır. Bu departman aracılığıyla, artırılan ücretlerin karşılığı olarak işçilerin tasarruflu ve sağlıklı yaşam standartlarına uyup uymadığı, evlerine gönderilen müfettişler tarafından denetlenmiştir[348].

---

[346] Ajunwa, "Algorithms at Work", 23.
[347] Manokha, "New Means of Workplace Surveillance", 28.
[348] Ajunwa vd., "Limitless Worker Surveillance", 741-42. Ford'un 1914 yılında hayata geçirdiği bir başka yenilik, çalışanları üzerinde daha kapsamlı bir kontrol mekanizması oluşturma amacıyla kurduğu Ford Sosyolojik Departmanı olmuştur. Bu departman, Ford fabrikasındaki işçilerin yaşam tarzlarını denetleyerek davranışlarını düzenlemeye yönelik bir araç işlevi görmüştür. Ford yönetimi, işçilerin zorlu fabrika koşullarından ayrılmalarını önlemek amacıyla bir ücret düzenlemesi getirmiş; 1914 yılında günlük işçi ücretlerini iki katına çıkararak 5 dolara yükseltmiştir. Ancak bu yüksek ücretten faydalanmak, belirli koşullara bağlanmıştır. Bu koşullar arasında işçilerin tasarruflu, temiz ve sağlıklı bir yaşam sürmesi, genç olanların ise evli olması gibi kriterler yer almıştır. Söz konusu kurallara uyumun denetlenmesi amacıyla Ford, işçilerin evlerini ziyaret ederek yaşam tarzlarını gözlemleyen müfettişler görevlendirmiştir. Ayrıca, fabrika ortamında iletişimsizliğin kazalara yol açabileceği gerekçesiyle, işçilerin İngilizce bilmesi de zorunlu kılınmıştır. Bu sistem, işverenin paternalist bir yaklaşımla ("sizin için en iyisini ben bilirim" anlayışıyla) işçilerin hem özel hem de mesleki yaşamlarını katı kurallara bağlamasının tipik bir örneğini teşkil etmiştir. Zamanla eleştirilere maruz kalan bu denetleyici yaklaşımın, maliyetli bulunması sebebiyle terk edildiği anlaşılmaktadır. Ford'un bu "iyi niyetli" kontrol mekanizmasının, zaman içinde yerini daha sert ve gizli denetim yöntemlerine bıraktığı görülmüştür. Ayrıntılı bilgi için bknz. Michael Ballaban, "When Henry Ford's Benevolent Secret Police Ruled His Workers", Jalopnik, 2014, https://jalopnik.com/when-henry-fords-benevolent-secret-police-ruled-his-wo-1549625731.

Günümüzde teknolojik gelişmeler, işçinin performansını ölçmek amacıyla yürütülen gözetim faaliyetlerini çok daha sofistike hâle getirmiş ve bu izleme, iş ilişkisi sınırlarını aşarak özel hayata uzanan bir boyut kazanmıştır[349]. Bu durum özellikle tele çalışma modelinde yaygınlaşan dijital izleme yöntemleriyle daha da belirginleşmektedir. Zira bu model, geleneksel fiziki denetim yöntemlerini işlevsiz kılarken, işin doğası gereği dijital araçlarla yürütülmesi izleme ve gözetlemeyi teknik olarak daha da kolaylaştırmaktadır. Bu kapsamda, tele çalışanların bilgisayar ekranlarından periyodik ekran görüntüsü alınmasından klavye ve fare hareketlerinin anlık takibine, hatta iş süresi boyunca çevrim içi kalma sürelerinin raporlanmasına kadar uzanan çeşitli dijital izleme yöntemleri kullanılmaktadır. Buna ek olarak, bazı sistemlerde tamamlanan görev sayısı, belge düzenleme sıklığı, video konferans katılım yoğunluğu ya da dijital üretkenlik puanları gibi performans metriklerinin otomatik olarak raporlanması da yaygınlaşmaktadır.

3.3.2.6. İşverenin Yükümlülüklerinin Yerine Getirilmesine Yönelik İzleme ve Gözetleme

İşverenin, işçiyi gözetme borcunun en temel yansımalarından biri, bu yükümlülüğün yerine getirilip getirilmediğini denetlemek amacıyla gerçekleştirdiği izleme ve gözetleme faaliyetleridir. Bu çerçevede yürütülen faaliyetler, iş ilişkisi kapsamında ortaya çıkacak risklerin periyodik olarak izlenmesi, gerekli denetimlerin titizlikle yapılması ve tespit edilen olası ihlallerin hızla giderilmesi gibi yöntemlerle öncelikli olarak iş sağlığı ve güvenliği mevzuatına uyum sağlanmayı hedeflemektedir[350]. Nitekim, işverenin çalışanların sağlığını ve güvenliğini koruma yönündeki bu temel sorumluluğu, hem Türk Borçlar Kanunu'nun 417. maddesi ile genel olarak işçiyi gözetme borcu kapsamında, hem de İş Sağlığı ve Güvenliği Kanunu'nun 4. maddesi ile açıkça düzenlenmiştir. Bu düzenlemeler ışığında, işverenin belirtilen koruma ve gözetme yükümlülüğünü etkin bir şekilde yerine getirebilmesi için belirli izleme ve denetim faaliyetlerinde bulunması kaçınılmaz ve hatta zorunlu hâle gelmektedir[351].

---

[349] Sánchez-Monedero ve Dencik, "The Datafication of The Workplace", 15 vd.
[350] Savaş, "İş Hukukunda 'Siber Gözetim'", 101; Dulay Yangın, "Avrupa İnsan Hakları Mahkemesi'nin İşçilerin Elektronik Konum Belirleme Sistemleri (GPS) İle Takip Edilmesine İlişkin 13 Aralık 2022 Tarihli Gramaxo Kararı Üzerine Değerlendirmeler", 875.
[351] Kahraman Akgül, "İşçinin İşyerinde İzlenmesi ve Gözetlenmesinin Hukuki Sonuçları", 87; Savran, "İşçinin İşyerinde Elektronik Yöntemlerle İzlenmesi", 71.

Tele çalışma modelinde, işverenin çalışanların belirli aralıklarla mola verip vermediklerini takip etmesi ya da ergonomik çalışma koşullarına uygunluk açısından çalışma biçimini gözetmesi, iş sağlığı ve güvenliği yükümlülüklerinin yerine getirilmesine yönelik bir denetim biçimi olarak değerlendirilmektedir.

Son olarak işverenler için güvenlik kavramının artık tek bir boyutta ele alınamayacağını belirtmek gerekir. Bu kapsamda siber tehditlere karşı alınan önlemler, fiziksel alanların korunmasıyla birleştiğinde gerçek anlamda bir koruma kalkanı oluşturmaktadır. Örneğin, bir yandan işletme ağına yönelik sızma girişimlerini tespit eden bağlantı kontrol sistemleri devrededir; diğer yandan hassas bölgelere giriş ve çıkışlar kartlı okuyucular veya sensörlerle titizlikle izlenir. Bu tür bütünleşmiş sistemler, hem çalışanların can ve mal güvenliğini sağlama hem de kurumun yasal mevzuat uyumluluğunu denetleme gibi çift yönlü kritik bir amaca hizmet edebilmektedir.

3.4. İşyerinde İzleme ve Gözetleme Uygulamalarına İlişkin Düzenlemeler

3.4.1. Uluslararası Hukukta İzleme ve Gözetlemeye İlişkin Düzenlemeler

İzleme ve gözetlemeye ilişkin uluslararası düzenlemeler, başta Avrupa Birliği ve Uluslararası Çalışma Örgütü olmak üzere çeşitli uluslararası kuruluşların benimsediği normatif çerçevede şekillenmektedir. Bu düzenlemeler, izleme ve gözetleme uygulamalarını temelde bireyin özel hayatının gizliliği hakkı, kişisel verilerin korunması, onurlu ve insan onuruna yaraşır çalışma koşulları gibi temel haklar ekseninde değerlendirmektedir. Aynı zamanda, işverenin yönetim hakkı ile işletme güvenliği, verimlilik ve mülkiyetin korunması gibi meşru menfaatleri arasında adil bir denge kurulması amaçlanmaktadır. Bu denge gözetilirken, izleme ve gözetleme faaliyetlerinin hukuka uygun kabul edilebilmesi; ölçülülük, gereklilik, açık ve önceden bilgilendirme gibi temel ilkeler çerçevesinde gerçekleştirilmesine bağlıdır[352]. Ayrıca, bazı ülkelerde çalışan temsilciliği ve sendikal onay gibi kolektif haklar, gözetim araçlarının kullanımında belirleyici olmaktadır. Özellikle elektronik iletişim

[352] İş hukukunda ölçülülük ilkesine ilişkin ayrıntılı bilgi için bknz. Deniz Ugan Çatalkaya, *İş Hukukunda Ölçülülük İlkesi* (Beta, 2019).

araçlarının izlenmesine ilişkin uygulamalarda, haberleşmenin gizliliğinin korunması, bireylerin temel hak ve özgürlükleri açısından vazgeçilmez bir hukuki güvence alanı teşkil etmektedir. Günümüzde yapay zekâ ve dijital teknolojilerin yükselişiyle birlikte, izleme ve gözetleme uygulamalarına ilişkin yeni hukuki sorunlar, uluslararası belgelerde düzenlenen normatif yaklaşımlar çerçevesinde yeniden değerlendirilmektedir. Bu çerçevede AİHS, GDPR, 108+ sayılı Sözleşme, e-Gizlilik Direktifi, Uluslararası Çalışma Örgütü'nün ilgili uygulama kuralları ve rehberleri, Avrupa Birliği Yapay Zekâ Tüzüğü ve son olarak Birleşmiş Milletler'in konuya ilişkin rehber ilkeleri ayrı başlıklar altında incelenecektir.

3.4.1.1. Avrupa İnsan Hakları Sözleşmesi

Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi, iş ilişkisi kapsamında uygulanan denetim mekanizmalarının hukuki sınırlarını değerlendirmede temel dayanaklardan biri olarak öne çıkmaktadır. Sözleşmenin 8. maddesi, herkesin özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahip olduğunu hüküm altına almakta olup, bu korumanın yalnızca özel hayatla sınırlı olmadığı, iş yaşamını da kapsayabileceği AİHM içtihatlarıyla sabittir. Bu çerçevede çalışanların izlenmesi ve gözetlenmesi, AİHS'nin 8. maddesi kapsamında özel hayata müdahale olarak değerlendirilmekte ve bu müdahale sıkı bir denge denetimine tabi tutulmaktadır[353].

Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi kapsamında özel hayata yönelik bir müdahalenin hukuka uygun sayılabilmesi için üç temel şartın birlikte gerçekleşmesi gerekmektedir. Bu şartlar; müdahalenin kanunla açık ve öngörülebilir bir şekilde düzenlenmiş olması, Sözleşme'de belirtilen meşru amaçlardan birine (örneğin başkalarının hak ve özgürlüklerinin korunması, kamu güvenliği veya suçun önlenmesi gibi) dayanması ve son olarak, söz konusu meşru amaca ulaşmak için demokratik bir toplumda gerekli ve orantılı bir tedbir niteliği taşımasıdır. Bu bağlamda, özellikle iş ve

[353] Bknz. Case of Halford V. the United Kingdom, Application no. 20605/92 (European Court of Human Rights (Grand Chamber) 25 Haziran 1997), https://hudoc.echr.coe.int/tur?i=001-58039; Case of Bărbulescu V. Romania, Application no. 61496/08 (European Court of Human Rights (Grand Chamber) 05 Eylül 2017), https://hudoc.echr.coe.int/fre?i=001-177082; Case of Antović and Mirković v. Montenegro, No. 70838/13 (ECtHR 28 Kasım 2017), https://hudoc.echr.coe.int/fre?i=001-178904; Case of Libert V. France, Application no. 588/13 (European Court of Human Rights (Fifth Section) 02 Temmuz 2018), https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-181273%22]}.

özel hayat sınırlarının giderek daha fazla iç içe geçtiği tele çalışma ilişkilerinde kullanılan dijital izleme uygulamalarının, yalnızca işverenin verimlilik beklentileri temelinde değil; esas olarak insan haklarına saygılı, şeffaf ve hukuk devleti ilkeleriyle uyumlu bir biçimde kurgulanması ve uygulanması büyük önem taşımaktadır.

Avrupa İnsan Hakları Mahkemesi, bu dengeyi değerlendirdiği içtihatlarında, işverenin denetim yetkisinin mutlak olmadığını açıkça ortaya koymuştur. Örneğin, Bărbulescu/Romanya kararında AİHM, çalışanın işletme bilgisayarından özel mesajlar göndermesi nedeniyle işten çıkarılmasını ve bu kapsamda yapılan denetimin çalışan tarafından önceden açık şekilde bilgilendirilmeden gerçekleştirilmesini, Sözleşme'nin 8. maddesi bağlamında ihlal olarak değerlendirmiştir. AİHM, Bărbulescu kararında iş ilişkisi kapsamındaki izleme uygulamalarının hukuka uygun sayılabilmesi için bir dizi kriter belirlemiştir: Öncelikle, çalışana izleme yapılacağına dair önceden açık ve net bilgilendirme yapılması esastır. İkinci olarak, gerçekleştirilen gözetimin kapsamının ve derinliğinin, izleme amacıyla orantılı ve sınırlı olması gerekmektedir. Üçüncüsü, işverenin bu izlemeyi gerçekleştirmek için meşru bir amacının bulunması şarttır. Dördüncüsü, işverenin bu meşru amaca ulaşmak için daha hafif müdahale araçlarının veya yöntemlerinin mevcut olup olmadığının titizlikle değerlendirilmesi zorunludur[354]. Benzer şekilde, López Ribalda/İspanya kararında da AİHM, işverenin çalışanları habersiz kamera ile izlemesinin AİHS 8. maddesi bağlamında bir müdahale teşkil ettiğini kabul etmiş, ancak müdahalenin sınırlı süreli, belirli alanda yapılmış olması ve ciddi bir usulsüzlük şüphesine dayanması gerekçeleriyle ihlal olmadığı sonucuna varmıştır[355].

3.4.1.2. Avrupa Birliği Temel Haklar Şartı

Avrupa Birliği hukuk düzeni içerisinde, çalışanların izleme ve gözetleme uygulamalarına karşı korunmasında temel bir hukuki dayanak da Lizbon Antlaşması

---

[354] *Case of Bărbulescu V. Romania*; Burak Gemalmaz, "Çalışanların İnternet İletişiminin İşverence İzlenmesi Özel Yaşam Hakkına Aykırı Mıdır?: AİHM Büyük Dairenin 05 Eylül 2017 Tarihli Barbulescu Kararı", Lexpera Blog, 09 Eylül 2017, https://blog.lexpera.com.tr:443/calisanlarin-internet-iletisiminin-isverence-izlenmesi-ozel-yasam-hakkina-aykiri-midir-aihm-buyuk-dairenin-05-eylul-2017-tarihli-barbulescu-karari/.

[355] López Ribalda and Others v. Spain, 1874/13, 8567/13 (AİHM 17 Ekim 2019), https://hudoc.echr.coe.int/fre?i=001-197098.

ile AB Anlaşmalarıyla aynı hukuki değere sahip kılınan Avrupa Birliği Temel Haklar Şartı'dır. Şart, AB tarafından yapılan tüm eylemlerin ve çıkarılan tüm ikincil mevzuatın (tüzükler, direktifler vb.) uymak zorunda olduğu birincil hukuk kaynağı niteliğindedir[356]. Bu nedenle, iş ilişkisi kapsamındaki izleme ve gözetleme faaliyetlerinin hukuki sınırlarını belirleyen GDPR gibi düzenlemeler, Şart'ta güvence altına alınan temel haklar süzgecinden geçirilerek yorumlanmak zorundadır.

Şart'ın konumuzla doğrudan ilgili olan en temel hükümleri, 7. ve 8. maddeleridir. Madde 7, "Özel hayata ve aile hayatına saygı hakkı"nı güvence altına alarak, bir önceki bölümde incelenen AİHS'nin 8. maddesine paralel bir koruma sağlamaktadır. Bu madde, özellikle iş ve özel hayat sınırlarının iç içe geçtiği tele çalışma modelinde, çalışanın konutundaki mahremiyet alanının korunmasında kritik bir rol oynamaktadır. Daha da önemlisi, madde 8, "kişisel verilerin korunması hakkı"nı, özel hayatın gizliliğinden bağımsız, müstakil bir temel hak olarak açıkça tanımaktadır. Bu temel hak, kendisinden sonraki bölümde incelenecek olan Genel Veri Koruma Tüzüğü'nün varlık nedenini ve felsefi temelini oluşturmaktadır. Dolayısıyla, tele çalışmada kişisel veri niteliğindeki her türlü izleme verisinin işlenmesi, öncelikle Şart'ın 8. maddesinde tanınan bu temel hakkın bir ihlali potansiyelini taşımakta ve meşruiyeti, ancak sıkı koşullar altında sağlanabilmektedir. Bununla birlikte, Şart'ın madde 1'de düzenlenen "insan onuru" ilkesi, teknolojinin çalışanlar üzerindeki etkilerini değerlendirmede merkezi bir öneme sahiptir. Özellikle yapay zekâ destekli sürekli performans analizi, duygu tanıma sistemleri veya nöroteknoloji gibi müdahaleci nitelikteki teknolojiler, çalışanı sürekli denetim altında tutarak bir "dijital panaptikon" etkisi yaratma ve bireyi nesneleştirme riski taşımaktadır. Bu tür uygulamaların, Şart'ın temel değeri olan insan onuruna aykırı olup olmadığı, her somut izleme yönteminin niteliğine göre ayrıca değerlendirilmelidir. Son olarak, Şart'ın madde 31'de yer alan "adil ve hakça çalışma koşulları" hakkı da işverenin izleme ve gözetleme yetkisinin, çalışanların sağlığını, güvenliğini ve onurunu koruyan bir çerçevede kullanılması gerektiğini ortaya koyan genel bir ilke olarak dikkate alınmalıdır.

[356] Avrupa Birliği Temel Haklar Şartı, AB Resmi Gazetesi, 26.10.2012, C 326, s. 391-407. (erişim 05.05.2025), https://eur-lex.europa.eu/legal-content/TR/TXT/?uri=celex:12012P/TXT.

Netice itibarıyla, Avrupa Birliği Temel Haklar Şartı, tele çalışmada izleme ve gözetleme faaliyetlerinin hukuka uygunluk denetiminde soyut bir referans noktası olmanın ötesinde, GDPR gibi teknik düzenlemelerin ruhunu ve amacını belirleyen bağlayıcı bir üst normdur. İşverenin meşru menfaatleri ile çalışanın temel hakları arasındaki denge kurulurken, Şart'ta yer alan bu güvenceler vazgeçilmez bir ölçüt olarak kabul edilmelidir.

3.4.1.3. Genel Veri Koruma Tüzüğü

Avrupa Birliği'nin 2016 yılında kabul ettiği ve 2018 itibarıyla yürürlüğe giren Genel Veri Koruma Tüzüğü (General Data Protection Regulation), iş ilişkisi kapsamında çalışanlara yönelik izleme ve gözetleme uygulamalarını da kapsayan kapsamlı bir veri koruma rejimi oluşturmaktadır. GDPR, kişisel verilerin işlenmesine ilişkin temel ilkeleri 5. maddesinde detaylı bir şekilde düzenlemektedir. Bu maddeye göre, kişisel veriler; hukuka ve dürüstlük kurallarına uygun ve şeffaf bir şekilde işlenmelidir. Ancak, işverenin çalışanları izleme faaliyetinde özel nitelikli kişisel verilerin işlenmesi söz konusuysa, GDPR'ın 6. ve 9. maddeleri birlikte değerlendirilmelidir. Bu düzenlemelerden madde 6, kişisel verilerin işlenmesinin hukuka uygun olabilmesi için gerekli yasal dayanakları belirlerken, madde 9 ise özel nitelikli verilerin işlenmesini genel olarak yasaklamakta ve belirli istisnai durumlarda bu yasağın kaldırılabileceğini belirtmektedir. Böylece genel nitelikli kişisel veriler ile özel nitelikteki kişisel verilerin işlenmesi ayrı kurallara bağlanmıştır. Hukuka uygunluk nedenlerinin yanı sıra kişisel verilerin işlenmesinde uygulanacak ilkeler de söz konusudur. Bu kapsamda kişisel veriler, belirli, açık ve meşru amaçlar için toplanmalı ve bu amaçlarla bağdaşmayan şekilde işlenmemelidir. Ayrıca, işleme amacı için gerekli olanla sınırlı, ölçülü ve ilgili olmalı ve işleyenin bu ilkelere uyduğunu gösterebilmesi gerekmektedir. Bu bağlamda işverenin çalışanları izleme hakkı, meşru menfaat temelli veri işleme şartına (madde 6/1-f) dayanabilir; ancak bu menfaatin, çalışanın temel hak ve özgürlükleri karşısında ağır basması ve izlemenin orantılı olması gerekmektedir. Özellikle kamera gözetimi, internet ve e-posta takibi, konum izleme gibi uygulamalarda, Tüzük'ün öngördüğü şeffaflık ve bilgilendirme yükümlülükleri (madde 13-14) de titizlikle yerine

getirilmelidir[357]. Aksi takdirde veri işlemenin hukuka aykırı sayılması ve ciddi yaptırımlarla karşılaşılması mümkündür.

GDPR, çalışanların yalnızca veri işleme sürecinden haberdar olmasını değil, bu sürece ilişkin haklarını aktif olarak kullanabilmelerini de güvence altına almaktadır. Özellikle GDPR 21. maddesi uyarınca, veri sahibinin kendisiyle ilgili verilerin işlenmesine, belirli koşullarda itiraz etme hakkı; 22. madde çerçevesinde ise yalnızca otomatik işleme sonucunda alınan kararlara karşı korunma hakkı bulunmaktadır. Bu düzenlemeler, çalışanların yapay zekâ tabanlı teknolojilerle performans takibi veya algoritmik denetim sistemleri gibi gözetim araçlarının kullanımında özel bir önem arz etmektedir.

Genel Veri Koruma Tüzüğü, özellikle yüksek risk barındırma potansiyeli taşıyan gözetim faaliyetleri bakımından işverene 35. madde kapsamında önemli bir yükümlülük getirmektedir: Bu yükümlülük, veri koruma etki değerlendirmesi yapma zorunluluğu (Data Protection Impact Assessment)[358] olarak düzenlenmiştir. Belirtilen yükümlülük uyarınca işveren, planladığı izleme faaliyetine başlamadan önce, söz konusu işlemenin kişisel veriler üzerindeki etkilerini ve çalışanların temel hak ve özgürlükleri açısından doğurabileceği riskleri kapsamlı biçimde değerlendirmeli; bu riskleri en aza indirecek uygun teknik ve idari tedbirleri önceden belirlemelidir[359]. GDPR, bu hükümler aracılığıyla, iş ilişkisi kapsamında yürütülen izleme gözetleme uygulamalarının keyfilikten uzaklaştırılmasını ve yalnızca orantılılık, şeffaflık, hesap

---

[357] Veri Koruma Direktifi'nde ise, Avrupa Birliği içerisinde çalışanların bilgilendirilmesi ve istişare edilmesi hakkına ilişkin asgari şartları belirleyen genel bir çerçeve sunmaktadır. Bu bağlamda, işyerinde izleme ve gözetlemeye ilişkin doğrudan bir düzenleme öngörülmese de dolaylı olarak iş organizasyonunda ve sözleşme ilişkilerinde önemli değişikliklere yol açabilecek kararların çalışan temsilcileriyle zamanında paylaşılmasını ve bu temsilcilerle danışma sürecinin işletilmesini zorunlu kılmaktadır (madde 4/2/-c). Özellikle iş gücünün yapısı, istihdamın gelişimi ve bu alanlarda öngörülen önlemler hakkında bilgi verilmesi ve istişarede bulunulması yükümlülüğü (madde 4/2-b) kapsamında, çalışanların gözetim teknolojilerine tabi tutulmalarına yönelik kararların da bu prosedür dâhilinde ele alınması gerekmektedir. Bu durum, çalışan izleme uygulamalarının yalnızca veri koruma açısından değil aynı zamanda çalışanların örgütlü katılımı ve sosyal diyalog ilkeleri çerçevesinde değerlendirilmesini de gerekli kılmaktadır. Bknz. European Parliament and Council, "Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 Establishing a General Framework for Informing and Consulting Employees in the European Community", Official Journal of the European Communities, 23 Mart 2002, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0014.

[358] Bozkurt Gümrükçüoğlu ve Yakacak, "Yapay Zekânın İşe Alım Süreçlerinde Kullanımı ve Algoritmik Ayrımcılık", 1739.

[359] Bozkurt Gümrükçüoğlu ve Yakacak, "Yapay Zekânın İşe Alım Süreçlerinde Kullanımı ve Algoritmik Ayrımcılık", 1740-42.

verebilirlik ve temel haklarına saygı gibi ilkeler çerçevesinde, hukuken denetlenebilir ve meşru bir zeminde gerçekleştirilmesini hedeflemektedir[360].

3.4.1.4. 108 Sayılı Sözleşme ve Tavsiye Kararları

Çalışma yaşamında elektronik izleme ve gözetleme araçlarının kullanımının artmasıyla birlikte, çalışanlara ilişkin büyük miktarda kişisel veri toplanmakta ve bu veriler çeşitli otomatik sistemlerle analiz edilerek işveren kararlarına temel teşkil etmektedir. Avrupa Konseyi tarafından kabul edilen ve Türkiye'nin de taraf olduğu 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin Sözleşme, kişisel verilerin korunmasına yönelik uluslararası düzeyde bağlayıcı nitelikteki ilk ve en temel belgelerden biridir[361]. Bu Sözleşme, 2018 yılında yapılan bir protokolle güncellenerek "108+ Sözleşmesi" adını almış ve dijital çağın getirdiği yeni tehditlere karşı koruma kapsamı genişletilmiştir. Türkiye, bu revize metni 2022 yılında imzalamış olmasına rağmen onay süreci henüz tamamlanmadığından, Sözleşme'nin getirdiği yeni güvenceler iç hukukta tam olarak yürürlüğe girmemiştir[362].

Revize edilen 108 sayılı Sözleşme, dijital teknolojilerin iş yaşamında gözetim ve kontrol amacıyla kullanımının artması karşısında, kişisel verilerin işlenmesine ilişkin temel hakları güçlendirmeyi hedeflemektedir. Özellikle 9. madde kapsamında düzenlenen otomatik karar alma süreçleri ve profilleme, işverenin çalışanlar hakkında veri temelli değerlendirmeler yaptığı uygulamaları doğrudan ilgilendirmektedir. 9. madde uyarınca, bireyler yalnızca otomatik işlemeye dayalı olarak haklarını veya

---

[360] Türkiye her ne kadar Avrupa Birliği üyesi olmasa da, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun hazırlık sürecinde 95/46/EC sayılı eski Veri Koruma Direktifi temel alınmış, ancak günümüzde kişisel verilerin korunmasına ilişkin değerlendirme ve uygulamalarda büyük ölçüde GDPR normları esas alınmakta ve özellikle yüksek riskli veri işleme faaliyetlerinde AB standartlarıyla uyumlu yorumlar geliştirilmektedir. Ayrıtnılı bilgi için bknz. Mehmet Bedii Kaya ve Furkan Güven Taştan, "Kişisel Veri Koruma Hukuku - Mevzuat, İçtihat, Bibliyografya", *Çevrimiçi Sürüm 3.0*, 2025, 5787-6642.

[361] Yeliz Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", içinde İş Hukukunda Yeni Yaklaşımlar (Beta Yayınları, 2017), 46.

[362] Ayrıca, 108+ metni ile birlikte yürürlüğe giren T(2015)5 sayılı Tavsiye Kararı**,** işyerinde kişisel verilerin korunmasına ilişkin spesifik ilkeler sunmakta; sürekli, sınırsız veya habersiz gözetim uygulamalarının demokratik toplum düzeniyle bağdaşmadığını vurgulamaktadır.

durumlarını önemli ölçüde etkileyen bir karara tabi tutulmama hakkına sahiptir[363]. Bu hüküm, çalışanların yalnızca algoritmik performans puanlamaları sonucu işten çıkarılması veya ödüllendirilmesi gibi kararlarda insan müdahalesinin gerekliliğini ortaya koymakta; otomatik kararların ancak bireye uygun güvenceler sağlanmışsa meşru olabileceğini ifade etmektedir[364]. Bu bağlamda Sözleşme, işverenin dijital gözetim araçlarıyla elde ettiği verileri işleyerek çalışan hakkında tek taraflı ve denetlenemez sonuçlar üretmesini sınırlandırmaktadır

Sözleşme, otomatik veri işlemeye dayalı kararlarla karşı karşıya kalan bireylere önemli usûli güvenceler tanımaktadır. 9. maddenin 2. fıkrası uyarınca, bireyin bu tür bir karara maruz kalması hâlinde, kararın alınmasında kullanılan mantıksal yöntemi öğrenme, karara ilişkin kendi görüşünü ifade etme ve bu karara itiraz etme haklarına sahip olması gerektiği açıkça düzenlenmiştir[365]. Bu güvenceler, özellikle profilleme uygulamalarının iş ilişkileri bağlamındaki yansımaları açısından hayati bir öneme sahiptir. Zira günümüz işverenleri, verimliliği artırma, performansı ölçme ve iş süreçlerini denetleme gibi meşru menfaatler doğrultusunda, çalışanların dijital ayak izlerini sistematik olarak kaydetme ve analiz etme eğilimindedirler. Özellikle uzaktan çalışma modelinde, yapay zekâ sistemleri ve gelişmiş veri analitiği araçları; çalışanların iş yapma biçimleri, dijital araçları kullanma hızları, tepki süreleri ve iletişim kalıpları gibi çok çeşitli veriler üzerinden profiller oluşturmaktadır. Bu profillere dayalı öngörüler, işverenin işe alım, terfi veya iş sözleşmesinin feshi gibi kararlarını doğrudan etkileyebilmektedir. Bu çerçevede 108+ sayılı Sözleşmesi'nin getirdiği şeffaflık ve itiraz hakkı gibi güvenceler, çalışanın yalnızca karar sonucunu değil, aynı zamanda bu sonucun hangi veri setlerine ve mantıksal süreçlere dayandığını öğrenerek sürece müdahale edebilmesini sağlamaktadır[366]. Böylece karar alma

[363] Bu düzenleme, yalnızca 108+ sayılı Sözleşme'ye özgü olmayıp, Avrupa Birliği'nin 95/46/EC sayılı Direktifi ve Uluslararası Çalışma Örgütü tarafından kabul edilen uygulama kodları gibi diğer uluslararası belgelerde de yankı bulmaktadır. Bknz. Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 73 vd.
[364] Council of Europe, Convention 108+ – Convention for the Protection of Individuals with Regard to the Processing of Personal Data, as Amended by the Protocol CETS No. 223, 18 Mayıs 2018, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.
[365] Article 9 Council of Europe, Convention 108+.
[366] Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 66 vd.

süreçlerinin şeffaf, hesap verebilir ve birey haklarına saygılı yürütülmesi için normatif bir zemin oluşturulmaktadır.

Sözleşme'de doğrudan adı geçmese de ele alınan bir diğer önemli kavram "sistematik gözetleme"dir (systematic monitoring). Bu tür uygulamalar, işverenin yönetim hakkı, denetim menfaati ve mülkiyetinin korunması gibi çıkarları ile çalışanın kişilik hakları, özel hayatı ve bilgilerin geleceğini belirleme hakkı arasında hassas bir denge kurulmasını gerektirmektedir. Bu bağlamda 108+ sayılı Sözleşmesi'nin 5. maddesinde tanımlanan veri işlemenin adil, meşru bir amaca yönelik ve orantılı olma yükümlülüğü, işverenin sürekli izleme yöntemleri (örneğin, ekran kayıt sistemleri, GPS izleme, klavye hareket analizleri) kullanması halinde, bu uygulamaların mutlaka amaçla sınırlı ve ölçülü olması gerektiğini ortaya koymaktadır[367]. Çalışanın sürekli izlendiği hissi, psikolojik açıdan baskı ve strese yol açabileceği gibi iş ilişkilerindeki güven duygusunu da zedeleyebilmektedir. Bu nedenle 108+ sayılı Sözleşmesi, yalnızca teknik veri koruma standartları belirlemekle kalmamakta, aynı zamanda çalışanların insan onuru, özel hayatı ve karar süreçlerine katılım haklarını güvence altına alan bütüncül bir koruma anlayışı benimsemektedir.

108+ sayılı Sözleşme'nin Türkiye tarafından imzalanmış olmasına karşın onay sürecinin henüz tamamlanmamış olması önemli bir hukuki belirsizlik alanı yaratmaktadır. Bu durum, Kişisel Verilerin Korunması Kanunu'nun genel nitelikte olması ve çalışma ilişkilerine özgü ayrıntılı düzenlemeler içermemesi nedeniyle daha da derinleşmektedir. Mevcut yasal çerçeve genel koruma ilkeleri sunsa da 108+ sayılı Sözleşme'nin ele aldığı profilleme, algoritmik yönetim ve sistematik dijital gözetim gibi yeni nesil tehditlere karşı spesifik güvencelerden yoksun kalmaktadır. Bu gecikme, işverenlerin teknolojik imkânları yasal denetimden uzak bir şekilde kullanma riskini artırırken, çalışanları dijital çağın hak ihlallerine karşı daha savunmasız bırakmaktadır. Dolayısıyla, Sözleşme'nin getirdiği normların ve bu alanda hazırlanacak özel bir kanunun bir an önce iç hukukun parçası hâline getirilmesi, çalışma yaşamında temel hak ve özgürlüklerin teknolojik gelişmeler karşısında etkin bir şekilde korunabilmesi için büyük önem arz etmektedir[368].

---

[367] Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 63 vd.
[368] Bozkurt Gümrükçüoğlu, 97-98.

3.4.1.5. 2002/58 Sayılı Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Özel Hayatın Korunmasına İlişkin Avrupa Birliği Direktifi

Avrupa Birliği'nde elektronik iletişim sektöründe kişisel verilerin işlenmesine yönelik özel düzenlemeler, 2002/58/EC sayılı Direktif ile belirlenmiştir. Bu Direktif, o dönemde yürürlükte olan 95/46/EC sayılı Genel Veri Koruma Direktifi'nin benimsediği ilkeleri, özellikle haberleşmenin gizliliği, iletişimle ilişkili trafik ve konum verilerinin işlenmesi, çerez kullanımı ve istenmeyen e-posta gibi spesifik konular açısından elektronik iletişim hizmetlerine özgü daha detaylı hükümlerle tamamlamayı amaçlamıştır. Sözü geçen Direktif uyarınca, temel ilke, kullanıcıların iletişim içeriklerinin ve bu iletişimle bağlantılı trafik verilerinin, açık rızaları olmaksızın dinlenmesi, kaydedilmesi, izlenmesi veya herhangi bir şekilde işlenmesinin yasak olmasıdır. Bu tür veri işleme faaliyetlerine yalnızca, iletişimin teknik olarak sağlanması için zorunlu olan hâllerde veya kanunla açıkça düzenlenmiş belirli yasal istisnalar çerçevesinde izin verilmektedir. Ayrıca, çerezlerin ve benzeri teknolojilerin kullanıcı cihazına yerleştirilmesi ancak açık, anlaşılır bilgilendirme ve kullanıcı rızası ile mümkün kılınmıştır. Böylece 2002/58 sayılı Direktif, telekomünikasyon ve internet hizmetleri üzerinden yürütülen iletişimde mahremiyetin korunmasına yönelik sektörel zemin oluşturmakta ve işverenlerin elektronik haberleşme yoluyla gerçekleştirebileceği gözetim faaliyetlerinin hukuki sınırlarının çizilmesine katkıda bulunmaktadır[369].

3.4.1.6. Uluslararası Çalışma Örgütü İşçilerin Kişisel Verilerinin Korunması Hakkında Uygulama Kodu

Uluslararası Çalışma Örgütü tarafından 1996 yılında kabul edilen ve 1997'de yürürlüğe giren Kişisel Verilerinin Korunması Hakkında Uygulama Kodu (Code of Practise on the Protection of Workers' Personel Data), işverenlerin çalışanların kişisel verilerini toplama, işleme ve kullanma süreçlerinde uyması gereken ilkeleri

[369] Directive 2002/58/EC on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) (2002), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058.

belirlemektedir[370]. Bu Kod, bağlayıcı bir uluslararası sözleşme niteliğinde olmayıp, üye devletlere yönelik rehberlik sağlayan bir uygulama kılavuzudur.

Sözü geçen Kod'un 3. maddesinde, izleme; bilgisayar, kamera, ses kayıt cihazı, telefon gibi araçlar yoluyla gerçekleştirilen gözetimin yanı sıra, kimlik ve konum belirleme yöntemlerini de kapsayacak şekilde tanımlanmıştır. Ardından 4. maddesinde, kişisel verilerin korunmasına ilişkin kuralların kamu ve özel sektördeki tüm manuel ve otomatik veri işleme faaliyetlerine uygulanacağını düzenlemektedir. 5. maddesinde ise, izleme faaliyetlerinin yalnızca meşru, orantılı ve şeffaf bir şekilde yürütülebileceği açıkça belirtilmiş; sistem güvenliği amacıyla toplanan verilerin, çalışanların davranışlarını denetleme amacıyla kullanılması yasaklanmıştır. Ayrıca aynı maddede, izleme yoluyla elde edilen kişisel verilerin, işçi hakkında alınacak kararlarda tek başına belirleyici unsur olarak kullanılamayacağı vurgulanmış; işverenlerin veri işleme uygulamalarını düzenli aralıklarla gözden geçirmesi ve yalnızca gerekli verilerin toplanmasını sağlayacak şekilde veri minimizasyonu ilkesine uygun hareket etmesi gerektiği ifade edilmiştir. Ayrıca, çalışanın mahremiyet hakkının devredilemeyeceği açıkça belirtilmiş ve kişisel verilerin işlenmesinde temel hak ve özgürlüklerin korunmasına öncelik verilmiştir[371].

Kodu'un 6. maddesi kapsamında ise, izleme faaliyetlerine başlanmadan önce çalışanların, izlemenin amacı, süresi, kullanılacak yöntemler ve toplanacak veriler hakkında açıkça bilgilendirilmesi zorunluluğu getirilmiştir. Sürekli izleme uygulamaları, yalnızca iş sağlığı ve güvenliğinin sağlanması veya işverenin mülkiyetinin korunması gibi zorunlu hâllerde hukuka uygun kabul edilmekte; gizli izlemeye ise ancak ulusal mevzuatta açıkça öngörülmesi ya da ciddi bir suç veya ağır bir usulsüzlük şüphesinin bulunması durumunda izin verilmektedir. Aynı maddede, özel nitelikteki kişisel verilere yönelik özel koruma mekanizmaları öngörülmüş; cinsel yaşam, siyasi veya dini görüşler ile adli sicil bilgileri yalnızca istisnai hâllerde ve ulusal hukuk açıkça izin verdiği takdirde işlenebileceği hüküm altına alınmıştır. Sendikal faaliyetlere ilişkin veriler yalnızca yasal bir yükümlülüğün veya toplu iş

[370] International Labour Organization, Protection of Workers' Personal Data: An ILO Code of Practice (1997), https://www.ilo.org/resource/other/protection-workers-personal-data.
[371] International Labour Organization, Protection of Workers' Personal Data, 1997 Protection of Workers' Personal Data, 1997.

sözleşmesi hükmünün bulunması hâlinde işlenebilirken; yalan makinesi (poligraf) gibi araçların kullanımı tamamen yasaklanmıştır. Kişilik testlerinin sadece çalışanın açık onayıyla uygulanabileceği, genetik tarama ve uyuşturucu testlerinin ise ancak ilgili düzenlemelere uygun biçimde gerçekleştirilebileceği hükme bağlanmıştır[372].

Her ne kadar 1996 yılında kabul edilmiş olsa da Uluslararası Çalışma Örgütü'nün İşçilerin Kişisel Verilerinin Korunması Hakkında Uygulama Kodu'nda yer alan temel ilkeler, günümüzde tele çalışma kapsamında kullanılan ve özel hayata müdahale potansiyeli yüksek olan yeni nesil dijital izleme teknolojilerinin hukuka uygunluk denetiminde hala önemli bir referans niteliği taşımaktadır. Özellikle şeffaflık, orantılılık ve amaçla sınırlılık gibi ilkeler, bu yeni teknolojilerin çalışan haklarını ihlal etmeden kullanılabilmesi için yol göstericidir.

3.4.1.7. Uluslararası Çalışma Örgütü Çalışan Sağlığının Gözetimine İlişkin Teknik ve Etik İlkeler Rehberi

ILO tarafından 1998 yılında yayımlanan Çalışan Sağlığının Gözetimine İlişkin Teknik ve Etik İlkeler Rehberi başlıklı belgede, iş ilişkileri kapsamında izleme ve gözetleme uygulamaları, çalışan sağlığının korunması bağlamında teknik ve etik ilkeler ışığında kapsamlı şekilde ele alınmıştır. Bu bağlamda, çalışan sağlığı gözetimi iş görme ediminin ifa edildiği ortamın denetimiyle birlikte yürütülmesi gereken ve iş kaynaklı hastalık ve kazaların birincil olarak önlenmesini amaçlayan sistematik bir süreç olarak tanımlanmıştır. Rehberin ikinci bölümünde vurgulandığı üzere, sağlık gözetimi yalnızca bireysel sağlık durumunu izlemekle sınırlı kalmamalı, aynı zamanda toplu sağlık eğilimlerinin saptanmasına, epidemiyolojik araştırmaların desteklenmesine ve çalışma koşullarının iyileştirilmesine katkı sağlamalıdır. Bu uygulamalar yalnızca meşru, gerekli ve bilimsel geçerliliği bulunan amaçlar doğrultusunda gerçekleştirilmeli; veri gizliliği, mahremiyet ve profesyonel bağımsızlık ilkeleri mutlaka gözetilmelidir (madde 2/5, 4/1, 4/5)[373].

---

[372] International Labour Organization, Protection of Workers' Personal Data, 1997 Protection of Workers' Personal Data, 1997.

[373] International Labour Organization, Technical and Ethical Guidelines for Workers' Health Surveillance, Occupational Safety and Health Series No. 72 (Geneva, 1998), https://www.ilo.org/publications/technical-and-ethical-guidelines-workers-health-surveillance Technical and Ethical Guidelines , 1998.

İşyerinde sağlık gözetimi çerçevesinde yapılacak tıbbi muayene ve testler, çalışanın açık rızasına dayanmalı ve yalnızca iş sağlığının korunmasına yönelik olmalıdır (madde 3/16, 3/18). Genetik taramalar gibi doğrudan bedensel temas gerektiren uygulamalar, bilimsel yetersizlik ve hak ihlali riski gerekçesiyle yasaklanmakta ya da sıkı sınırlamalara tabi tutulmaktadır (madde 3/20). İş kazaları ve meslek hastalıklarına ilişkin bildirim sistemleri ile hastalık ve devamsızlık nedenlerinin izlenmesi de olası risklerinin belirlenmesi açısından önem arz etmektedir (madde 3/21–3/26). Bununla birlikte, sağlık profesyonellerinin yalnızca tıbbi yönlerden sorumlu olmaları ve idari kontrol mekanizmalarının dışında kalmaları gerektiği belirtilmiştir. Sağlık verilerinin toplanması ve işlenmesi sürecinde kişisel gizliliğe azami özen gösterilmeli, bu tür veriler yalnızca ilgili tıbbi personelin erişimine açık tutulmalı ve üçüncü taraflarla paylaşım ancak çalışanın aydınlatılmış rızası ile gerçekleştirilmelidir (madde 4/5, 4/8). Nihayetinde bu Rehber, sağlık gözetiminin yalnızca bireyin değil, tüm işyerinin güvenliği ve sağlığı için bir önleme aracı olarak yapılandırılması gerektiğini, izleme uygulamalarının ise ancak etik ve hukuki ilkelere bağlı kalınarak meşrulaşabileceğini ortaya koymaktadır[374].

Uluslararası Çalışma Örgütü'nün bu Rehberi, genel olarak iş sağlığına odaklansa da içerdiği ilkeler tele çalışmada öne çıkan ergonomik risklerin ve psikososyal sorunların (örneğin stres, tükenmişlik) önlenmesi ile takibi amacıyla kullanılan modern izleme teknolojilerinin etik sınırlarını belirlemede önemli bir referans niteliğindedir. Bu kapsamda, duruş bozukluklarını tespit eden yazılımların yanı sıra kalp atış hızı, deri iletkenliği veya solunum gibi biyometrik verileri ölçerek stres seviyesini analiz etmeye çalışan giyilebilir cihazlar da giderek daha fazla kullanılmaktadır. Ancak giyilebilir teknolojiler, doğası gereği, veri minimizasyonu ve amaçla sınırlılık ilkelerine aykırı olarak, işverenin meşru işleme amacını aşan ve sağlık verisi gibi özel nitelikli kişisel verileri de içerebilen bilgilere erişmesine neden olabilmektedir. Bu nedenle Rehber'de ortaya konulan ilkeler, bu tür teknolojilerin kullanımında insan onuruna saygı, veri minimizasyonu ve şeffaflık gibi temel etik ve hukuki ilkelere uygun bir veri işleme çerçevesi oluşturulmasına katkı sağlar niteliktedir.

[374] International Labour Organization, Technical and Ethical Guidelines , 1998 Technical and Ethical Guidelines , 1998.

3.4.1.8. Avrupa Birliği Yapay Zekâ Tüzüğü

Avrupa Birliği'nin Yapay Zekâ Tüzüğü (Artificial Intelligence Act), 13 Mart 2024 tarihinde kabul edilmiş, 12 Temmuz 2024 tarihinde AB Resmî Gazetesi'nde yayımlanmıştır[375]. Bu düzenleme, yapay zekâ sistemlerine ilişkin Avrupa genelinde kapsamlı ve bütüncül bir hukukî çerçeve oluşturmayı hedeflemektedir. Tüzüğün temel amacı, yapay zekâ teknolojilerinin geliştirilmesi ve kullanılmasının temel haklara, güvenliğe ve etik ilkelere uygun biçimde gerçekleştirilmesini sağlamaktır.

Avrupa Birliği Yapay Zekâ Tüzüğü, getirdiği risk esaslı yaklaşım ve kademeli yürürlük takvimi ile alanda temel bir çerçeve oluşturmaktadır. Bu yaklaşım uyarınca Tüzük, yapay zekâ sistemlerini dört ana kategoriye ayırmaktadır: asgari risk, sınırlı risk, yüksek risk ve kabul edilemez risk. Bununla birlikte Tüzük, 2024 yılı ortasında yürürlüğe girmiş olmasına rağmen, hükümlerinin tamamı hemen uygulanmamaktadır. Uygulama takvimi, 24 ila 36 aylık bir geçiş sürecine yayılmıştır. Bu çerçevede, kabul edilemez riskli sistemlere yönelik yasaklar 2025 yılı başı itibarıyla uygulanmaya başlamış, genel amaçlı yapay zekâ yönetişimine ilişkin kurallar ise 2025 yılı ortasında yürürlüğe girmiştir. Tüzüğün en önemli bölümünü oluşturan yüksek riskli sistemlere yönelik yükümlülüklerin büyük bir kısmının 2026 ortasında, belirli ürünlere entegre sistemler için ise 2027 ortasında tam olarak uygulanır hâle gelmesi beklenmektedir. Bu kademeli yaklaşım, üye devletlere yeni yükümlülüklere uyum sağlamaları için bir adaptasyon imkânı sunmaktadır[376].

Avrupa Birliği Yapay Zekâ Tüzüğü, istihdam alanında kullanılan yapay zekâ sistemlerini, bireylerin temel hakları ve sosyoekonomik gelecekleri üzerindeki derin potansiyel etkileri nedeniyle "yüksek riskli" olarak sınıflandırmıştır. Bu sınıflandırma, Tüzüğün Ek III listesi uyarınca, işe alım ve seçme süreçlerinden başlayarak çalışma ilişkisinin tüm evrelerini kapsamaktadır. Bu çerçevede, aday başvurularını tarayarak

---

[375] European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 March 2024 on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 13 Mart 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

[376] European Parliament and Council of the European Union, *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 March 2024 on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, md. 113.

liyakat veya uygunluk temelinde filtreleyen, sıralayan ve değerlendiren yapay zekâ uygulamaları yüksek riskli kabul edilmiştir. Bunun yanı sıra, çalışma ilişkisi devam ederken çalışanların performansını ve davranışlarını izleyen, bu verilere dayanarak terfi, görev dağılımı veya iş sözleşmesinin feshi gibi kritik kararları destekleyen ya da otomatikleştiren algoritmik yönetim sistemleri de aynı kategoride değerlendirilmiştir. Bu düzenlemenin temelinde, yapay zekâ destekli otomasyonun istihdam alanında yaratabileceği ayrımcılık, şeffaflık eksikliği ve keyfilik gibi riskleri en aza indirerek çalışanlar için hukuki bir güvence ve denetim mekanizması oluşturma amacı yatmaktadır.

Yüksek riskli yapay zekâ sistemlerinin istihdamda kullanımı, Tüzük uyarınca işverenlere bir dizi kapsamlı teknik ve organizasyonel yükümlülük getirmektedir. Bu yükümlülüklerin başında, sistemin kullanıma sunulmasından önce Tüzük'te tanımlanan standartlara uygunluğunu teyit eden bir değerlendirme yapma zorunluluğu gelir. İşverenler ayrıca, sistemin yaşam döngüsü boyunca ortaya çıkabilecek riskleri proaktif bir şekilde yönetmekle, kullanılan verilerin doğru ve güncel olmasını sağlamakla ve olası algoritmik ön yargıları tespit edip azaltacak tedbirleri almakla mükelleftir. Bu çerçevede, sistemin yetenekleri, sınırları ve mantığı hakkında şeffaflık sağlanması esastır. En kritik güvencelerden biri ise, özellikle otomatik karar alma süreçlerinde, nihai kararın bir insan tarafından gözden geçirilmesini ve potansiyel hataların düzeltilmesini olanaklı kılan etkin bir insan denetimi mekanizmasının varlığının güvence altına alınmasıdır.

Çalışanların davranışlarını manipüle etme potansiyeli taşıyan veya onları sürekli gözetim altında tutan yapay zekâ sistemleri, bireyin özel hayatı ve insan onuru açısından ciddi riskler barındırmaktadır. Söz konusu riskleri dikkate alarak, sosyal puanlama, manipülatif izleme veya işçinin davranışlarını etkilemeye yönelik yapay zekâ sistemleri gibi kabul edilemez risk kategorisinde yer alan sistemlerin kullanımı, 2 Şubat 2025 tarihinden itibaren yasaklanmıştır. Öte yandan, yüksek riskli sistemlere ilişkin yükümlülüklerin kademeli olarak devreye girmesi planlanmakta olup, bu hükümlerin tümüyle bağlayıcı hâle gelmesi 2 Ağustos 2026 tarihine kadar gerçekleşecektir.

Tüzük yalnızca bir uyum çerçevesi sunmakla kalmamakta, aynı zamanda işverenleri, yapay zekâ teknolojilerinin iş ilişkilerine entegrasyonu sürecinde çalışanlarla iş birliği içinde hareket etmeye teşvik etmektedir. Bu doğrultuda, çalışanların izlenmesine ve gözetlenmesinde kullanılan yapay zekâ sistemlerinin kullanımı hakkında çalışanların önceden bilgilendirilmesi, teknolojik değişimlere uyum sağlanabilmesi için gerekli eğitimlerin verilmesi ve çalışanların bu süreçlere katılımının sağlanması önem arz etmektedir. Bu katılımcı yaklaşım, şeffaflığı artırmakta, güven ortamı oluşturarak teknolojinin iş yaşam kalitesini artırıcı şekilde kullanılmasını sağlamaktadır.

3.4.1.9. Birleşmiş Milletler Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler

Birleşmiş Milletler, kişisel verilerin korunması alanındaki uluslararası çerçevenin oluşturulmasında rol oynamıştır. BM İnsan Hakları Komitesi, kişisel verilerin korunması hakkını özel hayatın gizliliği kapsamında değerlendirmiştir. Bu doğrultuda, 1990 yılında BM Genel Kurulu tarafından Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler (Guidelines For The Regulation Of Computerized Personal Data Files) kabul edilmiştir[377]. Bu ilkeler, konuyla ilgili özel bir düzenleme getirmekte olup, iş ilişkileri kapsamındaki veri işleme pratikleri için de bir referans noktası oluşturmaktadır. Ancak, söz konusu Rehber İlkeler'in hukuken bağlayıcı bir niteliği bulunmamaktadır[378].

Rehberin temelini, veri işlemenin meşru bir zemine oturtulması oluşturur. Hukuka ve Adalete Uygunluk İlkesi, kişisel verilerin yasa dışı veya adil olmayan yöntemlerle toplanmasını ve BM Antlaşması'nın amaçlarına aykırı şekilde kullanılmasını yasaklar. Buna paralel olarak, Amaçla Sınırlılık İlkesi, veri toplama amacının meşru ve spesifik olmasını, elde edilen verilerin bu amaçla ilgili ve yeterli düzeyde tutulmasını gerektirir. Veriler, ilgili kişinin onayı olmadan belirlenen amaçlarla bağdaşmayan şekillerde kullanılamaz ve amacın gerektirdiğinden daha uzun süre saklanamaz.

---

[377] UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files (UN General Assembly, 1990), https://www.refworld.org/policy/legalguidance/unga/1990/en/13761.
[378] Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 44.

Verinin niteliği ve bireyin hakları da ilkelerin merkezindedir. Doğruluk İlkesi, veri sorumlularına, tuttukları kayıtların doğruluğunu, ilgililiğini ve güncelliğini düzenli olarak denetleme yükümlülüğü getirir. Bireylere tanınan Erişim Hakkı ise, herkesin kimliğini ispatlayarak kendisiyle ilgili verilerin işlenip işlenmediğini öğrenmesine, bu bilgilere makûl bir sürede ve masrafsızca ulaşmasına ve hatalı veya yasa dışı kayıtların düzeltilmesini ya da silinmesini talep etmesine olanak tanır.

Rehber, belirli veri türleri ve sistemler için özel koruma mekanizmaları öngörür. Ayrımcılık Yasağı İlkesi, ırk, etnik köken, siyasi görüş, sendika üyeliği ve cinsel hayat gibi keyfi veya yasa dışı ayrımcılığa yol açabilecek özel nitelikli verilerin derlenmesini yasaklar. Veri sistemlerinin bütünlüğünü korumayı amaçlayan Güvenlik İlkesi ise, dosyaların kazara kaybolma gibi doğal tehlikelere ve yetkisiz erişim, sahtekârlık veya kötüye kullanım gibi insan kaynaklı risklere karşı uygun önlemlerle korunmasını zorunlu kılar.

İlkelerin hayata geçirilmesi için kurumsal bir yapı da tarif edilmiştir. Her ülkenin, bu ilkelere uyumu denetlemekle sorumlu, tarafsız ve bağımsız bir denetim otoritesi belirlemesi esastır. Bu otorite, ihlaller durumunda uygulanacak cezai veya diğer yaptırımların belirlenmesinde de rol oynar. Bu evrensel ilkeler, modern veri koruma hukukunun temel taşlarını oluşturarak, sonraki yıllarda hazırlanan daha kapsamlı uluslararası düzenlemelere de zemin hazırlamıştır.

Bu çerçevede rehber ilkeler, iş ilişkisi çerçevesinde kullanılan gözetim araçlarının, yalnızca verimlilik gerekçesiyle değil, bireyin mahremiyet hakkı ve insan onuruna saygı temelinde değerlendirilmesini zorunlu kılmakta; ulusal mevzuatlara yön verici nitelikte evrensel bir standart oluşturmaktadır. Nitekim, bu 1990 tarihli Rehber İlkeler'de ortaya konan temel ilkelerin birçoğu, daha sonra Avrupa Birliği Genel Veri Koruma Tüzüğü ve modernize edilmiş 108+ sayılı Sözleşme gibi daha güncel ve kapsamlı uluslararası belgelerde de yankı bulmuş ve daha da geliştirilmiştir.

3.4.2. Mukayeseli Hukuk Düzenlemeleri

Mukayeseli hukuk analizinde, izleme ve gözetleme uygulamalarına ilişkin normatif düzenlemelerin ülkeden ülkeye farklılık gösterdiği görülmektedir. Bu alanda yeknesak

bir yaklaşımdan söz etmek mümkün değildir. Ancak, Avrupa Birliği üyesi ülkeler özelinde, konuyu düzenleyen ve geniş uygulama alanına sahip uluslararası normlar mevcuttur. Bu normların başında yukarıda açıklanan Avrupa Birliği Temel Haklar Şartı, Avrupa İnsan Hakları Sözleşmesi, Genel Veri Koruma Tüzüğü ve Yapay Zekâ Tüzüğü gelmektedir.

Daha önce ele alınan izleme ve gözetleme araç ve yöntemleri teknik açıdan benzerlik arz etse de bunlara ilişkin yasal çerçeveler ulusal düzeyde önemli farklılıklar barındırmaktadır. Takip eden bölümlerde bu düzenlemeler, tele çalışma uygulamaları odağında mukayeseli olarak incelenecektir. Analizin temel amacı, Avrupa Birliği, Birleşik Krallık ve Amerika Birleşik Devletleri örneklemi üzerinden, çalışanların mahremiyet hakkı ile işveren menfaatleri arasındaki hassas dengeyi karşılaştırmalı bir yöntemle ortaya koymaktır.

3.4.2.1. Avrupa Birliğine Üye Devletler

Örneğin, Almanya'da genel kişilik hakkının anayasal düzeyde korunması ve işyeri temsilciliklerinin (Betriebsrat) teknik izleme araçlarının kurulumunda sahip olduğu ortak karar hakkı ilgi çekicidir. Fransa'da ise İş Kanunu, işverenin müdahalelerinin işin niteliğiyle bağlantılı ve orantılı olmasını, ayrıca Sosyal ve Ekonomik Komite (Comité Social et Économique - CSE) nezdinde çalışanların önceden bilgilendirilip danışılmasını öngörmektedir. Diğer Avrupa Birliği üye devletleri de özellikle COVID-19 sonrası uzaktan çalışma uygulamalarının yaygınlaşmasıyla, video gözetimi, konum takibi ve algoritmik yönetim gibi konularda çalışan mahremiyetini korumaya yönelik özel düzenlemeler getirmiş veya mevcut mevzuatlarını güncellemiştir[379]. Bu bölümde Avrupa Birliği üyesi devletlerin düzenlemeleri ele alınacaktır.

[379] Nitekim Avusturya, Finlandiya ve Hollanda gibi bazı Avrupa ülkelerinde, işyerinde izleme ve gözetleme teknolojilerinin uygulanmasından önce, çalışan temsilcilerinin (örneğin işyeri konseyleri veya sendikaların) süreç hakkında bilgilendirilmesi ve kimi durumlarda açık onaylarının ya da görüşlerinin alınması zorunluluğu getirilmiştir. Sara Riso ve Chiara Litardi, "Employee Monitoring: A Moving Target for Regulation", Eurofound, 15 Temmuz 2024, https://www.eurofound.europa.eu/en/resources/article/2024/employee-monitoring-moving-target-regulation.

3.4.2.1.1. Almanya

Alman Hukuku'nda işverenlerin çalışanları izleme ve gözetleme kapsamında değerlendirilebilecek faaliyetleri, çeşitli açılardan sınırlamalara tabi tutulmuştur. Bu bakımdan özellikle kişilik hakkının korunmasına ilişkin düzenlemeler, veri koruma hukukuna ilişkin normlar ile işçi temsilciliklerinin katılım hakkı önem taşımaktadır. Alman Hukuk sisteminde sistematik ve sürekli gözetleme uygulamaları kişilik hakkına bir müdahale olarak değerlendirilmektedir. Federal Anayasa Mahkemesi (Bundesverfassungsgericht-BVerfG) de bu hakkın, Federal Alman Anayasası'nın (Grundgesetz für die Bundesrepublik Deutschland- GG) 1. maddesinin 1. fıkrası (insan onuru) ile 2. maddesinin 1. fıkrası (kişiliğin serbestçe geliştirilmesi hakkı) temelinde şekillendiğini ve anayasal güvencelerle somutlaştırdığını kabul etmektedir[380]. Teknolojinin hızla ilerlemesiyle birlikte, BVerfG, modern bilgi ve iletişim teknolojilerinin (BİT) ve yapay zekânın yarattığı yeni tehditler karşısında, genel kişilik hakkının koruma alanını bu gelişmeleri de kapsayacak şekilde genişletme eğilimindedir. Bu doğrultuda, kişilik hakkının yeni dijital tehditler karşısında daha etkin korunabilmesi amacıyla, özellikle bilgi teknolojisi sistemlerinin gizliliği ve bütünlüğüne odaklanan tamamlayıcı bir yaklaşım geliştirilmiştir. Genişletilmiş ve tamamlayıcı koruma mekanizmaları; bilgisayar, diğer elektronik cihazlar, telefon görüşmeleri ve e-posta gibi modern iletişim araçlarını da kapsamına almaktadır[381].

Alman Hukuku'nda, yukarıda Avrupa Birliği düzenlemelerine yer verirken açıkladığımız Avrupa Birliği Genel Veri Koruma Tüzüğü'nün yanı sıra uygulama alanı bulan Alman Federal Veri Koruma Kanunu (*Bundesdatenschutzgesetz* – BDSG)[382] ile kişisel verilerin korunması hukuku düzenlenmiştir. Belirtmek gerekir ki, GDPR, AB düzeyinde doğrudan uygulanabilir bir tüzüktür. Bu nedenle de veri koruma alanında diğer AB üyesi ülkelerde olduğu gibi Almanya'da da birincil düzenleyici

[380] Aloisi ve Gramano, "Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context", 119.
[381] Aloisi ve Gramano, "Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context", 119.
[382] 2018 yılında BDSG, GDPR'a uyum sağlanması amacıyla önemli ölçüde değiştirilmiştir. BDSG, GDPR'da yer verilen ulusal düzenlemelere yer verme (*opening clauses*) hükümleri çerçevesinde uygulanmaktadır. Alman Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz - BDSG), § 26, Federal Adalet Bakanlığı tarafından "Gesetze im Internet" portalı üzerinden yayımlanmıştır, erişim 30 Mayıs 2025, https://www.gesetze-im-internet.de/bdsg_2018/__26.html.

çerçeveyi teşkil etmektedir. BDSG ise ulusal düzeyde GDPR'ın tamamlayıcı ve açıklayıcı hükümlerini içeren ikincil bir norm niteliğindedir.

İnceleme konumuza ilişkin düzenlemeler getiren BDSG hükümleri de söz konusudur. Zira çalışanların kişisel verilerinin işlenmesi bakımından, GDPR'ın 88. maddesinde ulusal düzenlemeler getirilmesine imkân tanınmış olup, § 26 BDSG ile özel düzenleme getirilmiştir. 26. madde, istihdam ilişkileri için özel bir düzenleme niteliği taşıyarak, veri işleme faaliyetlerinin hukuki zeminini ve sınırlarını net bir şekilde belirlemektedir. Maddenin temel ilkesi, kişisel verilerin ancak işe alım süreçlerinde karar vermek, mevcut bir iş sözleşmesini ifa etmek veya sona erdirmek ya da kanun veya toplu sözleşmelerden doğan çalışan temsilciliği hak ve yükümlülüklerini yerine getirmek amacıyla "gerekli" olması hâlinde işlenebileceğidir. Bu genel kural, veri işlemenin keyfiliğini önleyerek, yalnızca iş ilişkisinin doğal gerekliliklerileyle sınırlı bir çerçeve çizer. Bununla birlikte, maddenin en dikkat çekici yönlerinden biri, iş ilişkisi çerçevesinde suç tespiti amacıyla kişisel verilerin işlenmesine getirdiği katı sınırlamalardır. Bu tür bir işleme, ancak çalışanın iş ilişkisi sırasında bir suç işlediğine dair somut ve belgelenmiş bir gerekçenin varlığı, işlemenin suçun soruşturulması için zorunlu olması, işçinin menfaatlerinin işverenin menfaatlerine göre ağır basmaması ve son olarak müdahalenin türü ve kapsamının şüphenin nedeni ile orantılı olması gibi kümülatif şartlar altında mümkündür[383].

İş ilişkisindeki yapısal güç dengesizliğini tanıyan Alman kanun koyucu, "açık rıza" mekanizmasının geçerliliğini de özel koşullara bağlamıştır. Buna göre, rızanın özgür iradeye dayanıp dayanmadığı değerlendirilirken, çalışanın işverene olan bağımlılığı ve rızanın verildiği özel koşullar dikkate alınır. Rızanın, özellikle çalışana hukuki veya ekonomik bir avantaj sağlaması ya da işveren ile çalışanın ortak menfaatleri doğrultusunda hareket etmesi gibi durumlarda özgürce verildiği kabul edilmektedir. İşveren, bu süreçte çalışanı veri işleme amacı ve rızayı geri çekme hakkı konusunda

[383] Alman Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz - BDSG), § 26, Federal Adalet Bakanlığı tarafından "Gesetze im Internet" portalı üzerinden yayımlanmıştır, erişim 30 Mayıs 2025, https://www.gesetze-im-internet.de/bdsg_2018/__26.html.

metin formatında bilgilendirmekle yükümlüdür, bu da aydınlatma yükümlülüğünün önemini pekiştirmektedir[384].

Özel nitelikli kişisel verilerin işlenmesi ise daha da sıkı kurallara tabidir. Bu tür veriler, ancak iş hukuku, sosyal güvenlik ve sosyal koruma hukukundan doğan hakların kullanılması veya hukuki yükümlülüklerin yerine getirilmesi için zorunluysa ve çalışanın ağır basan meşru bir menfaatinin bulunmadığına inanmak için bir neden yoksa işlenebilmektedir. Bu veriler için alınacak rızanın ise açıkça özel nitelikli verilere yönelik olması gerekmektedir. Veri işleme için bir diğer meşru zemin ise toplu iş sözleşmeleridir. Kanun, bu sözleşmeler aracılığıyla hem genel hem de özel nitelikli kişisel verilerin işlenmesine olanak tanımaktadır[385].

Maddenin koruma kapsamı da oldukça geniştir. Bu hükümler, verilerin bir veri kayıt sisteminde bulunup bulunmamasından bağımsız olarak uygulanmaktadır. Ayrıca, işverenin temel veri koruma ilkelerine uyum sağlama yükümlülüğü ile işyeri temsilciliklerinin (Betriebsrat) katılım haklarının saklı tutulması, denetim ve denge mekanizmalarını güçlendirmektedir. 26. maddenin 8. fıkrası, "çalışan" tanımını oldukça geniş tutarak mevcut çalışanların yanı sıra; mesleki eğitim alanları, stajyerleri, gönüllüleri, ekonomik olarak bağımlı kişileri, iş başvurusunda bulunan adayları ve iş ilişkisi sona ermiş kişileri de bu hukuki korumanın içine dâhil etmektedir[386].

Almanya'da işverenin çalışanlarını teknik araçlarla izlemesi, temel olarak İşyeri Teşkilat Yasası'nın (Betriebsverfassungsgesetz – BetrVG) 87. maddesi ile düzenlenmektedir[387]. Maddenin 1. fıkrasının 6. bendine göre, çalışanların davranış veya performanslarını izlemeye elverişli teknik donanımların işyerine kurulması ve kullanılması, öncelikle yasal bir düzenleme veya toplu iş sözleşmesi ile hüküm altına

---

[384] Alman Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz - BDSG), § 26, Federal Adalet Bakanlığı tarafından "Gesetze im Internet" portalı üzerinden yayımlanmıştır, erişim 30 Mayıs 2025, https://www.gesetze-im-internet.de/bdsg_2018/__26.html.
[385] Alman Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz - BDSG), § 26, Federal Adalet Bakanlığı tarafından "Gesetze im Internet" portalı üzerinden yayımlanmıştır, erişim 30 Mayıs 2025, https://www.gesetze-im-internet.de/bdsg_2018/__26.html.
[386] Alman Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz - BDSG), § 26, Federal Adalet Bakanlığı tarafından "Gesetze im Internet" portalı üzerinden yayımlanmıştır, erişim 30 Mayıs 2025, https://www.gesetze-im-internet.de/bdsg_2018/__26.html.
[387] Almanya İşyeri Teşkilat Yasası (Betriebsverfassungsgesetz - BetrVG), § 87, Abs. 1, Nr. 6, Federal Adalet Bakanlığı tarafından "Gesetze im Internet" portalı üzerinden yayımlanmıştır, erişim 30 Haziran 2025, https://www.gesetze-im-internet.de/betrvg/__87.html.

alınmamışsa, işyeri çalışan temsilciliğinin (Betriebsrat) ortak karar hakkına tabidir. Federal İş Mahkemesi'nin kararı uyarınca bir yazılımın bu kapsama girmesi için özel olarak izleme amacıyla tasarlanmış olması gerekmez; çalışanların davranış veya performansına ilişkin veri toplamaya ve işlemeye elverişli olması yeterlidir. Bu bağlamda, Microsoft Teams veya Outlook gibi standart ofis yazılımları dahi, içerdikleri izleme potansiyeli taşıyan fonksiyonlar (örneğin aktivite durumu, giriş-çıkış saatleri) nedeniyle bu madde kapsamında değerlendirilmekte ve kurulumları temsilciliğin onayını gerektirmektedir. Konumuz açısından bu durum, işverenin tele çalışanların bilgisayarlarına uzaktan izleme yazılımı yüklemesinin veya video konferans sistemleri üzerinden sürekli bir gözetim yapmasının, kural olarak işçi temsilciliğinin katılımını zorunlu kıldığı anlamına gelmektedir. Bununla birlikte, yalnızca sistem güvenliğini sağlamaya yönelik veya mevcut izleme kapasitesini değiştirmeyen yazılım güncellemeleri yeni bir ortak karar süreci gerektirmezken, izleme fonksiyonlarını güçlendiren her türlü güncelleme veya eklenti, yeni bir teknik cihazın devreye alınması olarak kabul edilir ve tekrar temsilcilik katılımını zorunlu kılmaktadır[388].

İşverenin denetim yetkisinin sınırları ve hukuka aykırılığının sonuçları, Federal İş Mahkemesi'nin (Bundesarbeitsgericht - BAG) 27 Temmuz 2017 tarihli Keylogger Kararı (2 AZR 681/16) ile somutlaşmıştır. Mahkeme bu kararında, çalışanın bilgisayarına gizlice keylogger yazılımı yüklenmesinin, ancak bir suç işlendiğine veya ağır bir görev ihlali yapıldığına dair somut, olgusal temellere dayanan bir şüphe varlığında ve daha hafif yöntemlerin tüketilmiş olması koşuluyla meşru olabileceğine hükmetmiştir. Sadece genel bir kuşkuyla ve rastgele yapılan gizli gözetim ise çalışanın anayasal güvence altındaki bilgiye dayalı kendi kaderini tayin ve kişilik haklarını ihlal eden, ölçüsüz bir müdahaledir. En önemlisi, mahkeme bu tür hukuka aykırı yöntemlerle elde edilen verilerin, bir fesih davasında delil olarak kullanılamayacağını kesin bir dille ifade etmiştir. Bu çerçevede, işverenin yazılım yoluyla elde ettiği verileri çalışan performansının izlenmesinde kullanabilmesi, ancak meşru bir menfaatin

[388] Klaus Thönißen, "Perennial Issue: Software Vs. Co-Determination (Section 87 (1) No. 6 BetrVG) - On the Trials and Tribulations of the German Federal Labour Court", Blog, LUTHER, 26 Mayıs 2021, https://www.luther-lawfirm.com/en/newsroom/blog/detail/dauerbrenner-software-vs-mitbestimmung-87-abs-1-nr-6-betrvg.

varlığı, ölçülülük ilkesine riayet ve işçi temsilciliğinin katılımı ile mümkündür[389]. Son olarak, İşyeri Teşkilat Yasası'nın 87. maddesi uyarınca, bu tür teknik izleme konularında işveren ile işyeri çalışan temsilciliği arasında bir anlaşmaya varılamaması durumunda, nihai kararı uzlaştırma kurulu (Einigungsstelle) vermektedir[390].

Sonuç olarak, BDSG 26. madde ve BetrVG 87. madde çalışan verilerinin korunması alanında detaylı, öngörülebilir ve bütüncül bir hukuki rejim oluşturmaktadır. Türkiye'deki mevzuatın daha genel nitelikte olduğu düşünüldüğünde, bu madde, özellikle rızanın geçerliliği, meşru menfaat dengesi ve müdahalelerin orantılılığı gibi konularda, mukayeseli hukuk açısından değerli bir model sunmaktadır.

3.4.2.1.2. Fransa

Fransız hukukunda çalışanların izlenmesi ve gözetlenmesi, hem temel hak ve özgürlüklerin korunması hem de işverenin yönetim ve denetim yetkilerinin sınırlandırılması bakımından kapsamlı bir şekilde ele alınmıştır. Bu bağlamda ilk olarak Fransız İş Kanunu'nun (Code du travail) L.1121-1 maddesi[391], işverenin çalışanların temel hak ve özgürlüklerine müdahalesini yalnızca işin niteliğiyle doğrudan bağlantılı ve ulaşılmak istenen meşru amaçla orantılı olması koşuluyla mümkün kılmaktadır[392]. Bu düzenleme, işverenin izleme araçlarını keyfi biçimde

---

[389] LTO, "BAG zu Kündigungsprozess: Keylogger-Daten unverwertbar", Legal Tribune Online, erişim 12 Nisan 2025, https://www.lto.de/recht/hintergruende/h/bag-urteil-2azr68116-arbeitgeber-ueberwachung-dienst-pc-keylogger-beweise-unverwertbar.

[390] Almanya İşyeri Teşkilat Yasası (Betriebsverfassungsgesetz - BetrVG), § 87, Abs. 2, Federal Adalet Bakanlığı tarafından "Gesetze im Internet" portalı üzerinden yayımlanmıştır, erişim 30 Haziran 2025, https://www.gesetze-im-internet.de/betrvg/__87.html.

[391] Code du travail - Article L1121-1 https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006900839 erişim 22.05.2025.

[392] Bu yasal çerçeve, Avrupa İnsan Hakları Mahkemesi'nin Libert v. Fransa kararında da değerlendirme konusu olmuştur. Söz konusu davada, Fransız Ulusal Demiryolu Şirketi (Société Nationale des Chemins de fer - SNCF) çalışanı Eric Libert'in iş bilgisayarında, "rire" (gülme) adı verilen bir klasör içerisinde pornografik içerikler ve sahte belgeler bulunduğu gerekçesiyle iş sözleşmesi feshedilmiştir. Başvurucu, bu klasörde yer alan dosyaların kişisel nitelikte olduğunu iddia etmiş; ancak klasörü açıkça "özel" (privé) olarak etiketlemediği ve şirketin bu konudaki iç düzenlemelerine aykırı davrandığı gerekçesiyle başvurusu reddedilmiştir. AİHM, işverenin söz konusu denetimini meşru, gerekli ve orantılı bularak, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinin ihlal edilmediğine karar vermiştir. *Case of Libert V. France*.

kullanmasının önüne geçmeyi ve "ölçülülük" (proportionnalité) ilkesini korumayı amaçlamaktadır[393].

İzleme ve gözetleme sistemlerinin kurulabilmesi için birkaç temel koşul bulunmaktadır. Öncelikle sistemin meşru bir amaca hizmet etmesi (örneğin, ağ güvenliğini sağlamak veya kurumsal kaynakları korumak) şarttır. İkinci olarak, çalışanların Sosyal ve Ekonomik Komite'nin (Comité Social et Économique)[394]

---

[393] Savaş, "İş Hukukunda 'Siber Gözetim'", 110; Ugan Çatalkaya, *İş Hukukunda Ölçülülük İlkesi*, 255 vd.; Aloisi ve Gramano, "Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context", 109-11.

[394] Fransız İş Hukuku'nda yer alan Sosyal ve Ekonomik Komite (Comité Social et Économique – CSE), işyerindeki tüm çalışanların temsilini üstlenen temel bir kurumsal mekanizmadır. Bu komite, işveren ve bir personel delegasyonundan oluşmaktadır. Personel delegasyonu, eşit sayıda asil ve yedek üyeden meydana gelmekte; yedek üye, asil üyenin yokluğunda toplantılara katılmaktadır. CSE, doğrudan bir sendikal yapı olmasa da sendikal yapılanmalarla yakın ilişki içinde faaliyet göstermektedir. Örneğin, 300'den az çalışanı olan şirketlerde bir işyeri temsilcisi otomatik olarak CSE'de sendika temsilcisi sayılırken, 300'den fazla çalışanı olan şirketlerde her temsili sendika organizasyonu CSE'ye bir temsilci atayabilmektedir. Ayrıca, iş sağlığı ve güvenliği ile ilgili toplantılara işyeri hekimi ve iç güvenlik departmanı başkanı da katılmaktadır. İşveren, her 4 yılda bir CSE üyelerinin seçimini düzenlemekle yükümlüdür. Ancak bir toplu sözleşme ile bu süre 2 ile 4 yıl arasında farklı bir zaman dilimi olarak belirlenebilmektedir. Komite kurma zorunluluğu, bir işyerinde arka arkaya 12 ay boyunca en az 11 çalışan istihdam edilmesiyle başlamaktadır. Eğer şirket çalışan sayısı üst üste 12 ay boyunca 11'in altına düşerse, mevcut komitenin görev süresi sonunda komite yenilenmemektedir. CSE'nin temel yetkileri, 11'den fazla çalışanı olan şirketlerde başlamaktadır. Bu ölçekteki şirketlerde komite, çalışanların bireysel ve kolektif taleplerini işverene sunmakla görevlidir. Bu görevler; ücretler, İş Kanunu'nun uygulanması ve sosyal koruma ile ilgili yasal hükümler hakkındaki talepleri iletmeyi içermektedir. Komite aynı zamanda şirkette sağlık, güvenlik ve çalışma koşullarının geliştirilmesine katkıda bulunmakta, iş kazaları veya meslek hastalıklarıyla ilgili soruşturmalar yapmakta ve yasal hükümlerin uygulanmasıyla ilgili tüm şikayet ve gözlemleri İş Müfettişliği'ne (Inspection du travail) bildirme hakkına sahiptir. Çalışan sayısı 50'yi aştığında, CSE'nin yetkileri önemli ölçüde genişlemekte ve stratejik bir nitelik kazanmaktadır. Komite, şirketin genel işleyişini ilgilendiren konularda düzenli olarak bilgilendirilmekte ve kendisine danışılmaktadır. Bu konular arasında şirketin stratejik yönelimleri, ekonomik ve mali durumu, sosyal politikası, iş gücünün yapısını veya büyüklüğünü etkileyebilecek önlemler, şirketin ekonomik veya hukuki organizasyonundaki değişiklikler, yeni teknolojilerin uygulamaya konulması ve çalışanların faaliyetlerini denetlemek için kullanılan yöntemlerin uygulanması yer almaktadır. Genişletilmiş yetkiler kapsamında, CSE üyeleri çeşitli durumlarda işverenden açıklama talep etmelerini sağlayan bir uyarı hakkına (droit d'alerte) sahiptir. Bu hak; bireylerin haklarının (örneğin psikolojik taciz), fiziksel ve zihinsel sağlıklarının veya bireysel özgürlüklerinin ihlali, halk sağlığı ve çevre için ciddi ve yakın bir tehlike oluşması ve şirketin ekonomik durumunu endişe verici şekilde etkileyebilecek olguların öğrenilmesi gibi durumlarda kullanılabilmektedir. Şirket büyüdükçe, CSE bünyesinde özel komisyonlar kurulması zorunlu hale gelmektedir. 300 ve üzeri çalışanı olan şirketlerde Sağlık, Güvenlik ve Çalışma Koşulları Komisyonu, Eğitim Komisyonu, Konut Bilgilendirme ve Yardım Komisyonu ve Fırsat Eşitliği Komisyonu gibi yapılar kurulmaktadır. 1.000 ve üzeri çalışanı olan şirketlerde ise bu komisyonlara ek olarak, şirketin ekonomik ve mali belgelerini incelemekle görevli bir Ekonomik Komisyon da kurulmaktadır. CSE üyelerinin görevlerini etkin bir şekilde yerine getirebilmeleri için çeşitli kaynaklar sağlanmaktadır. Asil üyeler, görevlerini yerine getirmek için ücret kaybı olmaksızın kullanabilecekleri delegasyon saatlerine sahiptirler; bu süre ayda en az 18 saattir. Komite toplantılarında geçirilen süre bu saatlerden düşülmemekte ve çalışma süresi olarak ücretlendirilmektedir. Ayrıca üyeler, görevleriyle bağlantılı olası işveren misillemelerine karşı kendilerini koruyan özel bir işten çıkarılmaya karşı korumadan yararlanmaktadırlar. Bu yapı, işyerindeki kararların yalnızca işveren iradesine bırakılmayıp, çalışan temsilcilerinin katılımıyla şekillenmesini güvence altına almaktadır. Ayrıntılar için bknz. "Social and

usûlüne uygun şekilde bilgilendirilmesi ve danışma sürecine dâhil edilmesi zorunludur. Son olarak, kurulan sistemin ölçülülük ilkesine uygun olması gerekmektedir. Ayrıca, sistemin işleyişi sırasında ortaya çıkan olağan dışı bir durum ya da somut bir şüphe, işverenin belirli bir çalışanı daha yakından incelemesi, soruşturma başlatması ya da disiplin süreci işletmesi gibi müdahaleler açısından belirleyici bir unsur teşkil etmektedir[395]. Bu tür adımların hukuka uygunluğu, başvurulan önlemin gerekçesi, müdahalenin kapsam ve niteliğiyle orantılı olmasına bağlıdır[396]. Anayasal ve yasal güvenceler, yalnızca meşruluk ve ölçülülük ilkeleriyle sınırlı olmayıp, aynı zamanda şeffaflık yükümlülüğünü de içermektedir. Örneğin, işverenin çalışana sürekli kamera takibi veya çalışma saatleri dışında GPS ile konum izleme gibi araçlarla müdahalesi özel hayatın gizliliğinin ihlali olarak değerlendirilmektedir[397].

Economic Committee (ESC)", erişim 30 Haziran 2025, https://entreprendre.service-public.fr/vosdroits/F34474/personnalisation/resultat?lang=en.

[395] Çalışanların işveren tarafından izlenmesine ilişkin uyuşmazlıklarda, çoğu zaman esas mesele, kullanılan gözetim aracının meşruiyeti ile bu araç vasıtasıyla elde edilen delillerin hukuka uygunluğudur. Fransız Yargıtayı Sosyal Dairesi (Cour de cassation, Chambre sociale), 23 Haziran 2021 tarihli kararında, video gözetim yoluyla gerçekleştirilen denetimin sınırları ve hukuki geçerliliğine dair dikkat çekici bir örnek sunmuştur. Somut olayda, bir pizzacıda aşçı olarak çalışan işçi, işverenin ciddi bir disiplin ihlali iddiasıyla iş sözleşmesini feshetmesi üzerine, bu feshin haksız olduğu gerekçesiyle endüstri mahkemesine başvurmuştur. İşverenin fesih gerekçesi, mutfakta kurulu güvenlik kamerasından elde edilen kayıtlara dayanmaktadır. Paris Temyiz Mahkemesi (Cour d'appel de Paris), işçinin başvurusunu kabul etmiş ve işvereni; ihbar süresi ücreti, buna bağlı izin alacakları, kıdem tazminatı, geçmişe dönük ücretler ve haksız fesih nedeniyle tazminat ödemeye mahkûm etmiştir. Temyiz Mahkemesi, işçinin yalnız başına çalıştığı bir alana kamera yerleştirilmesini özel hayatın ihlali olarak değerlendirmiş ve bu yolla elde edilen görüntülerin delil niteliği taşımayacağına hükmetmiştir. İşveren, gözetim sisteminin kurulmasını işin niteliği ve işyerindeki kişi ile mal güvenliğini sağlama amacıyla gerekçelendirmiş ve kararı Yargıtay'a taşımıştır. Ancak Fransız Yargıtayı Sosyal Dairesi, 23 Haziran 2021 tarihli kararında temyiz talebini reddederek alt derece mahkemesinin kararını onamıştır. Sosyal Daire, Fransız İş Kanunu'nun L.1121-1 maddesine atıfla, çalışanların hak ve özgürlüklerine getirilecek kısıtlamaların yalnızca görevin niteliğiyle haklılaştırılması ve ulaşılmak istenen amaçla orantılı olması gerektiğini vurgulamıştır. Somut olayda, işçinin mutfakta tek başına çalıştığı ve sürekli gözetim altında tutulduğu dikkate alındığında, video gözetiminin çalışanın özel hayatına ölçüsüz bir müdahale oluşturduğu ve işverenin öne sürdüğü güvenlik amacıyla bağdaşmadığı kanaatine varılmıştır. Bu nedenle, söz konusu görüntüler hukuken geçerli bir delil olarak kabul edilmemiştir. Cour de Cassation, Civile, Chambre Sociale, 23 juin 2021, 19-13.856, erişim 22 Mayıs 2025, https://www.legifrance.gouv.fr/juri/id/JURITEXT000043711120; "France: Video Surveillance Cannot Permanently Monitor the Activity of an Employee Working Alone", *L&E Global*, 29 Temmuz 2021, https://leglobal.law/2021/07/29/france-video-surveillance-cannot-permanently-monitor-the-activity-of-an-employee-working-alone/.

[396] Nancy E Muenchinger, "Workplace Privacy - France: Electronic Workplace Privacy in France", Computer Law & Security Report 18, sy 6 (2002): 421.

[397] Joelle Hannelais ve Sarah Machrhoul Lhotellier, "Protection Of Privacy At Work In France", Mondaq, 20 Eylül 2021, https://www.mondaq.com/france/employee-rights-labour-relations/1112712/protection-of-privacy-at-work-in-france; Stéphanie Dumas, "Social Media & Data Privacy in France", L&E Global, 22 Ekim 2024, https://leglobal.law/countries/france/employment-law/employment-law-overview-france/06-social-media-and-data-privacy-in-france/.

Fransız İş Kanunu'nun L.1221-9 maddesi uyarınca, bir iş başvurusunda bulunan aday hakkında kişisel nitelikte bilgi toplanması, yalnızca bu bilgilendirmenin önceden ve açık biçimde adayın bilgisine sunulmuş bir sistem aracılığıyla gerçekleştirilmişse mümkündür. Bu hüküm, iş ilişkisinin daha başında bile bireyin veri işleme faaliyetlerine ilişkin bilgilendirilme hakkını güvence altına almaktadır[398]. Veri sahibinin bilgilendirilmesi ilkesinin bir uzantısı olarak, aynı Kanunun L.1222-4 maddesi[399] önemli bir düzenleme getirmektedir. Bu maddeye göre işveren, daha önce çalışana bildirmediği herhangi bir cihaz aracılığıyla kişisel veri toplayamaz. Ayrıca, çalışan hakkında teknik bir sistemle bilgi toplanacaksa, bu işlemin açık ve önceden bir bilgilendirme süreciyle gerçekleştirilmesi zorunludur. Bu yükümlülük yalnızca geniş çaplı sistemleri değil, çalışan ekranlarının uzaktan görüntülenmesi ya da internet kullanımının yazılımlarla izlenmesi gibi işlemleri de kapsamaktadır. Bilgilendirmenin fiili olarak izleme aracının görünür olmasıyla sınırlı tutulması yeterli değildir. Açık, anlaşılır ve belgeye dayalı biçimde bilgilendirme yapılmalıdır.

İzleme sistemleri çoğu kez otomatik veri işleme faaliyetlerini içerdiğinden, Sosyal ve Ekonomik Komite'nin sürece dâhil edilmesi zorunludur. Fransız İş Kanunu'nun L.2312-8 ve L.2312-38. maddeleri, işe alım süreçlerinde kullanılan yöntemler ile personel yönetimine yönelik otomatik veri işleme sistemlerinin ve çalışan faaliyetlerini izlemeye yönelik tekniklerin uygulanmasından önce Sosyal ve Ekonomik Komite'nin bilgilendirilmesini ve görüşünün alınmasını zorunlu kılarak, işverenin gözetim yetkisinin şeffaflık, katılım ve temel haklara saygı ilkeleriyle dengelenmesini amaçlamaktadır[400].

---

[398] Fransız İş Kanunu (Code du travail), Madde L1121-1, "Legifrance" portalı üzerinden yayımlanmıştır, erişim 22 Mayıs 2025, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006900839.

[399] Fransız İş Kanunu (Code du travail), Madde L1124-4, "Legifrance" portalı üzerinden yayımlanmıştır, erişim 22 Mayıs 2025, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006900839.

[400] Savaş, "İş Hukukunda 'Siber Gözetim'", 111. Fransız İş Kanunu'nun daha önce yürürlükte olan ilgili maddelerine göre, işverenlerin çalışanları doğrudan etkileyen belirli teknolojik yenilikleri hayata geçirmeden önce, konuyu işçi temsilcilerinden oluşan kurula bildirme ve danışma zorunluluğu bulunuyordu. Bu zorunluluk; personel yönetimi için otomatik veri sistemleri kurma, yeni teknolojileri uygulama veya çalışanların faaliyetlerini denetleyen yöntemler geliştirme gibi durumları kapsıyordu. Yürürlükten kaldırılan bu eski yükümlülükler (madde 432-2 ve 432-2-1), artık yeni kanun kapsamında L.2312-8 ve L.2312-15 maddeleriyle güncellenerek yeniden düzenlenmiştir. Konuyla ilgili ayrıntılı bilgi için bu yeni maddeler incelenebilir. Ayrıntılar için bknz. Muenchinger, "Workplace Privacy - France: Electronic Workplace Privacy in France", 421-22.

2018 yılına kadar, 6 Ocak 1978 tarihli 78-17 sayılı Bilişim, Dosyalar ve Özgürlüklere İlişkin Kanun (Loi Informatique et Liberté) uyarınca, kişisel verilerin işlenmesine veya bu işleme imkân tanıyan araçların kullanımına ilişkin faaliyetlerin, Fransız Veri Koruma Otoritesi (Commission Nationale de l'Informatique et des Libertés) nezdinde önceden bildirilmesi zorunluydu. Bu yükümlülük özellikle çalışanlara ait internet bağlantı verileri, mesaj içerikleri ve bağlantı sürelerinin kaydedilmesini sağlayan yazılımlar için geçerliydi; video gözetim sistemlerinde ise bu zorunluluk, görüntüler aracılığıyla isimlendirilebilir nitelikte bir çalışan profili oluşturulması halinde doğmaktaydı[401]. Ancak 2018 yılında Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesiyle ön bildirim sistemi kaldırılmıştır[402]. Bunun yerine, veri sorumlularının kendi uyum süreçlerini yürüttüğü ve CNIL'in gerekli görmesi hâlinde sonradan denetim gerçekleştirdiği bir öz-denetim mekanizması benimsenmiştir[403].

Fransız hukukunun getirdiği bu sıkı bilgilendirme ve danışma yükümlülükleri, özellikle tele çalışma modelinde kullanılacak izleme yazılımları veya yöntemleri açısından da büyük önem taşımaktadır. Çalışanın kendi özel konutunda iş görmesi durumunda, işverenin uygulayacağı izleme tekniklerinin orantılılığı ve gerekliliği daha titiz bir değerlendirmeyi zorunlu kılar. Ayrıca, çalışanın (veya temsilcilerinin) süreç hakkında tam olarak bilgilendirilmesi de bir diğer önemli gerekliliktir. Örneğin, bir tele çalışanın bilgisayar aktivitelerini sürekli kaydeden bir yazılımın kurulması, hem

---

[401] Muenchinger, "Workplace Privacy - France: Electronic Workplace Privacy in France", 422.

[402] Fransız Yargıtayı'nın Sosyal Dairesi, 2014 yılında verdiği bir kararla, Avrupa Birliği Genel Veri Koruma Tüzüğü yürürlüğe girmeden önceki dönemin veri koruma kurallarının önemini vurgulayan bir ilkeye imza atmıştır. Söz konusu davada bir işveren, çalışanının bilgisayarına kurduğu bir yazılım aracılığıyla e-posta trafiğini denetlemiş ve çalışanın çalışma saatleri içinde toplam 1.228 adet kişisel e-posta gönderip aldığını tespit etmiştir. İşveren, bu tespiti çalışanın iş sözleşmesini feshetmek için delil olarak kullanmak istemiştir. Ancak, bu tür bir veri işleme faaliyeti için dönemin kanunları uyarınca Fransız Veri Koruma Otoritesi'ne (Commission Nationale de l'Informatique et des Libertés) yapılması zorunlu olan ön bildirimi, işten çıkarma süreci başladıktan sonra gerçekleştirmiştir. Yargıtay, veri işleme faaliyetine ilişkin yasal bildirim prosedürünün zamanında yerine getirilmemesi nedeniyle, elde edilen e-posta verilerinin hukuka aykırı delil niteliğinde olduğuna hükmetmiştir. Bu sebeple, söz konusu verilerin çalışanın işten çıkarılmasına gerekçe olarak sunulamayacağına ve mahkemede delil olarak kabul edilemeyeceğine karar vermiştir. Bknz. Arrêt du 8 octobre 2014, no. 13-14.991 (2014), https://www.legifrance.gouv.fr/juri/id/JURITEXT000029565250 https://www.legifrance.gouv.fr/juri/id/JURITEXT000029565250 erişim 22.05.2025; Myrtille Lapuelle, "Are You Monitoring Your French Employees? Make Sure You Have Registered That Activity with the CNIL!", *OF DIGITAL INTEREST*, 31 Ekim 2014, https://www.ofdigitalinterest.com/2014/10/are-you-monitoring-your-french-employees-make-sure-you-have-registered-that-activity-with-the-cnil/.

[403] Aloisi ve Gramano, "Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context", 111-12.

çalışana önceden detaylı bilgi verilmesini hem de Sosyal ve Ekonomik Komite'nin görüşünün alınmasını gerektirmektedir[404].

Fransız Medeni Kanunu'nun (Code Civil) 9. maddesi (Article 9 – Chacun a droit au respect de sa vie privée), "her bireyin özel hayatına saygı gösterilmesini isteme hakkına sahip olduğunu" düzenlemekte ve bu hüküm, kişisel mahremiyetin korunmasına dair temel bir anayasal ilkeye dayanmaktadır. Söz konusu hüküm, iş ilişkileri çerçevesinde gerçekleştirilen izleme ve gözetleme faaliyetlerine doğrudan uygulanmaktadır. Nitekim işverenin, çalışanları denetleme yetkisi bulunsa da bu yetkinin kullanımı sırasında çalışanın özel hayatına keyfî veya orantısız müdahalelerde bulunması hukuka aykırılık teşkil etmektedir. Özellikle dijital izleme araçları yoluyla çalışanın kişisel e-posta içeriklerine, özel olarak işaretlenmiş dosyalarına ya da internet kullanım geçmişine onun açık bilgisi ve rızası olmadan erişilmesi özel hayatın gizliliğinin ihlali olarak değerlendirilmektedir. Fransız Yargıtayı'nın içtihatları da bu doğrultuda gelişmiş ve işverenin denetim faaliyetlerinin, ancak meşru bir amaçla, şeffaflık ilkesine uygun biçimde ve orantılılık sınırları içinde gerçekleştirilebileceği vurgulanmıştır[405].

---

[404] Fransız Veri Koruma Otoritesi, çalışan gözetiminde orantılılık ilkesinin ihlaline dair önemli bir örnek teşkil eden bir karar vermiştir. Karara konu olan olayda, gayrimenkul sektöründe faaliyet gösteren bir şirket, iki farklı yöntemle çalışanlarını denetim altına almıştır. Bunlardan ilki, uzaktan çalışan personelin faaliyetlerini izlemek amacıyla bilgisayarlarına bir yazılım yüklemek; ikincisi ise, tesislerinde hırsızlık gibi maddi hasarları önleme gerekçesiyle bir video gözetim sistemi kurmaktır. Yapılan şikâyetler üzerine Fransız Veri Koruma Otoritesi tarafından gerçekleştirilen denetim, şirketin beyan ettiği amaçları aşan ve çalışanların özel hayatlarına ağır müdahalede bulunan uygulamaları ortaya çıkarmıştır. Denetimde, çalışanların mola zamanları da dâhil olmak üzere video gözetim sistemiyle kesintisiz olarak izlendikleri tespit edilmiştir. Buna ek olarak, yasal bir dayanağı olmaksızın ortam seslerinin de kaydedildiği ve bilgisayarlara kurulan yazılım aracılığıyla çalışanların performansının aşırı ayrıntılı ve müdahaleci bir şekilde analiz edildiği anlaşılmıştır. Bu ağır ihlaller neticesinde, Fransız Veri Koruma Otoritesi'nin yaptırım organı, şirkete 40.000 Avro idari para cezası uygulanmasına karar vermiştir. Para cezasının miktarı, ihlallerin ciddiyeti ile şirketin mali durumu arasında bir denge kurularak hem caydırıcı hem de orantılı olacak şekilde belirlenmiştir. İhlalin ciddiyeti ve diğer şirketlere örnek teşkil etmesi amacıyla kararın kamuoyuyla paylaşılmasına hükmedilmiştir. Ancak, denetim sırasında şirketin iş birliği yaparak söz konusu yazılımı derhal kaldırması ve küçük ölçekli bir işletme olması gibi hafifletici nedenler göz önünde bulundurularak, ticari itibarını korumak amacıyla şirket isminin gizli tutulmasına karar verilmiştir. Bknz. CNIL, "Surveillance Excessive Des Salariés: Sanction De 40 000 Euros À L'encontre D'une Entreprise Du Secteur Immobilier", Resmi Site, 04 Şubat 2025, https://www.cnil.fr/fr/surveillance-excessive-des-salaries-sanction-de-40-000-euros-entreprise-secteur-immobilier.

[405] Fransız Yargıtayı Sosyal Dairesi'nin (Cour de cassation - chambre sociale) 2 Ekim 2001 tarihli ve kamuoyunda "Nikon Kararı" olarak bilinen kararı, işyerinde mahremiyetin korunması açısından dönüm noktası niteliğindedir. Bu kararda, işverenin işçiye ait dijital içerikleri hangi koşullarda inceleyebileceği ve çalışanın özel yaşamının hangi sınırlar içinde korunacağı ayrıntılı biçimde değerlendirilmiştir. Sosyal Daire, özellikle çalışanın "kişisel" ibaresiyle açıkça işaretlediği e-posta mesajları, dijital belgeler ve diğer iletişim içeriklerinin özel hayat kapsamında değerlendirilmesi gerektiğini vurgulamıştır. Bu kapsamda, çalışanın kişisel alanına müdahale anlamına gelecek şekilde, işverenin çalışanın bilgisi ve

Fransız Ceza Kanunu'nda (Code pénal) ise çalışanların özel hayatının ve kişisel verilerinin korunmasına ilişkin önemli güvenceler içermektedir. Özellikle Fransız Ceza Kanunu 226-15. madde, haberleşme gizliliğini teminat altına alarak, işverenin çalışana ait kişisel e-posta içeriklerini rızası olmadan incelemesini açıkça yasaklamaktadır. Yargı içtihatları doğrultusunda, işveren yalnızca internet kullanım süreleri, erişilen web siteleri gibi sınırlı teknik verileri mahkemeye delil olarak sunabilmekte; buna karşılık kişisel e-posta içerikleri özel hayat kapsamında değerlendirilerek delil niteliği taşımadığı kabul edilmektedir[406]. Bu bağlamda, Fransız Ceza Kanunu 226-1. madde uyarınca kişinin rızası olmaksızın özel alanda görüntüsünün kayda alınması; 226-18. madde gereğince hukuka aykırı veya adaletsiz biçimde kişisel veri toplanması; 226-20. madde kapsamında verilerin gereğinden uzun süre saklanması; 226-21. madde uyarınca kişisel verilerin işlendiği sistemlerin amacına aykırı şekilde kötüye kullanılması ve R625-10. madde çerçevesinde

---

rızası olmaksızın bu tür içerikleri incelemesi hukuka aykırı bulunmuştur. Kararda, bu şekilde elde edilen verilerin disiplin süreçlerinde delil olarak kullanılamayacağı da açıkça belirtilmiştir. Mahkeme ayrıca, bu tür keyfî denetimlerin, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde güvence altına alınan özel hayatın ve haberleşmenin gizliliği hakkına ve Fransız Medeni Kanunu'nun 9. maddesinde düzenlenen özel yaşamın korunması ilkesine aykırılık teşkil ettiğini hükme bağlamıştır. Bknz. Muenchinger, "Workplace Privacy - France: Electronic Workplace Privacy in France", 423; Savaş, "İş Hukukunda 'Siber Gözetim'", 112.

[406] Fransız Yargıtayı Sosyal Dairesi, çalışanların gözetlenmesiyle elde edilen delillerin kullanılmasına ilişkin yerleşik içtihadında önemli bir istisna tanımlamıştır. Genel kural, çalışanlara önceden bildirim yapılmadan elde edilen video kayıtları veya kişisel e-posta yazışmaları gibi delillerin, özel hayatın gizliliğini ihlal etmesi nedeniyle hukuka aykırı sayılması ve mahkemede kullanılamamasıdır. Ancak Yargıtay, bu kararlarında, söz konusu delillerin işverenin haklarını korumak için vazgeçilmez olması durumunda, belirli şartlar altında kabul edilebileceğine hükmetmiştir. Bu içtihat değişikliğine yol açan olaylardan ilkinde, bir şirket, çalışanının çok gizli nitelikteki ticari bilgileri rakip bir firmaya aktardığını gösteren ve gizlice alınmış bir video kaydının dökümünü delil olarak sunmuştur. İkinci olayda ise, bir başka işveren, çalışanının kişisel e-posta hesabını kullanarak rakip bir şirket kurma hazırlığı yaptığını ve bu süreçte şirket sırlarını üçüncü kişilerle paylaştığını ispat etmeye çalışmıştır. Her iki davada da sunulan deliller, çalışana önceden bildirim yapılmaması ve kişisel iletişiminin denetlenmesi nedeniyle ilke olarak hukuka aykırı kabul edilmekteydi. Ancak Yargıtay, bu noktada yeni bir denge kurarak, çalışanın özel hayatına saygı hakkı ile işverenin meşru menfaatlerini ve ispat hakkını tartmıştır. Mahkeme, bu tür hukuka aykırı bir delilin mahkemede kabul edilebilmesi için iki şartın birlikte gerçekleşmesi gerektiğine karar vermiştir: 1. Sunulan delilin, işverenin iddialarını ispatlamak için sahip olduğu tek imkân olması (vazgeçilmezlik). 2. Çalışanın mahremiyetine yapılan müdahalenin, şirketin ticari sırları gibi korunmaya değer meşru menfaatiyle kıyaslandığında orantılı olması. Sonuç olarak bu kararlar, çalışanın özel hayatına saygı hakkının mutlak olmadığını; şirketin ticari sırlarının ifşası gibi ağır durumlarda, işverenin ispat hakkı ve meşru menfaatlerinin, sıkı bir orantılılık denetimi çerçevesinde çalışanın mahremiyet hakkına üstün gelebileceğini göstermektedir. Bknz. Arrêt n° 166 F-D, 26 février 2025, pourvoi n° 22-24.474. (2025), https://www.courdecassation.fr/decision/67bebec5ab77563075a5941e https://www.courdecassation.fr/decision/67bebec5ab77563075a5941e, erişim 22.05.2025; Arrêt du 22 février 2025. Pourvoi n° 22-18.179 (2025), https://www.courdecassation.fr/decision/67bebeb8ab77563075a5940e https://www.courdecassation.fr/decision/67bebeb8ab77563075a5940e, erişim 22.05.2025; "France: Video Surveillance Cannot Permanently Monitor the Activity of an Employee Working Alone".

bireylerin yeterli şekilde bilgilendirilmemesi hâllerinde, işverenin cezai sorumluluğu gündeme gelebilmektedir[407].

3.4.2.1.3. Diğer Avrupa Birliği Üye Devletleri

Covid 19 Pandemisi sonrasında uzaktan ve hibrit çalışma modellerinin hızla yaygınlaşması, dijital gözetim yazılımlarına yönelik ilginin artmasına neden olmuş ve bu alandaki hukuki belirsizlikleri daha görünür kılmıştır. Örneğin İtalya'da CCTV sistemlerinin kurulumu, işçi temsilcileriyle yapılacak toplu sözleşmeye bağlanmış ve yüksek risk taşıyan sistemlerde etki değerlendirmesi zorunlu tutulmuştur. İspanya, Kişisel Verilerin Korunması ve Dijital Hakların Güvence Altına Alınmasına İlişkin 3/2018 sayılı Organik Kanun ile video gözetim ve konum takibine karşı çalışanların mahremiyetini güvence altına alırken; Slovenya 2023 tarihli yeni Veri Koruma Kanunu kapsamında kamera sistemlerinin kurulmasından önce işçi temsilcileri ve sendikalarla istişare şartı getirmiştir. Danimarka'da ise 2023 yılında güncellenen Video Gözetim Kanunu, kamera kullanımına yalnızca güvenlik ve suç önleme amacıyla izin vermekte; çalışan performansının izlenmesini açıkça yasaklamaktadır[408].

Yunanistan'da çalışanların izlenmesi ve gözetlenmesine ilişkin hukuki çerçeve, özellikle 4808/2021 sayılı İş İlişkilerinin Korunması Hakkındaki Kanun ve bunu tamamlayan 5053/2023 sayılı İş İlişkilerinin Güçlendirilmesi Hakkındaki değişiklik kanunuyla düzenlenmiştir. Bu düzenlemeler, tele çalışmanın yaygınlaşmasıyla birlikte işverenin çalışan performansını denetleme yetkisini tanımakla birlikte, bu yetkinin kullanımını kişisel verilerin korunması ve özel hayata saygı ilkeleriyle sınırlandırmaktadır. İşverenlerin web kamerası yoluyla çalışanların performansını izlemesi açıkça yasaklanmış; klavye izleme (keylogger), görüntü tanıma yazılımları, ekran paylaşımı zorunluluğu gibi uygulamalar, Yunan Kişisel Verileri Koruma Kurumu (Hellenic Data Protection Authority) tarafından orantılılık ilkesine aykırı ve çalışanların profillenmesine yol açtığı gerekçesiyle yasa dışı kabul edilmiştir. Öte yandan, dijital çalışma kartı ve "ERGANI II" sistemi (çalışma sürelerinin ve iş gücü

[407] Eurofound, "France: Employee Monitoring and Surveillance", Restructuring Legislation European Restructuring Monitor (ERM), 01 Kasım 2023, https://apps.eurofound.europa.eu/legislationdb/employee-monitoring-and-surveillance/france.
[408] Riso ve Litardi, "Employee Monitoring: A Moving Target for Regulation".

hareketlerinin gerçek zamanlı olarak takip edilmesini sağlayan dijital kamu bilgi sistemi) aracılığıyla, çalışanların işe başlama-bitiş saatleri, molaları ve izin günleri gibi bilgiler işveren tarafından gerçek zamanlı olarak takip edilebilmektedir. Bununla birlikte, performans değerlendirmesi amacıyla CCTV kayıtlarının kullanılması yasaktır. Ayrıca, çalışanlara çalışma saatleri dışında dijital iletişime yanıt vermeme hakkı tanıyan "bağlantıyı kesme hakkı" yasal güvence altına alınmış ve bu hakkın kullanılması nedeniyle herhangi bir ayrımcılık yapılmayacağı hükme bağlanmıştır[409].

Güney Kıbrıs'ta 01 Aralık 2023 tarihinde yürürlüğe giren 120(I)/2023 sayılı "Uzaktan Çalışmanın Düzenlenmesine İlişkin Kanun" uyarınca, işverenlerin uzaktan çalışanların performansını değerlendirirken çalışanların özel hayatına saygılı olmaları ve kişisel verilerin korunmasına ilişkin mevzuata uygun hareket etmeleri zorunlu kılınmıştır. Söz konusu Kanun kapsamında, çalışan izleme sistemlerinin devreye alınmasından önce, işverenlerin Kişisel Verileri Koruma Komiseri (Commissioner for the Protection of Personal Data) ile önceden istişarede bulunmaları ve bir veri koruma etki değerlendirmesi (Data Protection Impact Assessment) gerçekleştirmeleri gerekmektedir. Bu yükümlülük, sistemin devreye alınmasından önce yerine getirilmelidir. Ayrıca ilgili Kanun'da açıkça, işverenlerin çalışan performansını izlemek amacıyla sürekli biçimde kamera veya benzeri müdahaleci teknolojik araçlar (örneğin, izleme yazılımları veya ekran kayıt sistemleri) kullanmaları yasaklanmıştır[410].

Portekiz, uzaktan gözetim araçlarının kapsamı ve kullanım biçimi hakkında çalışanlara ayrıntılı bilgi verilmesini zorunlu tutarak, iş ilişkilerinde şeffaflığın artırılmasını amaçlamıştır. 83/2021 sayılı Kanun ile Portekiz İş Kanunu'na (Código do Trabalho)

---

[409] Eurofound, Greece: Employee Monitoring and Surveillance (European Foundation for the Improvement of Living and Working Conditions (Eurofound), 2023), https://www.eurofound.europa.eu/data/platform-economy/employee-monitoring-and-surveillance/greece; "Greece: Greek Law 4808/2021 - Major Reforms in Employment Legislation", IOE-EMP, 23 Ağustos 2021, https://industrialrelationsnews.ioe-emp.org/industrial-relations-and-labour-law-august-2021-1/news/article/greece-greek-law-4808-2021-major-reforms-in-employment-legislation.

[410] Eliada Georgiades ve Nadia Tryfonidou, "Regulating Remote Work", 2023, https://gzg.com.cy/insights/insights/Regulating-Remote-Work-in-Cyprus/; George Apostolou ve Alexandros Tsolias, "Cyprus Employment Series: Navigating the Evolving Landscape of Remote Working and the Right to Disconnect in Cyprus", Harneys, erişim 22 Mayıs 2025, https://www.harneys.com/insights/navigating-the-evolving-landscape-of-remote-working-and-the-right-to-disconnect-in-cyprus/.

eklenen 169-A(4) ve (5), 170(1) ila (5) ve 20. maddeler uyarınca, tele çalışma kapsamında işverenin çalışan üzerindeki izleme yetkisi açık biçimde sınırlandırılmıştır. Anılan düzenlemelere göre, çalışanla sürekli sesli veya görüntülü bağlantı kurulması yasağı açıkça öngörülmekte; izleme faaliyetlerinin yalnızca çalışan tarafından bilinen iletişim ve bilişim sistemleri aracılığıyla, özel hayata saygı çerçevesinde ve orantılılık, şeffaflık ile bilgilendirme ilkelerine uygun biçimde yürütülmesi zorunlu kılınmaktadır. Bu normatif çerçeve, Portekiz Kişisel Verileri Koruma Kurumu (Comissão Nacional de Proteção de Dados) tarafından 17 Nisan 2020 tarihinde yayımlanan "Uzaktan Çalışmada Gözetim" başlıklı rehber ile de pekiştirilmiştir. Rehberde, çalışan performansının izlenmesine yönelik olarak kullanılan TimeDoctor, Hubstaff, ManicTime, TimeCamp gibi dijital yazılımların, izleme amacıyla gerçek zamanlı veri ve konum takibi yapmaları nedeniyle veri minimizasyonu ve çalışan mahremiyeti ilkelerine aykırılık teşkil ettiği ifade edilmiştir. Aynı belge, çalışanın konutunun işin ifa edildiği yer olmasının işverenin izleme yetkisini genişletmeyeceğini, aksine bu yetkinin fiziki olarak işyeri sınırlarını aşmaması gerektiğini açıkça vurgulamaktadır[411].

Görüldüğü üzere getirilen düzenlemeler, yalnızca soyut ilkeler ortaya koymakla yetinmeyip; belirli teknolojilerin kullanımını açıkça yasaklamak, veri koruma etki değerlendirmelerini şart koşmak ve düzenleyici otoritelerin yayımladığı rehberler vasıtasıyla sakıncalı yazılımlara işaret etmek gibi somut araçlarla etkin bir koruma çerçevesi tesis etmektedir. Bu hukuki yaklaşımın temelinde, çalışanın ikametgâhının işin ifa edildiği yere dönüşmesinin, işverene ilave gözetim yetkileri tanımayacağı prensibi yatmaktadır. Bu bağlamda, kullanılan yazılımların ayrıntılı olarak yasaklanması gibi kazuistik yöntemler tek başına bir çözüm teşkil etmese de müdahaleci nitelikteki uygulamaların barındırdığı riskler konusunda farkındalık yaratılması ve tele çalışanların mahremiyetini korumaya yönelik spesifik düzenlemelerle olası zararların proaktif bir şekilde önlenmesi elzem bir gereklilik olarak ortaya çıkmaktadır.

[411] Catarina de Oliveira Carvalho, "The New Regulation of Telework and Remote Work in Portugal: Considerations and Prospects", *E-Journal of International and Comparative Labour Studies* 11, sy 03 (2022): 15-16.

3.4.2.2. Birleşik Krallık

Birleşik Krallık, kodifiye edilmiş ve tekil bir anayasa metnine sahip olmamakla birlikte, temel hak ve özgürlüklerin korunması bakımından hem Avrupa İnsan Hakları Sözleşmesi'ne dayalı bir yapıya hem de Magna Carta (1215), Bill of Rights (1689), ve Habeas Corpus Act (1679) gibi tarihsel ve anayasal nitelikteki belgelere dayanan güçlü bir anayasal gelenek ve normatif çerçeveye sahiptir. 1998 yılında kabul edilen İnsan Hakları Kanunu (Human Rights Act 1998) ile AİHS hükümleri iç hukuka dâhil edilmiş ve 8. madde kapsamında yer alan özel hayatın gizliliği hakkı, Birleşik Krallık vatandaşları bakımından doğrudan ileri sürülebilir bir hak hâline gelmiştir[412].

Birleşik Krallık'ta işverenin çalışan üzerindeki denetim yetkisinin sınırları, bir yandan AİHS'nin 8. maddesi ile çizilirken, diğer yandan ulusal düzenlemelerle detaylandırılmıştır. Bu kapsamda, Birleşik Krallık'ın veri koruma hukuku önemli bir dönüşüm geçirmiştir. İlk olarak 1998 tarihli Veri Koruma Kanunu (Data Protection Act), o dönemdeki 95/46/EC sayılı Avrupa Birliği Veri Koruma Direktifi'ni iç hukuka aktarmıştır. Daha sonra bu Kanun, 2018 yılında AB Genel Veri Koruma Tüzüğü ile tam uyumlu hâle getirilmek üzere güncellenmiştir. Brexit sonrasında ise, 1 Ocak 2021 tarihi itibarıyla Birleşik Krallık, Avrupa Birliği veri koruma rejiminden ayrılmış ve Birleşik Krallık Genel Veri Koruma Kanunu 2018 (UK GDPR) yürürlüğe girmiştir. UK GDPR, esas itibarıyla AB GDPR'nin iç hukuka aktarılmış ve uyarlanmış versiyonu olup, veri sorumlularının yükümlülüklerini ve veri işleme faaliyetlerinin hukuka uygunluk kriterlerini korumaktadır. Böylelikle, güncel olarak Brexit sonrası Avrupa Birliği Genel Veri Koruma Tüzüğü, Birleşik Krallık iç hukukuna UK GDPR adıyla uyarlanmıştır. Bu düzenleme, Data Protection Act 2018 (DPA 2018) ile birlikte ele alınmaktadır[413].

Birleşik Krallık'ta iş ilişkileri çerçevesinde iletişim gözetimi, çeşitli düzenlemelerle hukuki çerçeveye oturtulmuştur[414]. Soruşturma Yetkilerinin Düzenlenmesi Kanunu 2000 (The Regulation of Investigatory Powers Act 2000 - RIPA), işverenlerin iletişim müdahalesi ve elektronik verilere erişim gibi gözetim faaliyetlerini yalnızca çalışanın

[412] Savaş, "İş Hukukunda 'Siber Gözetim'", 108.
[413] "Data Protection", Resmi Site, GOV.UK, erişim 13 Nisan 2025, https://www.gov.uk/data-protection.
[414] Savaş, "İş Hukukunda 'Siber Gözetim'", 108-9.

açık rızası ya da meşru bir yasal gerekçeye dayanarak gerçekleştirebileceğini öngörmektedir[415]. Mahremiyet ve Elektronik Haberleşme Düzenlemeleri 2003 (Privacy and Electronic Communications Regulations 2003 - PECR) ise e-posta, telefon ve internet gibi elektronik iletişim araçları üzerinden yapılan izlemelerde, işverenin çalışanı önceden bilgilendirme ve kimi hâllerde rıza alma yükümlülüğünü düzenlemektedir[416]. Bu düzenlemeleri tamamlayan Telekomünikasyon Düzenlemeleri 2000 (Telecommunications Regulations 2000), işverenin sistem güvenliğini sağlama veya kötüye kullanımı önleme gibi meşru amaçlarla işle ilgili iletişimleri, çalışan rızası olmaksızın izlemesine imkân tanımakta; ancak bu izleme faaliyetinin yalnızca işle sınırlı, önceden bildirilmiş ve ölçülü olması gerektiğini vurgulamaktadır[417]. Son olarak, doğrudan özel sektör işverenlerini hedef almamakla birlikte, Soruşturma Yetkileri Kanunu (Investigatory Powers Act 2016 - IPA) kamu otoritelerinin iletişim verilerine erişimini düzenleyerek haberleşme denetiminin genel sınırlarını belirleyen tamamlayıcı bir düzenleme işlevi görmektedir[418].

Birleşik Krallık'ta veri koruma alanındaki en önemli otorite olan Bilgi Komiserliği Ofisi (Information Commissioner's Office - ICO), iş ilişkileri kapsamındaki izleme ve gözetleme faaliyetlerine ilişkin temel standartları belirleyen ve işverenlere yol gösteren kapsamlı rehberler yayımlamaktadır. Özellikle Ekim 2023'te yayımlanan "İstihdam uygulamaları ve veri koruma: çalışanların izlenmesi" (Employment practices and data protection: monitoring workers) başlıklı güncel rehber, işverenlerin çalışanları izlerken uyması gereken temel ilkeleri modern çalışma pratiklerini de dikkate alarak açık bir şekilde ortaya koymuştur. Bu ilkeler arasında; çalışanların hangi izleme faaliyetlerine tabi tutulacakları konusunda açık, anlaşılır ve kolay erişilebilir bir şekilde bilgilendirilmesi, izlemenin dayandığı amaçların belirli, açık ve meşru olması, kullanılan izleme yöntemlerinin bu amaçlara ulaşmak için gerekli, orantılı ve en az müdahaleci nitelikte seçilmesi ile özellikle mahremiyet açısından yüksek risk taşıyan izleme faaliyetleri (örneğin, tele çalışma modelinde evden yapılan sürekli

---

[415] Regulation of Investigatory Powers Act 2000, c. 23 (2000), https://www.legislation.gov.uk/ukpga/2000/23.
[416] The Privacy and Electronic Communications (EC Directive) Regulations 2003, S.I. 2003 No. 2426 (2003), https://www.legislation.gov.uk/uksi/2003/2426/contents/made.
[417] PECR 2003, S.I. 2003 No. 2426.
[418] Investigatory Powers Act 2016 (2016), https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

izleme veya biyometrik veri işleme) öncesinde mutlaka veri koruma etki değerlendirmesi yapılması gibi kritik hususlar bulunmaktadır[419]. ICO'nun daha önce yayımladığı Çalışma Uygulamaları Kılavuzu (Employment Practices Code 2011) belgesi de benzer şekilde, izleme faaliyetlerinin şeffaf, ölçülü ve yalnızca meşru amaçlarla sınırlı olması gerektiğini vurgulamaktadır[420].

Günümüzde Birleşik Krallık veri koruma mevzuatında reform yapılması yönünde değişikler yapılmıştır. Bu kapsamda hazırlanan henüz kabul edilmeyen Veri Koruma ve Dijital Bilgi Kanunu (Data Protection and Digital Information Act), veri sorumlularının yükümlülüklerini sadeleştirmeyi, dijital kimliklerin kullanımını teşvik etmeyi ve Bilgi Komiserliği Ofisi'nin yapısını yeniden şekillendirmeyi amaçlamaktadır[421].

3.4.2.3. Amerika Birleşik Devletleri

Amerika Birleşik Devletleri'nde işçilere yönelik izleme faaliyetleri esas itibarıyla 1986 tarihli Elektronik İletişim Gizliliği Kanunu (Electronic Communications Privacy Act) kapsamında düzenlenmektedir. Bu Kanun, elektronik iletişimin kasıtlı olarak izlenmesini genel olarak yasaklamakla birlikte, "işin yürütülmesinden kaynaklanan meşru nedenler" (Business Purpose Exception) ve "çalışan rızası" gibi istisnalarla işverenlere takdir yetkisi tanımaktadır[422]. Ayrıca, iletinin anlık izlenmesi *(real-time*

---

[419] Information Commissioner's Office (ICO), Employment Practices and Data Protection: Monitoring Workers (Information Commissioner's Office (ICO), 2023), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/.

[420] Information Commissioner's Office (ICO), The Employment Practices Code (Information Commissioner's Office (ICO), 2011), https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf.

[421] Data Protection and Digital Information Bill, HL Bill 67, UK Parliament Sessions 2022–23, 2023–24, erişim 13 Mayıs 2025, https://bills.parliament.uk/bills/3430.

[422] Amerika Birleşik Devletleri'nde iş ilişkisinde izleme ve gözetlemeye ilişkin hukuki çerçeve, çeşitli yargı kararlarıyla biçimlenmiştir. Bu kararlar, özellikle çalışanların mahremiyet hakları ile işverenin denetim ve kontrol yetkisi arasında bir denge kurulması gerektiğini vurgulamaktadır. Kamu çalışanlarının işyerindeki mahremiyet haklarına ilişkin hukuki standardı belirleyen O'Connor v. Ortega (1987) davasında , Amerika Birleşik Devletleri Yüksek Mahkemesi (Supreme Court of the United States), devlet kurumlarında yapılan aramaların Anayasa'nın Dördüncü Değişikliği (Fourth Amendment) kapsamında nasıl değerlendirileceğine dair temel bir çerçeve çizmiştir. Dava, bir devlet hastanesinde çalışan doktorun (Ortega), göreviyle ilgili bir suistimal soruşturması sırasında ofisi ve çalışma masasının amirleri tarafından aranması üzerine açılmıştır. Yüksek Mahkeme, öncelikle kamu çalışanlarının işyerlerinde, özellikle kendi ofisleri, masaları ve dolapları gibi alanlarda, belirli bir ölçüde "makul bir gizlilik beklentisine" (reasonable expectation of privacy) sahip olduklarını kabul etmiştir. Ancak bu hakkın mutlak olmadığını belirten Mahkeme, işverenin denetimi için ceza hukukundaki gibi katı bir "muhtemel sebep" (probable cause) veya "arama kararı" (warrant) şartının aranmayacağını, zira

bunun kamu hizmetlerinin verimliliğini engelleyeceğini ifade etmiştir. Bunun yerine Mahkeme, bu tür aramaların meşruiyeti için iki aşamalı bir "makuliyet" (reasonableness) testi geliştirmiştir: Birincisi, aramanın başlangıçta haklı bir gerekçeye (örneğin, işle ilgili bir suistimal şüphesi veya kurumsal bir ihtiyacın karşılanması) dayanması; ikincisi ise aramanın kapsamının, başlangıçtaki amaçla orantılı ve ölçülü olmasıdır. Bu karar, kamu çalışanlarının mahremiyet hakları ile devletin bir işveren olarak verimli çalışma ortamı sağlama ve denetim yapma yönündeki meşru menfaatleri arasında bir denge kurmuş ve sonraki yıllarda dijital iletişim araçlarının denetlenmesi gibi konularda da referans alınan temel bir içtihat haline gelmiştir. Bknz. O'Connor v. Ortega 480 U.S. 709 (1987), No. 86-630 (Supreme Court of The United States 31 Mart 1987), https://supreme.justia.com/cases/federal/us/480/709/; City of Ontario v. Quon (2010) kararında, Amerika Birleşik Devletleri Yüksek Mahkemesi (Supreme Court of the United States), işverenin denetim yetkisini teknolojik gelişmeler bağlamında değerlendirmiştir. Dava, bir belediye polis memurunun (Jeff Quon), departman tarafından kendisine tahsis edilen bir çağrı cihazı (pager) üzerinden gönderdiği ve karakter sınırını aşması nedeniyle ek ücrete tabi olan kısa mesajların denetlenmesi üzerine açılmıştır. Yüksek Mahkeme, hızla değişen teknoloji karşısında çalışanların gizlilik beklentilerine ilişkin geniş ve kesin bir kural koymaktan bilinçli olarak kaçınmış; bunun yerine, davanın koşulları gereği çalışanın belirli bir ölçüde mahremiyet beklentisine sahip olduğunu varsayarak ilerlemiştir. Mahkeme, bu varsayıma rağmen denetimin hukuka uygun olduğuna karar vermiştir. Bu sonuca ulaşırken, denetimin temel amacının, mesajlaşma planının işle ilgili ihtiyaçlar için yeterli olup olmadığını belirlemek gibi meşru bir iş amacına dayandığını ve bir suistimal soruşturması niyetiyle başlamadığını tespit etmiştir. Ayrıca, yapılan incelemenin kapsamının bu amaçla sınırlı ve ölçülü tutulması, denetimi makul kılmıştır. Sonuç olarak Yüksek Mahkeme, işverenin, işle bağlantılı meşru bir gerekçeyle ve orantılı bir kapsamda gerçekleştirdiği bu denetimin, çalışanın Anayasal haklarını ihlal etmediğine hükmetmiştir. Bknz. Ontario v. Quon, 560 U.S. 746 (2010), No. 08-1332 (Supreme Court of The United States 17 Haziran 2010), https://supreme.justia.com/cases/federal/us/560/746/; Stengart v. Loving Care Agency, Inc. davasında, New Jersey Yüksek Mahkemesi (Supreme Court of New Jersey), işverenin denetim yetkisinin sınırlarını belirleyen önemli bir karara imza atmıştır. Davaya konu olan olayda, bir çalışan (Stengart), kendisine tahsis edilen şirket dizüstü bilgisayarını kullanarak kişisel ve şifre korumalı web tabanlı e-posta hesabına erişmiş ve bu hesap üzerinden, işverenine karşı açmayı planladığı bir dava ile ilgili olarak avukatıyla yazışmıştır. İşverenin, çalışan işten ayrıldıktan sonra bilgisayarın sabit diskinden bu e-postaları adli bilişim yöntemleriyle kurtarması ve davada delil olarak kullanmak istemesi üzerine mahkeme, çalışanın bu iletişimlerde makul bir gizlilik beklentisi (reasonable expectation of privacy) taşıdığına hükmetmiştir. Mahkeme, bu kararını iki temel gerekçeye dayandırmıştır: Birincisi, iletişimin kamu politikası tarafından güçlü bir şekilde korunan avukat-müvekkil gizliliği kapsamında olmasıdır. İkincisi ise, işverenin elektronik kullanım politikasının, kişisel web tabanlı e-posta hesaplarının içeriğinin izleneceği ve kaydedileceği konusunda açık ve net bir uyarı içermeyip, aksine "ara sıra kişisel kullanıma" izin vermesi nedeniyle belirsiz olmasıdır. Bu doğrultuda mahkeme, çalışanın şirket ekipmanını kullanmasının, özellikle bu denli ayrıcalıklı ve hassas kişisel içeriklerin işveren tarafından denetlenmesini otomatik olarak meşru kılmayacağını kesin bir dille ifade etmiştir. Bu karar, işverenin izleme politikasının kapsamı ve açıklığının hukuki sonuçlar doğuracağını ve avukat-müvekkil gizliliği gibi temel hakların, işyeri denetimi karşısında dahi güçlü bir korumaya sahip olduğunu gösteren kritik bir emsal oluşturmaktadır Stengart v. Loving Care Agency, Inc. (A-16-09), Nos. 300, 990 A.2d 650 (Supreme Court of New Jersey 30 Mart 2010), https://law.justia.com/cases/new-jersey/supreme-court/2010/a-16-09-opn.html; Smyth v. Pillsbury Co. davası, Amerika Birleşik Devletleri'nde işyerinde elektronik haberleşmenin gizliliğine ilişkin sınırları belirleyen ve bu alanda temel bir emsal teşkil eden öncü kararlardan biridir. Davanın temelinde, bir çalışanın (Smyth), şirket e-posta sistemi üzerinden yöneticisine, diğer şirket yöneticileri hakkında aşağılayıcı ve profesyonellik dışı ifadeler içeren mesajlar göndermesi ve bu sebeple iş sözleşmesinin feshedilmesi yatmaktadır. Olayı hukuken karmaşıklaştıran kilit nokta, işveren Pillsbury'nin daha önce çalışanlarına, e-posta iletişimlerinin tamamen gizli kalacağı ve bu yazışmaların denetlenerek bir fesih gerekçesi olarak kullanılmayacağı yönünde tekrarlanan güvenceler vermiş olmasıdır. Buna rağmen, davaya bakan Amerika Birleşik Devletleri Pensilvanya Doğu Bölgesi Bölge Mahkemesi (United States District Court for the Eastern District of Pennsylvania), çalışanın, işverene ait bir iletişim ağını gönüllü olarak kullandığı anda bu platform üzerinde makul bir gizlilik beklentisi (reasonable expectation of privacy) olamayacağına hükmetmiştir. Kararda, işverenin kendi bilişim sistemlerinde düzeni sağlama, uygunsuz ve potansiyel olarak yasa dışı iletişimi önleme yönündeki meşru işletmesel menfaatinin, çalışanın sınırlı mahremiyet beklentisine kıyasla daha ağır bastığı açıkça ifade edilmiştir. Böylece bu karar, işverenin kendi mülkiyetindeki elektronik sistemler üzerindeki denetim hakkını güçlendirirken, çalışanların işverence sağlanan iletişim araçlarını kullandıklarında mahremiyet korumalarının önemli ölçüde sınırlandığı ilkesini yerleşik hâle getirmiştir.

interception) ile gönderim sonrası erişim *(stored communication access)* arasında teknik bir ayrım yapılmakta; mahkeme kararları genellikle işverenlerin kendi sistemlerinde saklanan e-postalara erişimini hukuka uygun kabul etmektedir[423]. ECPA'nın ikinci bölümü olan Depolanmış İletişimler Kanunu (Stored Communications Act), elektronik iletişimlerin depolandığı sistemlere yetkisiz erişimi yasaklamaktadır[424]. Federal düzeyde, izleme faaliyetlerine dair çalışanlara önceden bildirimde bulunma zorunluluğu genel bir kural değildir; bu yükümlülük yalnızca bazı eyaletlerde açıkça düzenlenmiş, bu da ABD'de eyaletler arası önemli farklılıklar yaratmaktadır. Örneğin, California Tüketici Gizliliği Kanunu (California Consumer Privacy Act – CCPA) ve California Gizlilik Hakları Kanunu (California Privacy Rights Act – CPRA)[425] kapsamında çalışanlara, işverenin veri toplama süreçlerine ilişkin bilgilendirilme, erişim, düzeltme ve silme gibi haklar tanımıştır[426]. Illinois'te yürürlükte olan Biyometrik Bilgi Gizliliği Kanunu (Illinois Biometric Information Privacy Act - BIPA), biyometrik verilerin toplanması, saklanması ve imhası için açık yazılı rıza ve şeffaf politika belgeleri şartı getirmektedir[427]. New York, Connecticut ve Delaware gibi eyaletlerde ise dijital izleme faaliyeti öncesinde çalışanlara yazılı bildirimde bulunulması zorunludur[428]. Ayrıca, California, Florida, Louisiana ve South

---

Bknz. Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (United States District Court, E.D. Pennsylvania. 23 Ocak 1996), https://law.justia.com/cases/federal/district-courts/FSupp/914/97/2131293/.

[423] "Electronic Communications Privacy Act of 1986 (ECPA)", Resmi Site, Bureau of Justice Assistance, erişim 13 Nisan 2025, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285; "Electronic Communications Privacy Act (ECPA)", EPIC - Electronic Privacy Information Center, t.y., erişim 13 Nisan 2025, https://epic.org/ecpa/; "How Much Employee Monitoring Is Too Much?", erişim 13 Nisan 2025, https://www.americanbar.org/news/abanews/publications/youraba/2018/january-2018/how-much-employee-monitoring-is-too-much-/.

[424] Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & (and) the USA Patriot Act: Surveillance Law: Reshaping the Framework", George Washington Law Review 72, sy 6 (2003): 1238.

[425] 1 Ocak 2020'de yürürlüğe giren California Tüketici Gizliliği Kanunu (California Consumer Privacy Act – CCPA) kendisini güncelleyerek kapsamını (örneğin çalışan verilerini de içerecek şekilde) genişleten California Gizlilik Hakları Kanunu'n (California Privacy Rights Act – CPRA) 1 Ocak 2023'te yürürlüğe girmesiyle daha kapsamlı bir hale gelmiştir. Bknz. Kung Feng, "Overview of New Rights for Workers under the California Consumer Privacy Act", UC Berkeley Labor Center, 06 Aralık 2023, https://laborcenter.berkeley.edu/overview-of-new-rights-for-workers-under-the-california-consumer-privacy-act/.

[426] Lothar Determann ve Jonathan Tam, "The California Privacy Rights Act of 2020: A Broad and Complex Data Processing Regulation That Applies to Businesses Worldwide", Journal of Data Protection & Privacy 4, sy 1 (2020): 7.

[427] "Complete Guide to Employee Monitoring in the US | 2024", Jibble, t.y., erişim 13 Nisan 2025, https://www.jibble.io/article/us-employee-monitoring.

[428] Employers Engaged in Electronic Monitoring; Prior Notice Required, Civil Rights Law, CHAPTER 6, ARTICLE 5, Section 52-C*2 (2021), https://www.nysenate.gov/legislation/laws/CVR/52-C*2; HR

Carolina gibi bazı eyaletlerin anayasalarında mahremiyet hakkı açıkça tanınmış olup, bu durum izleme ve gözetleme faaliyetlerinin sınırlandırılmasında anayasal düzeyde bir koruma sağlamaktadır[429].

ABD'de çalışanların dijital gözetim ve izlenmesine ilişkin hukuki çerçeve hem federal hukuk normları hem de eyalet bazında farklılaşan düzenlemeler temelinde şekillenmektedir. Bu çok düzeyli (multi-level) yapı, işverenlerin yalnızca federal) kurallara değil, aynı zamanda faaliyet gösterdikleri her bir eyaletin kendi düzenlemelerine de uyum göstermesini zorunlu kılmaktadır. Federal düzeyde kapsamlı bir "çalışan izleme" kanunu bulunmamakla birlikte, belirli konular (örneğin ECPA kapsamında elektronik iletişimin izlenmesi) düzenlenmiştir. Ancak eyaletler, anayasal düzeyde mahremiyet hakkı tanımaktan, çalışanlara dijital izleme öncesi bilgilendirme yükümlülüğü getirmeye kadar geniş yelpazede farklı hükümler öngörebilmektedir. Zira, bir işverenin farklı eyaletlerde ikamet eden çalışanları için tek tip bir gözetim politikası oluşturması, her eyaletin veri koruma, izleme bildirimi ve mahremiyet haklarına ilişkin normlarının farklılık göstermesi nedeniyle hukuki belirsizlikler yaratmaktadır. Bu durum, coğrafi olarak değişen mahremiyet standartları karşısında çalışanların dijital haklarının eşit düzeyde korunmasını engelleyebildiği gibi, işveren açısından da hukuki sorunlar doğurmaktadır.

3.4.3. Ulusal Hukuk

Türk hukukunda işverenin çalışanları izleme ve gözetleme yetkisi, birbiriyle etkileşim içinde olan ve Anayasa'dan başlayarak özel kanunlara uzanan çok katmanlı bir normatif çerçeve tarafından sınırlandırılmıştır. Bu hukuki yapı, işverenin meşru yönetim ve denetim hakları ile çalışanın temel hak ve özgürlükleri arasında hassas bir denge kurmayı hedeflemektedir. Temel hakların en üst düzeyde korunduğu Anayasa, özel hayatın gizliliği, konut dokunulmazlığı ve kişisel verilerin korunması gibi temel

---

Solutions Blog Team, "Workplace Monitoring: What's Allowed, What's Off Limits?", erişim 13 Nisan 2025, https://sbshrs.adpinfo.com/blog/workplace-monitoring-whats-allowed-whats-off-limits; Mark H. Francis ve Sophie L. Kletzien, "New York Law Requires Notice of Employees' Electronic Monitoring Effective May 7, 2022", Holland & Knight LLP, 03 Mayıs 2022, https://www.hklaw.com/en/insights/publications/2022/05/new-york-law-requires-notice-of-employees-electronic-monitoring.

[429] "Managing Workplace Monitoring and Surveillance", SHRM, 20 Haziran 2024, https://www.shrm.org/topics-tools/tools/toolkits/managing-workplace-monitoring-surveillance.

güvencelerle bu çerçevenin zeminini oluşturmaktadır. Bu anayasal temel üzerine inşa edilen Türk Medeni Kanunu, kişilik haklarının korunmasına ilişkin genel hükümleriyle, işverenin denetim faaliyetlerinin dürüstlük kuralına ve hakkın kötüye kullanılması yasağına uygun olmasını zorunlu kılmaktadır.

İş ilişkisine özgü daha somut bir sınırlama ise Türk Borçlar Kanunu'nun 419. maddesi ile getirilmiştir. Bu madde, işçiye ait kişisel verilerin ancak işe yatkınlık veya sözleşmenin ifası için zorunlu olması hâlinde işlenebileceğini hükme bağlayarak, işverenin veri işleme yetkisini belirli ve dar bir alana hapsetmektedir. Buna ek olarak İş Kanunu, bir yandan işverenin yönetim hakkını tanırken, diğer yandan işçiyi koruma ve gözetme yükümlülüğünü düzenleyerek bu dengeye katkıda bulunmaktadır. Nihayetinde, Kişisel Verilerin Korunması Kanunu, veri işleme faaliyetlerinin hangi hukuki şartlara (örneğin açık rıza, meşru menfaat) dayanması gerektiğini ve hukuka ve dürüstlük kuralına uygunluk, amaçla sınırlılık, ölçülülük gibi temel ilkelere tabi olduğunu belirterek, modern teknolojik izleme araçları karşısında en somut ve detaylı güvence mekanizmasını sunmaktadır.

Belirtilen düzenlemelerin tümü, işverenin izleme ve gözetleme uygulamalarını kullanma yetkisinin keyfi ve sınırsız olmadığını; çalışanın özel hayatının gizliliği, haberleşme hürriyeti ve kişisel verilerinin korunması gibi temel haklarına azami saygı gösterilmesi gerektiğini ortak bir şekilde vurgulamaktadır. Özellikle, iş ve özel hayat sınırlarının iç içe geçtiği tele çalışma gibi modellerde, bu hukuki dengenin çok daha hassas bir teraziyle ve çalışan lehine bir yorumla kurulması zorunluluk arz etmektedir. Takip eden alt bölümlerde, bu yasal çerçeveyi oluşturan ulusal düzenlemeler ayrıntılı olarak incelenecektir.

3.4.3.1. Anayasa

Türkiye Cumhuriyeti Anayasası, bireyin maddi ve manevi varlığını serbestçe geliştirme hakkı, insan onuru ve özel hayatın gizliliği gibi temel hakları güvence altına almaktadır. Bu anayasal güvenceler, işverenlerin çalışanlarına yönelik izleme ve

gözetleme faaliyetlerini belirli sınırlar içerisinde yürütmelerini zorunlu kılmaktadır[430]. Bu çerçevede, Anayasa'nın 20. maddesinde yer alan "özel hayatın gizliliği" ilkesi, kişilerin özel ve aile hayatlarına keyfi müdahaleyi yasaklayarak mahremiyet alanının korunmasını esas almaktadır[431]. Aynı maddenin üçüncü fıkrasında ise kişisel verilerin korunması hakkı açıkça tanınmış; bu hakkın ne şekilde kullanılacağı ve korunacağı hususlarının kanunla düzenleneceği hüküm altına alınmıştır.

Anayasa'nın 21. maddesinde düzenlenen konut dokunulmazlığı kapsamında, çalışanın evinin tele çalışma nedeniyle işyeri hâline gelmiş olması, bu hakkın ortadan kalktığı anlamına gelmemekte; işverenin fiziksel veya dijital müdahaleleri bu anayasal koruma kapsamında değerlendirilmektedir. Anayasa'nın 22. maddesinde, haberleşmenin gizliliği güvence altına alınmıştır ve bu hakka, yalnızca millî güvenlik, kamu düzeni veya suçun önlenmesi gibi istisnai hâllerde ve hâkim kararıyla sınırlı ölçüde müdahale edilebilmektedir. Öte yandan, çalışanın dini inanç ve kanaatlerini açıklamaya zorlanamaması ve düşünce ile kanaat özgürlüğü de izleme ve gözetleme faaliyetlerinin kapsamı belirlenirken göz önünde bulundurulması gereken anayasal teminatlar arasında yer almaktadır.[432].

Bu doğrultuda, işyerlerinde yürütülen izleme ve gözetleme faaliyetleri, Anayasa'nın öngördüğü temel hak ve özgürlükler çerçevesinde değerlendirilmelidir[433]. İşverenlerin bu tür uygulamalarda bulunurken, ölçülülük ilkesine uygun ve temel haklara saygılı hareket etmeleri anayasal bir zorunluluktur. Bu anayasal yükümlülükler, çalışanların yalnızca fiziksel değil, aynı zamanda Anayasa'nın güvence altına aldığı kişilik hakkı ve manevi bütünlük kapsamında, kişinin düşünsel ve duygusal alanının da korunmasını gerekli kılmaktadır. Tele çalışma modelinde, çalışanın sürekli bir dijital gözetim altında olması, performansına ilişkin anlık ve yoğun geri bildirim beklentisi

---

[430] Savaş, "İş Hukukunda 'Siber Gözetim'", 128; Tekergül, "İşyerinde Elektronik Gözetim Uygulamaları", 53-55; Savran, "İşçinin İşyerinde Elektronik Yöntemlerle İzlenmesi", 28-31.

[431] Ayrıntılı bilgi için bkz. Gülay Aslan Öncü *Özel Yaşamın Korunması Hakkı* (İstanbul: Beta Basım Yayın, Mart 2011).

[432] Tekergül, "İşyerinde Elektronik Gözetim Uygulamaları", 55; Ali Korkmaz, "İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması", *Karamanoğlu Mehmetbey Üniversitesi Sosyal Ve Ekonomik Araştırmalar Dergisi* 2014, sy 3 (2014): 102; Şermin Birtane, "Özel Hayata Saygı Hakkı (AİHS 8. Madde) Bağlamında Çalışma Hakkı ve Mesleki Hayat İlişkisi", *Anayasa Yargısı* 38, sy 2 (2021): 69.

[433] Korkmaz, "İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması", 102; Birtane, "Özel Hayata Saygı Hakkı (AİHS 8. Madde) Bağlamında Çalışma Hakkı ve Mesleki Hayat İlişkisi", 60 vd.

veya iş ve özel hayat arasındaki sınırların belirsizleşmesi, bireyin kendini özgürce ifade etme, hata yapma veya sadece ulaşılabilir olmama hakkını kısıtlayarak Anayasa ile korunan kişilik haklarını ve manevi bütünlüğünü zedeleyebilir. Anayasal güvenceler, işverenin bu tür bir psikolojik baskı veya müdahaleci denetimden kaçınmasını da gerektirmektedir.

3.4.3.2. Türk Medeni Kanunu

Türk Medeni Kanunu'nun 2. maddesinde düzenlenen dürüstlük kuralı ve hakkın kötüye kullanılması yasağı, izleme faaliyetlerinin değerlendirilmesinde de temel ölçütleri oluşturmaktadır. Dürüstlük kuralı, tarafların hukuki ilişkilerinde adil, samimi ve doğru bir tutum sergilemelerini gerektirmektedir. Sözleşme ilişkileri açısından bu kural, tarafların sahip oldukları yetkileri kullanırken makûl, ölçülü ve sözleşmenin amacına uygun hareket etmelerini zorunlu kılmaktadır. Bu bağlamda dürüstlük kuralı, işverenlerin çalışanları izleme faaliyetlerinde, çalışanların haklarını gereksiz yere zedeleyici, aşırı ve ölçüsüz yöntemlerden kaçınmalarını zorunlu hâle getirmektedir[434]. Aksi hâlde, dürüstlük kuralının ihlali söz konusu olacaktır. Hakkın kötüye kullanılması yasağı ise hukukun tanıdığı bir hakkın, yalnızca başkasına zarar verme niyetiyle veya amacından saptırılarak kullanılması durumunda bu kullanımın hukuken korunmayacağını ifade etmektedir. İşçinin iş görme edimini işverenin emir ve talimatları altında yerine getirmesi, bu ilişkide işçinin kişiliğine ve özel hayatına müdahale riskini artırmaktadır[435]. İzleme ve gözetleme faaliyetleri açısından değerlendirildiğinde, hukuki bir dayanağı bulunmayan, amacı meşru olmayan veya çalışanlara ölçüsüz müdahalede bulunan uygulamalar, hakkın kötüye kullanımı kapsamında hukuka aykırı sayılacaktır[436].

---

[434] Mustafa Dural ve Tufan Öğüz, *Türk Özel Hukuku Cilt II Kişiler Hukuku*, 24. Baskı (Filiz Kitabevi, 2024), 99 vd.; Jale Akipek vd., *Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku*, 16. (Beta Basım Yayım Dağıtım Yayınları, 2020), 165; Pınar Arıoğlu, "İşverenin Yönetim Hakkının Kötüye KulIanılması" (Doktora Tezi, Çukurova Üniversitesi, 2024), 68 vd.

[435] Ertürk, İş İlişkisinde Temel Haklar, 89; K. Ahmet Sevimli, "İşçinin Özel Yaşam Hakkı Bağlamında İşçi İşveren İlişkisi", Sicil İş Hukuku Dergisi, sy 10 (2008): 53 vd.; Ali Güzel ve Deniz Ugan Çatalkaya, "İş Sözleşmesinin Uygulanmasında ve İşverenin Yönetim Yetkisinin Sınırlanmasında Dürüstlük (Objektif İyiniyet) Kuralının İşlevi Üzerine", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 20, sy 1 (2014): 57 vd., 1.

[436] Güzel ve Çatalkaya, "İş Sözleşmesinin Uygulanmasında ve İşverenin Yönetim Yetkisinin Sınırlanmasında Dürüstlük (Objektif İyiniyet) Kuralının İşlevi Üzerine", 63 vd.

Türk Medeni Kanunu, kişilik haklarını korumaya yönelik kapsamlı hükümler içermekte olup, izleme ve gözetleme uygulamalarının hukuki sınırlarının belirlenmesinde temel dayanağı oluşturmaktadır. TMK'nın 23. maddesi, kişilik hakkının doğuştan kazanılan, devredilemeyen ve vazgeçilemeyen nitelikte olduğunu; hiç kimsenin hak ve özgürlüklerinden tümüyle yoksun bırakılamayacağını açıkça ifade etmektedir[437]. İşçinin kişiliğinin korunması; yaşamı, sağlığı, bedensel ve ruhsal bütünlüğü, şeref ve haysiyeti (onuru), kişisel ve mesleki saygınlığı, özel hayat alanı ve genel olarak özgürlüğünün korunmasını içermektedir[438].

Türk Medeni Kanunu'nun 24. maddesi, kişilik haklarına yönelik hukuka aykırı saldırılara karşı korunmanın esasını oluşturmaktadır. Bu madde uyarınca, hukuka aykırı olarak kişilik hakkına saldırılan birey, saldırının durdurulması, önlenmesi ve saldırının hukuka aykırılığının tespiti için mahkemeye başvurabilmektedir. Ayrıca, Yargıtay içtihatları ve öğretide yapılan kişilik hakları geniş yorumlanarak özel hayatın gizliliğine yönelik ihlaller de bu kapsamda olarak değerlendirilmektedir. Ancak, TMK'nın 24. maddesinin ikinci fıkrası, kişilik hakkına müdahale oluşturan her eylemin mutlak surette hukuka aykırı sayılmayacağını, belirli koşulların varlığı hâlinde bu müdahalenin meşruiyet kazanabileceğini düzenlemektedir. Bu istisnalar; müdahale edilen kişinin açık rızasının bulunması, müdahaleyi haklı kılan daha üstün nitelikte özel veya kamusal bir yararın varlığı ya da kanun tarafından işverene tanınmış bir yetkinin kullanılmasıdır[439]. Bu koşullardan birinin somut olayda gerçekleşmesi durumunda, işverenin gerçekleştirdiği izleme ve gözetleme faaliyetleri hukuka uygun kabul edilecektir[440].

İşçinin belirli bir duruma özgü, açık ve bilgilendirilmiş bir rızası bulunsa dahi, bu rızanın kapsamı önem taşır. Sözleşmenin zayıf tarafı olan işçinin kişilik hakkına

---

[437] Mustafa Dural ve Tufan Öğüz, *Türk Özel Hukuku Cilt II Kişiler Hukuku*, 99-100; Beste Gemici Filiz, "Türk İş Hukuku'nda İş Sözleşmesinin Geçersizliği" (Doktora Tezi, İstanbul Kültür Üniversitesi, 2024), 61 vd.

[438] Sarper Süzek, "Yeni Türk Borçlar Kanunu Çerçevesinde İş Akdinin Geçersizliği", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi / Prof.Prof. Dr. Ali Rıza Okur'a Armağan 20, sy 1 (2014): 134, 1.

[439] Mustafa Dural ve Tufan Öğüz, *Türk Özel Hukuku Cilt II Kişiler Hukuku*, 152-68.

[440] Güzel ve Çatalkaya, "İş Sözleşmesinin Uygulanmasında ve İşverenin Yönetim Yetkisinin Sınırlanmasında Dürüstlük (Objektif İyiniyet) Kuralının İşlevi Üzerine", 61.

müdahale teşkil eden bir uygulamaya gösterdiği rızaya kuşkuyla yaklaşılmalıdır[441]. Eğer verilen rıza, gelecekte doğabilecek her türlü müdahaleyi kapsayacak kadar geniş tutulmuşsa, bu durum dürüstlük kuralına (TMK m. 2) aykırılık teşkil edebilir. Bu tür "feragat anlamına gelecek kadar geniş" rızaların, rızayı veren kişinin haklarını aşırı derecede kısıtlaması nedeniyle geçersiz olabileceğini kabul edilmektedir. Bu durumda, rızanın tamamının geçersiz sayılması yerine, dürüstlük kuralına aykırı olan ve feragat niteliği taşıyan kısımlarının "kısmi geçersizlik" veya "indirgemeci yorum" yoluyla kapsamının daraltılması gündeme gelecektir[442]. Örneğin, işçinin "tüm kişisel verilerinin işlenmesine" yönelik genel rızası, iş ilişkisiyle sınırlı ve ölçülü amaçlar için geçerli sayılırken, bu amaçları aşan kısımlar için geçersiz kabul edilecektir.

Son olarak, kişilik hakkı ihlal edilen kişinin başvurabileceği hukuki yollar ise TMK'nın 25. maddesinde düzenlenmektedir. Buna göre kişi, uğradığı saldırının durdurulmasını, önlenmesini veya hukuka aykırılığının tespit edilmesini mahkemeden talep edebilir. Aynı madde, kişilik hakkı ihlal edilen kişiye maddi veya manevi tazminat isteme hakkını tanımaktadır. Özellikle manevi tazminat, kişinin manevi bütünlüğüne yönelik ihlallerin giderilmesi bakımından önem taşımakta ve mahkemece her somut olayın özelliğine göre değerlendirilerek hükme bağlanmaktadır.

3.4.3.3. Türk Borçlar Kanunu

Türk Borçlar Kanunu'nun 27. maddesi uyarınca, kanunun emredici hükümlerine, ahlaka, kamu düzenine veya kişilik haklarına aykırı sözleşmeler veya sözleşme şartları, en başından itibaren kesin olarak hükümsüz sayılmaktadır. TBK 27. maddenin ikinci fıkrası gereğince, kural olarak sadece hukuka aykırı olan bu hükümler geçersiz kabul edilmekte ve sözleşmenin geri kalanı geçerliliğini korumaktadır. Ancak, tarafların bu geçersiz hükümler olmasaydı sözleşmeyi hiç yapmayacaklarının anlaşılması durumunda, istisnai olarak sözleşmenin tamamı geçersiz hâle gelmektedir[443]. Örneğin, bir iş sözleşmesindeki çalışanın özel hayatını ihlal eden

---

[441] Güzel ve Çatalkaya, "İş Sözleşmesinin Uygulanmasında ve İşverenin Yönetim Yetkisinin Sınırlanmasında Dürüstlük (Objektif İyiniyet) Kuralının İşlevi Üzerine", 61.
[442] Süzek, "Yeni Türk Borçlar Kanunu Çerçevesinde İşçinin Rekabet Etmeme Borcu", 140 vd.; Arıoğlu, "İşverenin Yönetim Hakkının Kötüye Kullanılması", 351-52.
[443] Süzek, "Yeni Türk Borçlar Kanunu Çerçevesinde İşçinin Rekabet Etmeme Borcu", 131 vd.; Arıoğlu, "İşverenin Yönetim Hakkının Kötüye Kullanılması", 58.

izleme ve gözetlemeye ilişkin bir madde kendi başına hükümsüz sayılmakta; fakat bu durum genellikle sözleşmenin tamamını etkilememekte ve iş ilişkisi o madde olmaksızın devam etmektedir.

Bu genel hükümsüzlük ilkesinin iş hukuku alanındaki en belirgin yansımalarından biri, çalışanların kişisel verilerinin korunması noktasında kendini göstermektedir. İş hukukunda çalışanların kişisel verilerinin korunması, Türk Borçlar Kanunu'nun 419. maddesi ile temel bir güvenceye kavuşturulmuştur. Bu madde, işverenin veri işleme yetkisine son derece önemli bir sınırlama getirerek, işçiye ait kişisel verilerin ancak iki koşulun varlığı hâlinde işlenebileceğini hükme bağlamaktadır: verinin, işçinin işe yatkınlığıyla ilgili olması veya hizmet sözleşmesinin ifası için zorunlu olması. Maddenin lafzındaki "kullanabilir" ifadesi, veri koruma hukukunun bütüncül yaklaşımı gereği, verinin toplanmasından silinmesine kadar tüm süreci kapsayan "işleyebilir" şeklinde geniş yorumlanması gerekmektedir[444].

Türk Borçlar Kanunu 419. maddesinin konumu, Kişisel Verilerin Korunması Kanunu karşısında ayrıca değerlendirilmelidir. Türk Borçlar Kanunu genel bir kanun olmakla birlikte, 419. maddesi, yalnızca iş ilişkisindeki veri işlemeyi düzenlemesi sebebiyle, veri korumanın genel kanunu olan KVKK karşısında özel hüküm niteliği taşımaktadır. Bu durum, işverenin veri işleme faaliyetinin çifte bir denetime tabi olduğu anlamına gelmektedir. İşveren, öncelikle TBK 419. maddedeki bu iki özel ve sınırlayıcı koşuldan birini karşılamakla yükümlüdür. Bu ilk ve daha dar olan süzgeç geçildikten sonra, gerçekleştirilecek veri işleme faaliyeti, aynı zamanda KVKK'nın 4. maddesinde sayılan hukuka ve dürüstlük kuralına uygun olma, ölçülülük, amaçla bağlantılı ve sınırlı olma gibi genel ilkelere de tam uyum göstermekle yükümlüdür[445].

Bu hukuki çerçevenin en titiz uygulanması gereken alanlardan biri de tele çalışmadır. İşin, çalışanın özel hayat alanında yürütüldüğü bu modelde, işverenin topladığı her

---

[444] K. Ahmet Sevimli, "Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419", *Sicil İş Hukuku Dergisi, Yıl* 4, sy 24 (2011): 134-35; Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 35 vd.; Güzel ve Çatalkaya, "İş Sözleşmesinin Uygulanmasında ve İşverenin Yönetim Yetkisinin Sınırlanmasında Dürüstlük (Objektif İyiniyet) Kuralının İşlevi Üzerine", 58-59.

[445] Sevimli, "Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419", 134-35; Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 35 vd.

türlü verinin, TBK madde 419'un aradığı "doğrudan bağlantılı olma" ve "zorunluluk" kriterlerini istisnasız bir şekilde karşılaması gerekmektedir. Örneğin, bir tele çalışanın verimliliğini ölçmek amacıyla evdeki çalışma ortamının sürekli kamera ile izlenmesi, özel olabilecek yazışmalarının içeriğine doğrudan erişilmesi veya dijital hareketlerinin işin gerekliliğini aşan ölçüde takip edilmesi, TBK madde 419'un bu sıkı testini geçemeyeceği için hukuka aykırı kabul edilecektir. Dolayısıyla, işçinin rızası alınsa dahi, işe yatkınlık veya sözleşmenin ifası ile doğrudan ilişkilendirilemeyen bir veri işleme faaliyeti, bu özel hüküm karşısında hukuka uygunluk kazanamayacaktır[446].

Kişilik haklarına, kişinin özel alanına yapılan müdahaleler kural olarak hukuka aykırı sayıldığından, geçerli bir şekilde kararlaştırılmayan izleme ve gözetleme faaliyetleri, TBK'nın 49. maddesi uyarınca haksız fiil sorumluluğunu doğuracaktır[447]. Anılan maddeye göre, hukuka aykırı ve kusurlu bir davranışla başkasına zarar veren kişi, meydana gelen zararı gidermekle yükümlüdür. Bu kapsamda, çalışanların özel hayatına müdahale teşkil eden, hukuka aykırı izleme faaliyetleri nedeniyle maddi veya manevi zarara uğrayan çalışan, haksız fiil hükümleri çerçevesinde işverenden tazminat talep edebilmektedir. Haksız fiil sorumluluğunun doğması için izleme faaliyetinin hukuka aykırı olması, kusurun bulunması, bir zararın ortaya çıkması ve izleme faaliyeti ile bu zarar arasında uygun illiyet bağının mevcut olması gerekmektedir. Böylece TBK, izleme faaliyetlerinde hukuki sorumluluk bakımından önemli bir güvence mekanizması sağlamaktadır.

3.4.3.4. Kişisel Verilerin Korunması Kanunu

İşverenler; iş ilişkisi kapsamında güvenlik, verimlilik ve yasal yükümlülüklerin yerine getirilmesi gibi amaçlarla başvurdukları izleme ve gözetleme faaliyetleriyle, esasen bir veri işleme faaliyeti yürütmektedir[448]. Çalışanların temel hak ve özgürlüklerini doğrudan etkileyen bu uygulamalar, bu sebeple Kişisel Verilerin Korunması Kanunu

[446] Sevimli, "Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419", 135; Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 81 vd.
[447] Fikret Eren, Borçlar Hukuku Genel Hükümler, 28. bs (Legem Yayınevi, 2023), 567; Şaban Kayıhan ve Mustafa Ünlütepe, Borçlar Hukuku Genel Hükümler (Seçkin Yayıncılık, 2018), 226.
[448] Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 19.

kapsamında ele alınmaktadır. Söz konusu Kanun, Anayasa'nın 20. maddesinde güvence altına alınan kişisel verilerin korunması hakkının temel yasal çerçevesini oluşturmakta ve bu doğrultuda kişisel veri işleme faaliyetini kural olarak bir istisnaya bağlamaktadır. Bu temel yaklaşım, veri işlemenin "izne bağlı yasak" olduğu ilkesine dayanmaktadır.

KVKK'nın 4. maddesi, tüm veri işleme faaliyetlerinin uymak zorunda olduğu temel ilkeleri belirlemiştir. Bu ilkeler; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma (veri minimizasyonu) ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmedir. İşverenin izleme ve gözetleme faaliyetleri, bu ilkelerin tamamına eksiksiz bir şekilde uymak zorundadır[449].

Söz konusu ilkelere ek olarak Kanun, kişisel verilerin işlenmesini belirli hukuka uygunluk sebeplerine dayandırmıştır. Kanun'un 5. maddesi uyarınca temel kural, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenememesidir[450]. Ancak, kanunlarda açıkça öngörülmesi, bir sözleşmenin kurulması veya ifasıyla doğrudan ilgili olması, veri sorumlusunun hukuki bir yükümlülüğü yerine getirmesi için zorunlu olması veya ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlemenin zorunlu olması gibi durumlarda açık rıza aranmaksızın veri işlenmesi mümkündür. Kanun'un 6. maddesi ise kişilerin ırkı, etnik kökeni, siyasi düşüncesi, sağlığı ve cinsel hayatı gibi özel nitelikli kişisel verilerin işlenmesini daha katı koşullara bağlamıştır.

İş ilişkilerinde Kişisel Verilerin Korunması Kanunun uygulanması işçi ve işveren ilişkisinin kapsamı bağlamında çeşitli zorluklar yaşanabilmektedir. Örneğin, iş ilişkisinin doğasındaki güç dengesizliği, işçinin işini kaybetme endişesiyle baskı altında açık rıza ile kişisel verilerin işlenmesine onay verebileceği gerçeği, bu rızanın özgür iradeye dayanıp dayanmadığı konusunda ciddi şüpheler doğurmaktadır. Bu nedenle, özellikle iş ilişkilerinde açık rızaya ancak diğer hukuka uygunluk şartlarının

[449] Ayrıntılı bilgi için bknz. Bölüm 4.3.
[450] Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 56 vd.

bulunmadığı istisnai durumlarda ve sınırlı olarak başvurulması gerektiği kabul edilmektedir[451]. Diğer bir örnek ise iş ilişkilerinde izleme ve gözetleme faaliyetleri kapsamında başvurulabilecek hukuka uygunluk sebeplerinden biri olan meşru menfaattir. İşverenin menfaatleri ile çalışanın temel hak ve özgürlükleri arasında hassas bir denge testi yapılmasını zorunlu kılmaktadır. İşverenin verimliliği artırma, mülkiyetini koruma veya iş süreçlerini denetleme gibi menfaatleri meşru kabul edilebilse de bu menfaatlerin çalışanın temel haklarına ölçüsüz bir müdahalede bulunmaması esastır.

Tele çalışma özelinde bu denge daha da hassaslaşmaktadır; zira işverenin işin yürütümü, veri güvenliği veya verimlilik gibi meşru menfaatleri ile çalışanın kendi konutundaki mahremiyet beklentisi ve özel hayatının gizliliği hakkı arasında çok daha dikkatli bir sınır çizilmesi gerekmektedir. Örneğin, bir tele çalışanın tüm gün boyunca web kamerasının açık tutulması veya klavye hareketlerinin kaydedilmesi gibi müdahaleci uygulamaların, meşru menfaat gerekçesiyle kolaylıkla haklılaştırılamayacağı kabul edilmelidir. Zira bu tür sürekli bir gözetim, işçi üzerinde baskı ve stres yaratabileceği gibi hem kişilik haklarına ağır bir müdahale teşkil eder hem de KVKK'nın 4. maddesinde sayılan ilkelere açıkça aykırılık teşkil edecektir[452].

Bu temel açıklamaların ardından, çalışmamızın ilerleyen bölümlerinde işçinin kişisel verilerinin korunmasına ilişkin hukuki rejim tele çalışmada izleme ve gözetleme uygulamalarının kullanılmasına ilişkin daha detaylı bir biçimde ele alınacaktır.

3.4.3.5 7545 Sayılı Siber Güvenlik Kanunu

Günümüzde siber güvenlik risklerinin yalnızca kamu kurumlarını değil, özel sektör kuruluşlarını da doğrudan tehdit etmesi, ilgili düzenlemelerin kapsamını genişletmiş ve işverenler açısından yeni sorumluluk ve yetki alanları doğurmuştur. Bu çerçevede, her ne kadar Siber Güvenlik Kanunu'nun[453] temel amacı kamu kurumlarını ve ulusal güvenliği siber tehditlere karşı korumak olsa da kanunun kapsamı özel sektör

[451] Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 55 vd.
[452] Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 81 vd.
[453] 7545 Sayılı Siber Güvenlik Kanunu, R.G. 19.3.2025, Sayı: 32846

kuruluşlarını da içine alacak şekilde genişletilmiştir. Bu durum, özellikle hassas ya da kritik nitelikteki verilerle çalışan şirketler bakımından, işverenlere siber saldırılara karşı önleyici tedbirler alma, kurumsal bilgi sistemlerinin güvenliğini sağlama ve bu doğrultuda çalışanların kullandığı özellikle işveren tarafından temin edilen dijital cihazlar üzerinde teknik denetimler gerçekleştirme yönünde genel bir yetki alanı sunabilmektedir. Söz konusu yetki, çalışanların kurum ağına uzaktan erişim sağladığı tele çalışma modellerinde artan siber güvenlik riskleri göz önüne alındığında, işverenler açısından daha da büyük önem arz etmektedir.

Bununla birlikte, bu yetkinin kullanımı mutlak veya sınırsız değildir. Kişisel Verilerin Korunması Kanunu'nun öngördüğü temel ilkeler, Siber Güvenlik Kanunu'ndan kaynaklanan her türlü izleme ve denetim faaliyetinde de titizlikle gözetilmelidir. Bu bağlamda, siber güvenlik gerekçesi, tek başına işverenin çalışan üzerindeki izleme yetkisini sınırsız biçimde meşrulaştırmaz; ancak izleme faaliyetlerinin belirli bir tehdide dayalı, açık şekilde tanımlanmış, şeffaf biçimde yürütülen ve yalnızca gerekli olanla sınırlı kaldığı ölçüde hukuken kabul edilebilir nitelik kazanabilir. Aksi hâlde, keyfî, genel geçer veya aşırı müdahaleci nitelikteki izleme uygulamaları, siber güvenlik gerekçesi ileri sürülse dahi hukuka aykırı kabul edilecektir.

BÖLÜM IV

TELE ÇALIŞMA SÜRECİNDE İZLEME ARAÇLARININ VERİ KORUMA HUKUKU AÇISINDAN ANALİZİ

4.1. Kişisel Veri Kavramı

Kişisel veri kavramı, Kişisel Verilerin Korunması Kanunu 3. maddesinin 1. fıkrasının (d) bendi, yürürlükten kaldırılan 95/46/EC sayılı Veri Koruma Direktifi'nin 2. maddesinin 1. fıkrasının (a) bendi hükmünden doğrudan çevrilerek, *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* şeklinde tanımlanmıştır. 2018 yılında yürürlüğe giren Genel Veri Koruma Tüzüğü 4. maddesinin 1. fıkrası ise aynı temel tanımı benimsemekle birlikte, bu tanımı önemli ölçüde genişletmiştir. Bu bağlamda Tüzük, "kimliği belirlenebilir gerçek kişi" tanımını, kimlik numarası, konum verileri, çevrim içi tanımlayıcılar gibi unsurları da içerecek şekilde somutlaştırmış; bu ifadenin kişinin fiziksel, fizyolojik, genetik, psikolojik, ekonomik, kültürel ya da toplumsal kimliğine özgü bir veya birden fazla niteliğe atıfla da anlaşılabileceğini açıklığa kavuşturmuştur[454]. Bununla birlikte, GDPR'ın 4. maddesinin 1. fıkrasında yer alan ayrıntılı tanımlayıcı unsurlar, özellikle "belirlenebilirlik" kriterinin kapsamını daha somut ve sistematik bir biçimde açıklığa kavuşturmaktadır[455].

---

[454] Oğuz Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması (Beta, 2008), 122; Aydın Akgül, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması (Beta Basım Yayım Dağıtım Yayınları, 2014), 17; Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", n. 15.

[455] 95/46/EC sayılı Veri Koruma Direktifi, "belirlenmiş veya belirlenebilir kişi"yi; bir kimlik numarası ya da kişiye özgü fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal özellikler aracılığıyla kimliği doğrudan veya dolaylı olarak saptanabilen kişi olarak tanımlamıştır. GDPR ise bu tanımı daha da ayrıntılı hale getirerek çevrim içi tanımlayıcılar (online identifiers) ve genetik veriler gibi yeni kategorileri de kapsama almış, böylece güncel teknolojik gelişmelere ve veri işleme yöntemlerine uygun, daha kapsamlı bir düzenleme sunmuştur. Ayrıntılı bilgi için bknz. Osman Gazi Güçlütürk, Yapay Zeka ve Verinin Kullanımı, 1. Baskı (On İki Levha Yayıncılık, 2020), 270-71.

KVKK'da bu ek açıklama açıkça yer almamakla birlikte, "kişisel veri" ve "kimliği belirlenebilir kişi" tanımlarına ilişkin paralel düzenlemeler, madde gerekçesinde ve Kurum rehberinde yer almaktadır[456]. GDPR, kişisel verilerin yalnızca geleneksel tanımlayıcılarla (isim, kimlik numarası vb.) sınırlı olmadığını; bireyleri dijital ortamda tanımlanabilir kılan çevrim içi tanımlayıcıları da kapsadığını Başlangıç bölümünün 30. maddesinde açıkça belirtilmiştir. IP adresleri, çerez kimlikleri ve benzeri dijital izler bu kapsamda değerlendirilmektedir[457]. Nitekim bu esnek yorum, KVKK'da yer alan "her türlü bilgi" ifadesinin de benzer bir esneklikle yorumlanması gerektiğine işaret etmektedir. Bu kapsamda, tele çalışma modelinde işverenlerin çalışanlarını dijital araçlarla izlemesi ve gözetlemesi sonucu elde edilen verilerin (örneğin, bilgisayar kullanım günlükleri, e-posta meta verileri, video konferans kayıtları, performans analizi yazılımlarından elde edilen veriler) büyük bir kısmının kişisel veri olarak kabul edilmesi ve veri koruma mevzuatı kapsamında korunması gerektiği anlamına gelmektedir[458].

Sonuç olarak, bir bilginin kişisel veri sayılabilmesi için temelde şu şartların bir arada bulunması gerekmektedir: Ortada bir bilgi (veri) olmalı, bu bilgi bir gerçek kişiye ilişkin olmalı ve bilginin ait olduğu gerçek kişinin kimliği belirli veya belirlenebilir olmalıdır. Bu unsurlar, bir verinin kişisel veri niteliği taşıyıp taşımadığının tespitinde temel ölçüt olarak kabul edilmelidir[459].

---

[456] Kişisel Verileri Koruma Kurumu, Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü, no. 68 (Kişisel Verileri Koruma Kurumu, 2025), Ayrıntılı bilgi için bknz.

[457] Lukas Feiler vd., The EU General Data Protection Regulation (GDPR): A Commentary (Globe Law And Business, 2021), 58.

[458] *"Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Bu bağlamda yalnızca bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle o kişinin tanımlanabilir hâle getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden bir içerik taşıması ya da kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm hâlleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kaydı, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılma özelliği nedeniyle kişisel verilerdir." Bknz. Kişisel Verileri Koruma Kurumu, Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü, 10.*

[459] Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 21-22; Murat Volkan Dülger, Kişisel Verilerin Korunması Hukuku, 2. Baskı (FA Hukuk Akademisi, 2019), 86-101; Miray Özer Deniz, "Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk" (Doktora Tezi, Çukurova Üniversitesi, 2022), 44.

4.1.1. Bilgi Unsuru

Kişisel veri tanımının ilk ve en geniş unsurunu, Kişisel Verilerin Korunması Kanunu'nda geçen "her türlü bilgi" ifadesi oluşturmaktadır. Bu ifadenin genişliği, veri koruma hukukunun kapsamını belirlemede temel bir rol oynamaktadır. Bir kavram olarak "veri", olgu veya komutların iletişim ve işleme uygun biçimsel bir gösterimi olarak tanımlanırken; bu ham bilginin analiz edilip işlenmesiyle elde edilen anlamlı bütüne "bilgi" denilmektedir[460]. Bununla birlikte, öğretide kişisel verilerin korunması açısından daha kapsayıcı bir yaklaşım benimsenerek, "veri", "enformasyon" ve "bilgi" kavramları arasında bir ayrım yapılmamasının daha isabetli olduğu da savunulmaktadır[461].

"Her türlü bilgi" ifadesi, verinin niteliği ve formatından bağımsız bir koruma alanı yaratmaktadır. Bilginin gizli olup olmaması, nesnel (örneğin sosyal güvenlik numarası) veya öznel (örneğin psikolojik durum) nitelik taşıması, hatta hatalı veya eksik olması dahi onun kişisel veri olma niteliğini ortadan kaldırmamaktadır. Korumanın kapsamı, bilginin bulunduğu formatı da dışlamaz; yazılı, sesli veya görüntülü veriler, kâğıt üzerindeki kayıtlar, elektronik ortamdaki bilgiler ve hatta insan dokusundan alınan hücre numuneleri dahi kişisel veri olarak kabul edilmektedir[462].

4.1.2. Gerçek Kişi Unsuru

KVKK'nın 3. maddesi uyarınca, sadece gerçek kişilerin kişisel verilerinin korunması esastır. GDPR 4. maddesinin 1. fıkrası ise veri öznesi olarak gerçek kişiyi hedef almış ve tüzel kişilere uygulanmayacağını Başlangıç bölümü 14. maddesinde açıkça belirtmiştir[463]. Bununla birlikte, tüzel kişilere yönelik veri işleme faaliyetlerinin, çoğu

---

[460] Akgül, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, 11; Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 21-22.

[461] Elif Küzeci, *Kişisel Verilerin Korunması Hukuku*, 4. (On İki Levha Yayıncılık, 2021), 12; Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", n. 12.

[462] Manav, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", 98; Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 22.

[463] Ölmüş kişilere ilişkin Madde 29 Çalışma Grubunun görüşü ve GDPR'daki düzenleme için bknz. Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 111-12. Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, 273.

zaman o tüzel kişiyle ilişkili gerçek kişilere (örneğin, çalışanlar, yöneticiler, iletişim noktaları) ait bilgileri de içerebileceği ve bu bilgilerin o gerçek kişiler açısından kişisel veri niteliği taşıyacağı unutulmamalıdır[464]. Başlangıç bölümü 14. maddesinde bu ayrımı netleştirirken, üye Devletlere ulusal hukuklarında tüzel kişilere veri koruma sağlamaları konusunda bir serbesti tanıdığını da belirtmektedir; bu durum, AB içinde dahi farklı uygulamaların olabileceğine işaret ederken, KVKK'nın bu konuda daha dar bir yorum benimsediği ve korumayı kesin olarak gerçek kişilerle sınırladığı görülmektedir[465]. Nitekim İtalya, Avusturya, Danimarka ve Lüksemburg gibi bazı AB üyesi devletler, kabul ettikleri ulusal veri koruma mevzuatlarında yer alan güvenlik tedbirleri gibi belirli hükümleri, tüzel kişilere ilişkin veri işleme faaliyetlerini kapsayacak şekilde genişletmiştir[466].

4.1.3. Belirli veya Belirlenebilir Olma Unsuru

Kişisel verilerin korunmasına ilişkin mevzuatın uygulanabilmesi için öncelikle bir bilginin kişisel veri niteliğini taşıması, başka bir deyişle belirli ya da belirlenebilir bir kişiyle ilişkilendirilebilir olması gerekmektedir. Bir kişiye ait olduğu açıkça anlaşılan bilgiler (örneğin, bir kişinin adı ve soyadı bir arada kullanıldığında) doğrudan kişisel veri olarak kabul edilmektedir [467]. Buna karşılık bir kişinin "belirlenebilir olması" kavramı, söz konusu kişinin kimliğinin doğrudan ya da dolaylı yollarla tespit edilebilmesini ifade etmektedir. Bu tespit, kişinin yalnızca adı gibi temel kimlik unsurlarıyla yapılabileceği gibi; kimlik numarası, fiziksel özellikler, ekonomik durum

---

[464] Örneğin, tele çalışma bağlamında, bir şirketin (tüzel kişi) namına hareket eden ve uzaktan çalışan bir temsilcisinin (gerçek kişi) veya bir danışmanlık şirketine (tüzel kişi) bağlı olarak proje bazlı tele çalışan bir uzmanın (gerçek kişi) e-posta yazışmaları, video konferans kayıtları veya performans verilerinin işveren veya hizmet alan şirket tarafından izlenmesi durumunda, bu veriler tüzel kişinin faaliyetleriyle ilgili olsa dahi, ilgili gerçek kişilerin kişisel verisi olarak korunacaktır. Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 112; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 363; Dülger, *Kişisel Verilerin Korunması Hukuku*, 172; Güçlütürk, *Yapay Zeka ve Verinin Kullanımı*, 273.

[465] Özer Deniz, "Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk", 44; KVKK, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*, no. 58 (2025), 48, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf.

[466] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 113.

[467] Elif Küzeci ve Şebnem Kılıç, "6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler", *Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi* 16, sy 63 (2019): 956; Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 111-15; Dülger, *Kişisel Verilerin Korunması Hukuku*, 91-101; Süleyman Yılmaz ve Gökçe Çavuşoğlu, *Kişisel Verileri Koruma Hukuku* (Yetkin Yayınları, 2020), 40; Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 3. Baskı (On İki Levha Yayıncılık, 2020), 45-49.

bilgileri, genetik veriler ya da kültürel ve sosyal özellikler gibi birden fazla faktörün bir araya getirilmesiyle de mümkün olabilir[468]. Örneğin, bir tele çalışanın, işverenin sağladığı yazılım tarafından kaydedilen klavye vuruş hızı dahi, onun üretkenliği veya stresi hakkında bilgi vererek kimliğini belirlenebilir kıldığı anda kişisel veri hâline gelir. GDPR Başlangıç bölümü 26. maddesinde kimliği belirlenebilir kişi tanımlanırken, yalnızca veri sorumlusunun değil, herhangi bir üçüncü kişinin de doğrudan ya da dolaylı olarak kimliği tespit edebileceği gerçek kişilerden söz edilmektedir[469]. Bu çerçevede, bir kişinin tanımlanabilir olup olmadığının değerlendirilmesinde, "makûl ölçüde kullanılması muhtemel olan tüm araçların" dikkate alınması gerektiği vurgulanmaktadır.

Bir bilginin kişisel veri olarak değerlendirilebilmesi için ilgili kişiyi açıkça tanımlayabilmesi veya tanımlanabilir hâle getirmesi gerekmektedir. Dolayısıyla, verinin sadece genel veya klasik tanımlayıcı unsurlar içermesi tek başına yeterli değildir[470]. Bu nedenle, bir verinin kişisel veri olup olmadığının tespiti, yalnızca içerdiği tanımlayıcıların türüne bakılarak değil, her durumda somut olayın özellikleri dikkate alınarak yapılmalıdır[471]. Bu değerlendirmede temel kriter, bilginin kişiyi belirli veya belirlenebilir kılıp kılmadığının incelenmesi olmaktadır[472].

---

[468] Örneğin, tele çalışma modelinde, işverenlerin kullandığı çeşitli izleme ve gözetleme araçları, çalışanı belirlenebilir kılan çok sayıda dijital iz ve veri üretmektedir. Örneğin, bir tele çalışanın ev ağından kullandığı kurumsal VPN bağlantısının IP adresi, iş için kullandığı bilgisayardaki uygulama kullanım günlükleri, klavye vuruş sıklığı veya fare hareketleri gibi performans metrikleri, video konferanslar sırasında elde edilen ses ve görüntü kayıtları (ki bunlar biyometrik veri içerebilir) ve hatta online takvimindeki toplantı yoğunluğu gibi veriler tek başlarına veya birleştirildiklerinde kişiyi kolaylıkla belirlenebilir kılmaktadır. Çalışmamızın ikinci bölümde detaylandırılan yapay zekâ destekli izleme sistemleri, bu farklı veri noktalarını analiz ederek çalışan hakkında detaylı profiller oluşturma ve böylece belirlenebilirliği daha da artırma potansiyeline sahiptir.

[469] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 56-57.

[470] Dülger, *Kişisel Verilerin Korunması Hukuku*, 91-92; Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 113; Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 2.

[471] *"Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade etmektedir. Kanunun gerekçesinde bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan verilerin yanı sıra, kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin verilerin de kişisel veri niteliğinde olduğu belirtilmiştir. Kişisel veriler, kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıyabileceği gibi, kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm verileri kapsamaktadır. Nitekim, Kanunun gerekçesinde de telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi verilerin dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel veri olarak kabul edilmesi gerektiğine işaret edilmiştir."* Bknz. Kişisel Verileri Koruma Kurumu, *6698 sayılı Kanunda Yer Alan Temel Kavramlar* (Ankara: Kişisel Verileri Koruma Kurumu, 2020), 14-15.

[472] Küzeci ve Kılıç, "6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler", 956-58.

Kişiyle hiçbir şekilde ilişkilendirilemeyen anonim bilgiler kişisel veri kabul edilmeyecektir[473]. Bu bağlamda, GDPR 4. maddesinin 5. fıkrasında tanımlanan "takma ad verilmiş veriler" (pseudonymised data), verilerin doğrudan bir gerçek kişiyle ilişkilendirilmesini zorlaştırmakla birlikte, tamamen anonim sayılmamaktadır. Söz konusu verilerin, belirli ek bilgilerle birleştirilerek ilgili kişinin kimliğinin yeniden tespit edilmesinin mümkün olması durumunda, bu veriler kişisel veri niteliğini korumaya devam etmektedir[474]. Örneğin, bir izleme yazılımında her çalışana "Kullanıcı 123" gibi takma bir ad verilmesi, veriyi tek başına anonim kılmaz. Çünkü işveren, "Kullanıcı 123"ün hangi çalışana karşılık geldiğini gösteren ek bir bilgiye (eşleştirme anahtarına) sahiptir. Bu nedenle, bu aktivite verileri kişisel veri olarak korunmaya devam eder. GDPR Başlangıç bölümü 28. maddesi, takma ad verilmiş verilerin kullanımının, ilgili veri sahipleri açısından riskleri azaltabileceğini ve veri sorumluları ile veri işleyenlerin veri koruma yükümlülüklerini yerine getirmelerine yardımcı olabileceğini belirtmektedir[475]. Bu çerçevede takma adlandırma, veri işleme süreçlerinde amaçla sınırlılık, ölçülülük ve veri güvenliği ilkelerinin sağlanmasına katkıda bulunabilecek etkili bir araç olarak değirilebilecektir.

4.1.4. Özel Nitelikli Veriler

Özel nitelikli kişisel veriler (hassas veriler), doğaları gereği işlenmeleri durumunda ilgili kişiler hakkında ayrımcılığa veya mağduriyete sebep olma riski taşıdıkları için daha sıkı korumaya tabi tutulan kişisel veri kategorisidir[476]. KVKK'nın 6. maddesinin

---

[473] Küzeci ve Kılıç, "6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler", 956-58. Örneğin, bir mahkeme kararının içeriğinde geçen kişilerin isimleri gizlenerek kararın yayımlanması durumunda, bu kararda yer alan veriler kural olarak kişisel veri niteliğini kaybedecektir. Ancak, söz konusu verilerin diğer bilgilerle kolayca eşleştirilmesi ve ilgili kişilerin kimliklerinin bu yolla belirlenebilmesi mümkünse, bu durumda halen kişisel veriden söz edilmesi gerekir. Konuyla ilgili diğer örnekler için bknz. Dülger, *Kişisel Verilerin Korunması Hukuku*, 93-102.

[474] Tele çalışmada, çalışanların performans metrikleri (örneğin, tamamlanan görev sayısı, çağrı yanıtlama süresi) başlangıçta bir kod veya takma ad ile kaydedilse bile, bu verilerin çalışanın proje atamaları, ekip bilgileri veya diğer sistemsel kayıtlarla birleştirilmesi halinde çalışanın kimliği kolaylıkla yeniden tespit edilebilir.

[475] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 58.

[476] Türkay Henkoğlu, "Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi" (Doktora Tezi, T.C. Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Bilgi ve Belge Yönetimi Anabilim Dalı, 2015), 18; Gürsel, İşçinin Kişisel Verilerinin Korunması Hakkı, 115-16; Erbil Beytar, İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması, 2. Baskı (On İki Levha Yayıncılık, 2018), 54-55; Berrak Yılmaz, "Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması" (Doktora Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, 2019), 17-18; Begüm

1. fıkrasına göre özel nitelikli kişisel veriler; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti[477], dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti[478] ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir. Ayrıca, özel nitelikli olmayan verilerin bile birleştirildiğinde bireyin özel hayatını derinden etkileyebileceği gerçeği; esasen "önemsiz veri" diye bir şey olmadığını ve hassas verilerin ayrı düzenlenmesinin diğerlerini daha az değerli kılmadığını göstermektedir[479]. Bu durum özellikle, verilerin analizi yoluyla yeni çıkarımlar üretilebildiği teknolojik izleme ortamlarında kritik bir önem kazanır. Örneğin, tele çalışma modelinde bir aktivite izleme yazılımının topladığı veriler (sürekli düşük aktivite, sık mola, düzensiz çalışma saatleri), bir çalışanın zihinsel veya fiziksel sağlık durumu (tükenmişlik, depresyon vb.) hakkında çıkarımlar yapmak için kullanılırsa, bu durum özel nitelikli sağlık verisinin işlenmesi anlamına gelebilir ve çok daha sıkı hukuki şartlara tabi olur[480].

Öztunay, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Işığında İşverenin Yönetim Hakkının Sınırları" (Yüksek Lisans Tezi, İzmir Ekonomi Üniversitesi Sosyal Bilimler Enstitüsü, 2019), 2; Küzeci, Kişisel Verilerin Korunması Hukuku, 277-89; Özer Deniz, "Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk", 54; Yiğit, İş İlişkisinde Kişisel Verilerin Korunması, 3-4.

[477] KVKK, "kılık ve kıyafet" ile "mezhep" bilgilerini özel nitelikli kişisel veriler arasında açıkça saymaktadır (madde 6/1). Buna karşın, GDPR madde 9(1)'de bu tür verileri ayrı ve bağımsız kategoriler olarak zikretmemektedir. "Mezhep" bilgisi, GDPR kapsamında daha genel bir kategori olan "dini veya felsefi inançlar" içinde değerlendirilebilecek nitelikte olmakla birlikte, "kılık ve kıyafet" verisi GDPR'da açıkça yer almamakta ve bu yönüyle KVKK'ya özgü bir koruma yaklaşımının yansıması olarak öne çıkmaktadır.

[478] KVKK, ceza mahkûmiyetine ve güvenlik tedbirlerine ilişkin verileri, 6. maddesi uyarınca doğrudan özel nitelikli kişisel veri kategorisine dâhil etmiştir. Buna karşılık, GDPR ise söz konusu verileri özel nitelikli veriler arasında değil, madde 10 kapsamında ayrı bir düzenlemeye tabi tutmakta ve bu tür verilerin işlenmesini yalnızca resmî makamların kontrolü altında ya da Birlik veya üye Devlet hukuku tarafından öngörülen uygun güvencelere tabi olarak mümkün kılmaktadır.

[479] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 119.

[480] Teknolojinin gelişmesiyle birlikte sağlıkla ilgili verilerin sınırları da giderek belirsizleşmiştir. Öyle ki, günümüzde "tüm veriler sağlık verisidir" ifadesi yaygın bir kabul görmeye başlamıştır. Sosyal medya platformları ve pazarlamacılar, meta verileri sürekli olarak bireylerin davranışlarını tahmin etme aracı olarak kullanmakta; örneğin, alışveriş alışkanlıklarına dayalı olarak birinin hamile olup olmadığını belirlemeye çalışmaktadırlar. Teknoloji hayatın her alanına daha derin nüfuz ettikçe ve veri analizi teknikleri geliştikçe, araştırmacılar ve kuruluşlar bu tür verilerden içgörüler elde etme konusunda daha cesur hale gelmektedir. Böyle bir ortamda, en önemsiz görünen veriler bile –örneğin bir video kaydındaki göz hareketleri veya akıllı cihazlar aracılığıyla toplanan sesli veriler– sağlık verisi olarak değerlendirilebilmektedir. Bu tür teknolojilerin sunduğu geniş veri akışı, yalnızca duygusal içeriklerin değil, aynı zamanda dil analizi veya konuşmadaki duraksamalar gibi unsurların da bireyin sağlık durumuna ilişkin önemli ipuçları olarak yorumlanmasına olanak tanımaktadır. Charlie Warzel, "Opinion | All Your Data Is Health Data", Opinion, The New York Times, 13 Ağustos 2019, https://www.nytimes.com/2019/08/13/opinion/health-data.html; The Data Will See You Now: Datafication and the Boundaries of Health (Ada Lovelace Institute, 2020), https://www.adalovelaceinstitute.org/report/the-data-will-see-you-now/.

Özel nitelikli kişisel verilerin işlenmesi hem KVKK'nın 6. maddesinin 3. fıkrası hem de GDPR 9. maddesinin 1. fıkrası uyarınca kural olarak yasaktır ve bu veriler, diğer kişisel verilere kıyasla daha sıkı koşullara tabidir. Söz konusu verilerin işlenmesine ancak ilgili kişinin açık rızası veya kanunda açıkça belirtilen istisnai durumlarda işlenebilir[481]. Açık rızaya dayalı özel nitelikli veri işleme faaliyetinde ise veri sahibinin ilgili konu hakkında yeterince bilgilendirilmesinin ardından, özgür iradesiyle ve belirli bir çerçevede onay vermesi gerekmektedir[482]. KVKK'nın 6. maddesinin 3. fıkrasına göre[483], özel nitelikli kişisel veriler, ancak aynı maddede açıkça öngörülen istisnai hâllerde, ilgili kişinin açık rızası aranmaksızın işlenebilecektir[484].

2024 yılında 7499 sayılı Kanun ile KVKK'nın 6. maddesinde yapılan değişiklikle, özel nitelikli kişisel verilerin açık rıza olmaksızın işlenebileceği istisnai hâllere yenileri eklenmiştir[485]. Yapılan bu düzenleme ile istihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarında, ilgili yükümlülüğün başka bir şekilde yerine getirilmesinin mümkün olmaması koşuluyla ve ölçülülük ilkesi çerçevesinde özel nitelikli kişisel verilerin açık rıza aranmaksızın işlenmesine olanak tanınmıştır[486]. Anılan yükümlülükler yalnızca kanun kaynaklı olmayıp; yönetmelik,

---

[481] Yılmaz, "Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması", 18.

[482] GDPR bağlamında da, rıza alınmış olsa bile işleme faaliyetinin her zaman madde 5'teki temel ilkelere (özellikle gereklilik, orantılılık, amaçla sınırlılık) uygun olması gerekmektedir.

[483] 7499 sayılı Kanun ile yapılan ve 1 Haziran 2024'te yürürlüğe giren değişiklik uyarınca, KVKK madde 6'da özel nitelikli kişisel veriler arasındaki (sağlık ve cinsel hayat verileri ile diğerleri) işleme şartı farklılığı kaldırılmıştır.

[484] 6698 sayılı Kişisel Verilerin Korunması Kanunu madde 6/3*: "Özel nitelikli kişisel verilerin işlenmesi yasaktır. Ancak bu verilerin işlenmesi;*
a) İlgili kişinin açık rızasının olması,
b) Kanunlarda açıkça öngörülmesi,
c) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
ç) İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,
d) Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,
e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,
f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,
g) Siyasi, felsefî, dinî veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması, halinde mümkündür.".

[485] Mehmet Bedii Kaya, KVKK Reformu 2024 Değişiklikleri (On İki Levha Yayıncılık, 2025), 11-27.

[486] Kaya, *KVKK Reformu 2024 Değişiklikleri*, 20.

yönerge, tebliğ gibi ikincil düzenlemelere veya taraflar arasında akdedilen sözleşmelere de dayanabilmektedir[487]. Bu durum, GDPR 9. maddesinin 2. fıkrasının (b) bendinde yer alan,

> işlemenin veri sorumlusunun veya veri sahibinin istihdam ve sosyal güvenlik ve sosyal koruma hukuku alanındaki yükümlülüklerinin yerine getirilmesi ve özel haklarının kullanılması amacıyla gerekli olması ve Birlik veya Üye Devlet hukuku veya Üye Devlet hukukuna tabi toplu sözleşmeler tarafından veri sahibinin temel hakları ve menfaatleri için uygun güvenceler sağlanması kaydıyla yetkilendirilmiş olması

hâline paralel bir hukuka uygunluk sebebi sunmaktadır[488].

Avrupa Birliği Yapay Zekâ Tüzüğü'nün 5. maddesi, GDPR ve KVKK'dan farklı olarak belirli veri türlerinin işlenmesini değil, bu verileri işleyerek "kabul edilemez risk" oluşturan spesifik yapay zekâ uygulamalarını yasaklamaktadır. Bu kapsamda; biyometrik verilerin bireylerin ırk, siyasi görüş, sendika üyeliği, dini inanç, cinsel yönelim gibi hassas özelliklerini ortaya çıkarmak amacıyla kullanılması; işyerleri ve eğitim kurumlarında duygu ve niyet analizi yapmak için biyometrik duygu tanıma sistemlerinin kullanılması; internet veya güvenlik kameralarından hedefsiz olarak yüz görüntülerinin toplanmasıyla yüz tanıma veri tabanlarının oluşturulması; kişisel

---

[487] Kişisel Verileri Koruma Kurumu, *Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Rehber* (KVKK Yayınları, 2025), 51:49-54.

[488] Bu kapsamda örnekler tele çalışma özelinde çeşitlilik göstermektedir: Tele çalışanın evinde yaşanabilecek bir sağlık sorununda hızlı müdahale için işverenin önceden alınmış sınırlı sağlık verilerine (örneğin, alerji bilgisi, acil durumda aranacak kişi) erişmesi; kurumsal sistemlere uzaktan ve güvenli erişim için tele çalışanın kendi cihazındaki biyometrik kimlik doğrulama (örneğin parmak izi veya yüz tanıma) verilerinin işlenmesi (ancak bu verilerin işveren tarafından saklanmaması ve yalnızca kimlik doğrulama amacıyla kullanılması kaydıyla); hassas verilerle çalışan bir tele çalışanın güvenilirliğinin teyidi amacıyla, işin niteliği gerektiriyorsa ve yasal dayanağı varsa, adli sicil kaydının talep edilmesi bu duruma örnek olarak gösterilebilir. Benzer şekilde, tele çalışma sırasında sürekli webcam izlemesi yapılıyorsa, çalışanın kılık ve kıyafetine ilişkin veriler de özel nitelikli veri (örneğin, dini inancı yansıtan giyim tarzı) kapsamına girebilir ve bu tür bir izlemenin meşruiyeti daha da sıkı koşullara bağlanır. Dinî inanç, mezhep, siyasi görüş veya etnik köken gibi verilerin ise, tele çalışanın işe alımında, görev dağılımında ya da performansının izleme araçlarıyla değerlendirilmesi sürecinde dikkate alınması hukuken ve etik olarak kabul edilemez. Dernek ve vakıf üyeliği gibi veriler ise yalnızca yasal zorunluluk gereği bildirim yapılması gereken hallerde ve sınırlı şekilde işlenebilir. Tele çalışanın sağlık durumunu veya yorgunluk seviyesini izlemek amacıyla kullanılan giyilebilir teknolojilerden elde edilen genetik veya diğer sağlık verileri ise, örneğin işe uygunluk testlerinde ya da sağlık taramalarında kullanıldığında, açıkça ölçülülük ve gereklilik testine tabi tutulmalıdır. Açık rızanın varlığı dahi bu tür verilerin her durumda işlenmesini meşru kılmaz. Bu nedenle, işverenin veri sorumlusu sıfatıyla yürüttüğü tüm veri işleme faaliyetlerinde, amaçla bağlantılılık, sınırlılık ve ölçülülük ilkelerine uygun hareket etmesi, çalışanların temel hak ve özgürlüklerinin korunması açısından zorunludur. Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 209-42; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 147-54; Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 188-90; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 228-47; Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 19-29; Yılmaz ve Çavuşoğlu, *Kişisel Verileri Koruma Hukuku*, 27-35.

özellikler veya sosyal davranışların, ilgisiz bağlamlarda ayrımcılığa yol açacak biçimde sosyal puanlama amacıyla işlenmesi; kişinin suç işleme riskini öngörmek amacıyla profilleme verilerinin kullanımı; bireylerin savunmasızlık durumlarının ciddi zarara neden olacak şekilde sömürülmesi; kolluk kuvvetlerinin kamuya açık alanlarda gerçek zamanlı biyometrik tanımlama yapması ve insanların bilinçaltı, manipülatif veya aldatıcı tekniklerle, kendi iradelerine aykırı şekilde yönlendirilmesi gibi faaliyetler yasaklanmıştır[489].

4.2. Hukuka Uygunluk Hâlleri

Kişisel verilerin korunması hukukunun temelini oluşturan ilkelerden biri, kural olarak kişisel verilerin işlenmesinin yasak olmasıdır[490]. Zira Anayasa'nın 20. maddesi uyarınca, kişisel veriler ancak kanunda öngörülen hâllerde veya ilgili kişinin açık rızasına dayanılarak işlenebilir. KVKK da bu anayasal çerçeveyi esas alarak kişisel veri işlemenin ancak açık rıza ya da kanunda sınırlı sayıda belirtilmiş hukuka uygunluk sebeplerine dayanarak gerçekleştirilebileceğini kabul etmiştir. Bu bağlamda kişisel verilerin işlenmesi hukuken yasak bir faaliyet olarak kabul edilmekte, ancak istisnai koşullar altında hukuka uygun hâle gelmektedir. Bu temel ilke, çalışanların özel hayat alanlarında gerçekleşebilen tele çalışmadaki izleme ve gözetleme faaliyetleri açısından büyük önem taşımaktadır. Zira bu tür faaliyetlerin doğası gereği müdahaleci olabilmesi, dayanacakları hukuka uygunluk sebebinin çok daha titiz bir değerlendirmeye tabi tutulmasını zorunlu kılmaktadır. Şunu da ifade etmek gerekir ki, iş ilişkisi gibi taraflar arasındaki güç dengesizliğinin belirgin olduğu hâllerde açık rızaya dayalı veri işlemesi de başvurulması gereken son çare niteliğindedir. Bu sebeple, diğer hukuka uygunluk sebeplerine dayanılmasının mümkün olduğu hâllerde açık rızaya başvurulmamalıdır. Önemine binaen hukuka uygunluk sebepleri aşağıda ayrıntılı olarak ele alınacaktır.

---

[489] Paul Voigt ve Nils Hullen, *The EU AI Act: Answers to Frequently Asked Questions* (Springer Berlin Heidelberg, 2024), 49-55, https://doi.org/10.1007/978-3-662-70201-7.

[490] Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 69; Nazlı Elbir, "Kişiliğinin Korunması Bağlamında İşçiye Ait Kişisel Verilerin Korunması" (Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2020), 148; Nazlıhan Özdemir Coşkun, "Kişisel Verilerin Korunması ve İşlenmesi" (Yayınlanmamış Yüksek Lisans Tezi, Kadir Has üniversitesi, 2022), 58; Hazar Can Kıpçak, *Çalışanların Kişisel Verilerinin İş İlişkisi Kapsamında Korunması* (Seçkin Yayıncılık, 2023), 55, https://www.seckin.com.tr/kitap/263371922; Yonca Dursun, *6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Işçinin Korunması*, 2. (Seçkin, 2023), 68.

Kişisel verilerin, veri koruma mevzuatında öngörülen hukuka uygunluk sebeplerinden herhangi birine dayanmaksızın işlenmesi, hukuka aykırılık teşkil etmektedir. Bu durum ise veri sorumlusu açısından hem özel hukuk hem de ceza hukuku yönünden sorumluluğa yol açabilmektedir. Ayrıca ifade edelim ki, hukuka uygunluk sebeplerinin varlığı veri işleme faaliyetinin hukuka uygun kabul edilebilmesi için yeterli olmayıp, ayrıca KVKK'nın 4. maddesinde düzenlenen ilkelere uygun şekilde veri işlemenin gerçekleştirilmesi gerekmektedir. Veri sorumlusunun, kanunda düzenlenen aydınlatma yükümlülüğü ile veri güvenliğini sağlama yükümlülüğü başta olmak üzere diğer yükümlülüklerini de usulüne uygun şekilde yerine getirmesi, veri işleme faaliyetlerinin hukuka uygunluğu ve ilgili kişilerin temel haklarının korunması açısından zorunluluk arz etmektedir. İlgili kişinin hukuka aykırılık hâlinde maddi ve manevi tazminat talep etme hakkı da varlığını korumaktadır[491]. Türk Ceza Kanunu'nun 135 ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak kaydedilmesi, yayılması veya ele geçirilmesi suç olarak tanımlanmıştır[492].

Kişisel Verilerin Korunması Kanunu'nda hukuka uygunluk sebepleri de genel nitelikli kişisel veriler ile özel nitelikli kişisel veriler bakımından ayrı ayrı düzenlenmiştir. Nitekim Kanun'un 5. maddesi genel nitelikli kişisel verilerin, 6. maddesi ise özel nitelikli kişisel verilerin işlenmesinde hukuka uygunluk sebepleri düzenlenmiştir. 5. maddenin kenar başlığı "Kişisel Verilerin İşlenme Şartları" olup, burada sayılan hukuka uygunluk sebepleri; açık rıza, kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rıza veremeyecek durumda olan kişinin veya bir başkasının hayatı ya da beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şeklinde sıralanmıştır. 6. maddenin kenar başlığı ise "Özel Nitelikli Kişisel Verilerin

[491] Gürsel, İşçinin Kişisel Verilerinin Korunması Hakkı, 414-19; Ömer Ekmekçi vd., Kişisel Verilerin Korunması Hukuku, 3. (On İki Levha Yayıncılık, 2025), 402-3.
[492] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 477-94; Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 190-97.

İşlenme Şartları" olup, bu hüküm çerçevesinde özel nitelikli verilerin işlenmesi kural olarak yasaktır. Maddeye göre;

> Ancak bu verilerin işlenmesi; a) İlgili kişinin açık rızasının olması, b) Kanunlarda açıkça öngörülmesi, c) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, ç) İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması, d) Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması, e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması, f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması, g) Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması, halinde mümkündür.

Belirtelim ki, sözü geçen hükmün 2024 yılında 7499 sayılı Kanun ile yapılan değişiklik öncesindeki hâlinde, özel nitelikli kişisel verilerin işlenmesine ilişkin hukuka uygunluk sebepleri, veri kategorilerine göre farklı şekilde düzenlenmişti. Ancak gerçekleştirilen değişiklikle tüm özel nitelikli kişisel veri türleri bakımından ortak düzenleme getirilmiş olup, kanaatimizce bu değişiklik de GDPR'a uyum bakımından isabetlidir. Aşağıda mevzuatta öngörülen hukuka uygunluk sebepleri öncelikle genel nitelikli kişisel verilerin işlenmesi, ardından özel nitelikli kişisel verilerin işlenmesi açısından ele alınacaktır. Her iki hâlde de ortak bir hukuka uygunluk sebebi olan "açık rıza" ise tekrara düşmemek adına yalnızca genel nitelikli kişisel verilerin işlenmesinde hukuka uygunluk sebepleri başlığı altında incelenecektir. Değerlendirmelerimizde yürürlükteki mevzuatın yanı sıra GDPR'ın ilgili hükümlerine yer verilerek, karşılaştırma yapılacaktır.

4.2.1. Genel Nitelikli Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebepleri

4.2.1.1. Açık Rıza

Kişisel verilerin korunması hukukunda açık rıza, KVKK'nın 3. maddesinin birinci fıkrasının (a) bendi uyarınca *"belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"*, GDPR 3. maddesinin birinci fıkrası kapsamında ise *"veri sahibinin, kendisine ilişkin kişisel verilerin işlenmesine, bir beyan yoluyla ya da*

açık bir onay eylemiyle özgürce, belirli, bilgilendirilmiş ve kesin bir şekilde (unambiguous) verdiği her türlü irade beyanı" olarak tanımlanmıştır[493]. Her ne kadar GDPR, KVKK gibi doğrudan "açık rıza" başlığı altında bir tanım yapmasa da rızanın geçerliliği için aradığı unsurlar büyük ölçüde paralellik göstermektedir. İki düzenlemede de açık rızanın geçerliliği için belirli kriterlerin aynı anda karşılanması gerekmektedir. Öncelikle, ilgili kişinin iradesinin hiçbir yoruma ihtiyaç bırakmayacak açıklıkta ve netlikte olması şarttır; GDPR, Başlangıç bölümü 32. maddesi bu noktada rızanın "açık bir onay eylemiyle" (clear affirmative action) verilmesi gerektiğini vurgular ki bu, sessiz kalma veya eylemsizliğin rıza olarak kabul edilemeyeceği anlamına gelmektedir[494]. İlgili düzenleme uyarınca, genel ya da belirsiz ifadeler geçerli bir açık rıza olarak kabul edilmemektedir. Rızanın belirli ve somut bir veri işleme faaliyetine yönelik olması, önceden yapılacak yeterli bir bilgilendirme sonucunda verilmesi ve rıza beyanının tamamen gönüllü olması gerekmektedir[495]. Söz konusu özel nitelikli kişisel veriler olduğunda, rızanın daha açık ve net biçimde ortaya konmalıdır. Ayrıca, veri işleme faaliyeti başlamadan önce alınmamış açık rıza hukuken geçerli sayılmaz[496].

İş ilişkisi kapsamında açık rızanın değerlendirilmesi ise, işveren ile işçi arasındaki bağımlılık ve güç dengesizliği nedeniyle daha önce de ifade ettiğimiz üzere özel bir önem arz etmektedir[497]. İşçinin işverene ekonomik ve sosyal yönden bağlı olması, açık

---

[493] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 193-209; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 154-57; Dülger, *Kişisel Verilerin Korunması Hukuku*, 138-47; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 264; Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 83-85; Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 49-63; Yılmaz, "Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması", 27; Canberk Yıldız, "Bir Gözetim Tekniği Olarak Kapalı Devre Kameraların Kullanılması ve Kişisel Verilerin Korunması" (Yayınlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, 2022), 158.

[494] Feiler vd., The EU General Data Protection Regulation (GDPR), 58.

[495] Bu unsurlar, tele çalışma modelinde kullanılan izleme ve gözetleme araçları için rıza alınırken özel bir titizlikle değerlendirilmelidir. Örneğin, bir tele çalışandan genel bir "çalışma faaliyetlerinin izlenmesine" yönelik rıza alınması yeterli olmayıp, hangi izleme yazılımının (örneğin, klavye hareketlerini kaydeden, ekran görüntüsü alan veya web kamerasını aktive eden bir yazılım) kullanılacağı, hangi tür verilerin (kullanılan uygulamalar, aktif/pasif çalışma süreleri, iletişim meta verileri vb.) ne sıklıkta ve hangi amaçla toplanacağı, bu verilere kimlerin erişeceği ve ne kadar süreyle saklanacağı gibi detayların açıkça belirtildiği spesifik bir bilgilendirmeye dayanmalıdır.

[496] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 193-97; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 155; Dülger, *Kişisel Verilerin Korunması Hukuku*, 141-47; Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 83-96; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 264-72; Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 50-61; Muhammed Esat Gül, "Kişisel Veri İşleme Şartlarından Açık Rıza" (Yüksek Lisans Tezi, İstanbul Üniversitesi, 2022), 45-66.

[497] Falque-Pierrotin, *Opinion 2/2017 on Data Processing at Work*, 22-24.

rızanın özgür iradeyle verilip verilmediği konusunda haklı bir şüphe yaratmaktadır[498]. Madde 29 Çalışma Grubu da işçinin iş sözleşmesini sürdürebilmesi için kişisel verilerinin işlenmesini kabul etmek zorunda kalması durumunda, bu rızanın açık rıza olarak değerlendirilemeyeceğini vurgulamıştır[499]. İş ilişkilerinde işçinin pazarlık gücünden yoksun oluşu, özellikle işe alım süreçlerinde kişisel verilerin işlenmesine ilişkin rıza beyanlarının gerçek anlamda özgür iradeye dayalı olarak verilmesini önemli ölçüde güçleştirmektedir. Zira şeklen bir rıza beyanı alınsa da fiilen özgür iradeye dayanıp dayanmadığının tespiti mümkün değildir. İşveren tarafından kişisel verilerin toplanması, bu veriler üzerinden algoritmik değerlendirmeler yapılması veya çeşitli testlerin uygulanması karşısında işçi, iş ilişkisinin kurulması veya sürdürülmesi endişesiyle bu şartları kabul etmek zorunda kalmaktadır[500]. Kişisel verilerin işlenmesinin, kişilik hakkına müdahale teşkil ettiği durumlarda yalnızca rızaya dayanan bir hukuka uygunluk sebebine dayanılması, veri sahibinin korunması açısından yetersiz kalmaktadır. Bu sebeple daha güçlü ve çok katmanlı bir hukuki koruma mekanizmasının uygulanması gerekmektedir[501]

GDPR, Başlangıç bölümü 43. maddesinde, rızanın özgürce verilmiş sayılabilmesi için, özellikle veri sahibi ile veri sorumlusu arasında açık bir dengesizlik olduğunda (örneğin işveren-işçi ilişkisi), rızanın verilmemesinin veri sahibi için olumsuz sonuçlar doğurup doğurmayacağının dikkate alınması gerektiğini belirtmektedir[502]. Bu durum özellikle, işçinin özgür iradesiyle rıza gösteremediği, rıza vermeye mecbur bırakıldığı veya reddetme seçeneğinin fiilen ortadan kaldırıldığı durumlarda ortaya çıkmaktadır[503]. Madde 29 Çalışma Grubu'nun (şimdiki Avrupa Veri Koruma Kurulu -

---

[498] Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 90.

[499] Alman Hukukunda sadece işçinin veya hem işverenin hem de işçinin menfaatine uygun olan durumlarda işçinin rızasının olduğu kabul edilmektedir. Ayrıntılar için bknz. Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 60; Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 243; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 156-57; Öztunay, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Işığında İşverenin Yönetim Hakkının Sınırları", 78.

[500] Sevimli, *İşçinin Özel Yaşamına Müdahalenin Sınırları*, 147; Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 90.

[501] Ugan Çatalkaya, İş Hukukunda Ölçülülük İlkesi, 278-90; Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 90.

[502] Feiler vd., The EU General Data Protection Regulation (GDPR), 81.

[503] Madde 29 Çalışma Grubu'nun 2017/2 sayılı görüşünde belirtildiği üzere, iş ilişkisinin kendine özgü yapısı gereği, işçinin kişisel verilerinin işlenmesine ilişkin olarak serbest iradesiyle açık rıza vermesi ve verdiği bu rızayı özgürce geri alabilmesi çoğunlukla mümkün değildir Ayrıntılı bilgi için bknz. Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251rev.01)* (European Commission, 2018),

EDPB) 2017/2 sayılı görüşünde de belirtildiği üzere, iş ilişkisinin kendine özgü yapısı gereği, işçinin kişisel verilerinin işlenmesine ilişkin olarak serbest iradesiyle açık rıza vermesi ve verdiği bu rızayı özgürce geri alabilmesi çoğunlukla mümkün değildir[504]. Bu sebeple, iş ilişkisinde rızanın özgürce verilip verilmediği her somut olayın koşullarına göre ayrı ayrı değerlendirilmelidir. İşverenin, işçinin açık rızayı reddetme imkânını fiilen ve hukuken sağlaması bu noktada kritik önem taşımaktadır[505].

Tele çalışma özelinde bu güç dengesizliği, işverenin belirli izleme araçlarını uzaktan etkin çalışma ve denetim için vazgeçilmez olarak sunması ve işçinin işini kaybetme endişesiyle söz konusu araçların kullanımına rıza vermek zorunda hissetmesi şeklinde tezahür edebilir. İşverenin, rıza talep ettiği izleme yöntemine alternatif, daha az müdahaleci bir denetim veya performans değerlendirme yöntemi sunup sunmadığı, rızanın özgürce verilip verilmediğinin tespitinde önemli bir kriter olacaktır. Bununla birlikte belirtelim ki, tele çalışma sözleşmesine "her türlü dijital izlemeye rıza gösteriyorum" şeklinde eklenen genel bir madde, rızanın belirli olma unsurunu karşılamadığı ve işçinin işi kaybetme baskısı altında özgür iradesini yansıtmadığı için hukuken geçersiz sayılacaktır[506].

---

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610164; Serhat Sezgin, *İş İlişkisinde İşçinin Kişilik Haklarına Yönelik Müdahaleler* (Seçkin, 2024), 72.

[504] Article 29 Data Protection Working Party, *Opinion 2/2017 on data processing at work*, 17/EN WP 249 (Brussels, Belgium, 2017), 4, http://ec.europa.eu/justice/data-protection/index_en.htm.

[505] Kişisel Verileri Koruma Kurumu, *Açık Rıza* (Kişisel Verileri Koruma Kurumu, 2020), 1-7, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf.

[506] Bu noktada, iş sözleşmelerinde yer alan belirli ve açık hükümlerin yargı mercileri tarafından nasıl yorumlandığına dikkat çekmek gerekir. Anayasa Mahkemesi'nin Celal Oraj Altunörgü kararı, bu duruma önemli bir örnek teşkil etmektedir. Başvuruda, özel bir banka çalışanının kurumsal e-posta hesabının, iş sözleşmesindeki bir maddeye dayanılarak incelenmesi ve bu yazışmalar gerekçe gösterilerek iş sözleşmesinin feshedilmesi ele alınmıştır. Başvurucu, bilgilendirme yapılmadan ve rızası alınmadan hesabının incelendiğini iddia etse de, Anayasa Mahkemesi, taraflar arasındaki iş sözleşmesini incelemiştir. Sözleşmede, "personelin banka mülkiyetinde olan elektronik posta adresini (kurumsal e-posta) sadece iş amaçlı olarak kullanmakla yükümlü olduğu" ve "kurumsal e-postanın banka yönetimi tarafından haber verilmeksizin denetlenebileceği, personelin bu konuda itirazının olmayacağı" şeklinde açık bir düzenlemenin yer aldığı tespit edilmiştir. Anayasa Mahkemesi, bu durumu, işverenin denetleme yetkisi ve usulü hakkında çalışana önceden açıkça bildirim yapıldığı ve başvurucunun da iş sözleşmesini imzalayarak bu denetime rıza gösterdiği şeklinde değerlendirmiştir. Bu karar, genel ve soyut ifadelerden farklı olarak, denetimin konusunu (kurumsal e-posta), amacını ve kapsamını yeterince belirgin kılan sözleşme hükümlerinin, hem aydınlatma yükümlülüğünü yerine getiren bir araç hem de geçerli bir "açık rıza" beyanı olarak kabul edilebileceğine dair önemli bir yargısal içtihat sunmaktadır. Bununla birlikte, kanaatimizce Anayasa Mahkemesi'nin bu yaklaşımı, kişisel verilerin korunması hukukunun temel ilkeleri, özellikle de rızanın özgür iradeye dayanması unsuru açısından eleştiriye açıktır. Çalışmamızda da vurgulandığı üzere, işveren ile işçi arasındaki açık güç dengesizliği, iş sözleşmesinin imzalanması sırasında verilen bir rızanın geçerliliğini şüpheli kılmaktadır. İşçinin, işi kaybetme veya hiç edinememe baskısı altındayken, denetim yetkisi tanıyan bir maddeyi müzakere etme veya reddetme imkânı fiilen bulunmamaktadır. Bu nedenle, sözleşmedeki bir

Veri koruma ilkeleri uyarınca, açık rızanın, diğer hukuka uygunluk sebeplerinin var olduğu durumlarda, yanıltıcı veya dürüstlük kuralına aykırı olmaması için tercih edilmemesi gerekir. Kişisel Verileri Koruma Kurumu'nun da belirttiği gibi, veri işleme faaliyetinin, açık rıza dışında bir hukuka uygunluk sebebine dayanılarak yürütülmesi mümkün iken açık rızaya dayandırılması, aldatıcı ve hakkın kötüye kullanımı niteliğinde olabilir[507]. Başka bir deyişle, iş ilişkisi içinde açık rıza, daha önce ifade ettiğimiz üzere ancak diğer hukuka uygunluk hâlleri bulunmadığında başvurulabilecek "son çare" niteliğindedir[508]. GDPR 7. maddesinin 4. fıkrası, bir sözleşmenin ifasının, o sözleşmenin ifası için gerekli olmayan kişisel verilerin işlenmesine rıza gösterilmesi koşuluna bağlanıp bağlanmadığına azami dikkat gösterilmesi gerektiğini belirterek, rızanın özgürlüğünü korumaya yönelik bir başka güvence sunmaktadır[509].

İşçinin verdiği açık rızanın her zaman koşulsuz olarak geri alınabileceği, veri sorumlusunun bu konuda gerekli kolaylığı sağlamak ve periyodik bilgilendirmelerde bulunmak zorunda olduğu da öğretide belirtilmektedir[510]. GDPR 7. maddesinin 3. fıkrası bu hakkı açıkça düzenleyerek, rızanın geri çekilmesinin rıza vermek kadar

---

imzanın, KVKK'nın aradığı bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza şartını tam olarak karşıladığını kabul etmek, işçinin daha zayıf konumunu ve rızanın diğer hukuka uygunluk nedenleri bulunmadığında başvurulacak bir son çare olması gerektiği ilkesini göz ardı etme riski taşımaktadır. Bu yorum, çalışanın temel haklarının, bir katılım sözleşmesi içerisinde pazarlık edilebilir bir unsur haline gelmesine ve rızanın özgürlüğü ilkesinin zayıflamasına zemin hazırlayabilir. Celal Oraj Altunörgü Başvurusu, Başvuru Numarası: 2018/31036 (Anayasa Mahkemesi 12 Ocak 2021), ¶ 40, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/31036 erişim 2025-03-02, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/31036.

[507] Söz konusu ilke, tele çalışma modelinde yürütülen izleme faaliyetlerinin hukuki meşruiyeti açısından, işverene bir önceliklendirme yükümlülüğü getirmektedir. Bu doğrultuda işveren, öncelikle meşru menfaat veya sözleşmenin ifası gibi hukuki sebeplere dayanmalı; rızayı ise ancak diğer hukuki dayanakların mevcut olmadığı durumlarda başvurulabilecek istisnai bir yol olarak kabul etmelidir. Kişisel Verileri Koruma Kurumu, *6698 sayılı Kanunda Yer Alan Temel Kavramlar*, 23.

[508] Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 53-54; Yıldız Güler, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Kişisel Verilerinin Korunması" (Yayınlanmamış Yüksek Lisans Tezi, İzmir Ekonomi Üniversitesi, 2022), 48; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 137.

[509] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 87.

[510] Nurşen Caniklioğlu, "Kişisel Verilerin Korunması Açısından İşçilerin Hakları", içinde *Prof. Dr. Turhan Esener III. İş Hukuku Uluslararası Kongresi*, 34. bs (Seçkin Yayıncılık, 2021), 271; Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 57. İşçinin açık rızasını geri alma hakkına sahip olması, kişisel verilerin işlenmesine ilişkin genel kural olmakla birlikte; işçinin bu hakkı kötüye kullanması veya hakkın kötüye kullanılması yasağı çerçevesinde kötü niyetli bir tutumla rızasını geri çekmesi halinde, kişisel verilerin işlenmesinin durdurulması söz konusu olmayacaktır. Başka bir ifadeyle, işçinin açık rızayı geri alma yetkisi, dürüstlük kuralı ile sınırlanmakta olup, hakkın kötüye kullanıldığı durumlarda kişisel veri işleme faaliyetleri hukuken kesintiye uğratılmayacaktır. Bknz. Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 156; Selen Uncular, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, 2. Baskı (Seçkin, 2018), 141-48.

kolay olması gerektiğini ve geri çekmenin ileriye dönük olarak geçerli olacağını belirtir[511]. İşçinin açık rızayı geri alma yetkisi, dürüstlük kuralı ile sınırlı olup, hakkın kötüye kullanıldığı durumlarda farklı değerlendirmeler gündeme gelebilecektir[512].

4.2.1.2. Kanunda Açıkça Öngörülme

Kanunda veri işleme faaliyetini açıkça öngören bir düzenlemenin bulunması hâlinde, ilgili kişinin açık rızası olmasa dahi bu faaliyet KVKK'nın 5. maddesinin 2. fıkrasının (a) bendi gereğince hukuka uygun kabul edilecektir. Bu düzenleme, TMK'nın 24. maddesinde yer alan "kanunun verdiği yetkinin kullanılması" ilkesine paralel bir nitelik taşımaktadır[513]. 95/46/EC sayılı Veri Koruma Direktif ve GDPR'da ise hukuka uygunluk nedenleri arasında "kanunlarda açıkça öngörülme" sebebine yer verilmemiştir[514]. GDPR 6. maddesinin 1. fıkrasının (c) bendi *"veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uyması"* veya GDPR 6. maddesinin 1. fıkrasının (e) bendi *"kamu yararına bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin kullanılması"* gibi daha spesifik yasal temellere atıfta bulunmaktadır. KVKK düzenlemesi bu noktada Direktif ve GDPR'a göre daha geniş bir hukuka uygunluk nedeni ihdas etmektedir[515].

Kanunda açıkça öngörülme şartının bir gereği olarak veri sorumlusu, veri işleme faaliyetini mutlaka açık, belirli ve doğrudan bir kanuni yetkiye dayandırmak zorundadır[516]. Aksi hâlde, yani veri işlemenin yeterli açıklık ve zorunluluk içermeyen

---

[511] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 87.

[512] Tele çalışma bağlamında, bir çalışanın daha önce, örneğin sürekli ekran kaydı alınmasına verdiği rızayı geri çekmesi durumunda, işverenin bu durumu nasıl yöneteceği (örneğin, alternatif bir çalışma düzenlemesi sunup sunamayacağı veya rızanın geri çekilmesinin iş ilişkisine etkisi) önemli bir hukuki sorundur ve rızanın geri alınabilirliği ilkesiyle işin sürekliliği ihtiyacı arasında bir denge kurulmasını gerektirmektedir.

[513] Elbir, "Kişiliğinin Korunması Bağlamında İşçiye Ait Kişisel Verilerin Korunması", 126.

[514] Ayrıca, GDPR md. 6/1-(e) kamu yararına yürütülen görevler veya veri sorumlusuna tanınan resmî yetkinin icrası amacıyla kişisel verilerin işlenmesine hukuki dayanak teşkil etmektedir. Bu zemin, özellikle belediyeler, bakanlık birimleri ya da devlet üniversiteleri gibi kamu işverenlerinin tele çalışma ortamındaki izleme faaliyetlerinde geçerlilik kazanmaktadır. Bkz. Genel Veri Koruma Tüzüğü (Regulation (EU) 2016/679), md. 6/1-(e) ve Gerekçe 45; European Data Protection Board (EDPB), Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, 07.07.2021, s. 8-9; Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 842/14/EN, 9 Nisan 2014, s. 13-14.

[515] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 243.

[516] KVKK'nın dayandığı mehaz düzenleme olan 95/46/EC sayılı Direktifte bu yönde açık bir hükme yer verilmemiştir. Kanun koyucu, KVKK ile sözleşmesel ilişki kapsamında veri işlemenin hukuka uygunluk şartları arasında sayılması suretiyle, önceki düzenlemeye kıyasla veri işlemede hukuka

ya da belirsiz bir normatif temele dayandırılması durumunda, ilgili işleme faaliyeti hukuka uygunluk ölçütlerini karşılamayacak ve geçerlilik kazanamayacaktır[517]. Nitekim İş Kanunu'nun 75. maddesi uyarınca işverenin, işçiye ait kimlik bilgilerini özlük dosyasında bulundurma yükümlülüğü, işverenin bu kapsamdaki kişisel veri işleme faaliyetini açıkça öngören bir kanuni düzenleme örneğini teşkil etmektedir[518].

Kanaatimizce, tele çalışma modelinde çalışanların çeşitli dijital araçlarla sürekli ve müdahaleci bir biçimde izlenmesi ve gözetlenmesi söz konusu olduğunda, bu tür faaliyetlerin hukuka uygunluk zeminine oturtulması oldukça zordur. 1 Haziran 2024'te yürürlüğe giren 7499 sayılı Kanun ile Kişisel Verilerin Korunması Kanunu'nda yapılan değişiklikler, bu değerlendirmeyi daha da önemli hâle getirmiştir. Yapılan değişiklikle KVKK'nın 6. maddesine, özel nitelikli kişisel verilerin işlenmesi için yeni hukuka uygunluk sebepleri eklenmiştir. Özellikle, *"İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması"* yeni bir hukuka uygunluk şartı olarak getirilmiştir. Ancak bu istisna, işverenlere çalışanlarını sınırsız bir gözetleme yetkisi vermemektedir. Öncelikle bu şart, yalnızca özel nitelikli kişisel veriler için geçerlidir ve genel nitelikli verilerin (klavye hareketleri, ekran görüntüleri, e-posta içerikleri vb.) işlenmesini kapsamaz. Dahası hem bu yeni istisnanın hem de genel nitelikli veriler için öne sürülebilecek meşru menfaat gibi diğer işleme şartlarının temel bir koşulu vardır: ölçülülük ve zorunluluk. İşverenin, sürekli webcam ile izleme, klavye hareketlerini kaydetme veya ev ortamındaki sesleri analiz etme gibi yoğun ve özel hayata derinlemesine müdahale eden yöntemlerin, belirli ve meşru bir amacı gerçekleştirmek için zorunlu olduğunu ve daha az müdahaleci bir yöntemle aynı amaca ulaşılamayacağını ispatlaması gerekmektedir. İş Kanunu madde 75 gibi genel nitelikteki yönetim hakkı veya iş sağlığı ve güvenliğini sağlama yükümlülüğü, bu derece müdahaleci yöntemleri kendiliğinden "zorunlu" kılmaz ve hukuka uygun hâle getirmez. Dolayısıyla, bu tür yoğun gözetim faaliyetlerinin "kanunda açıkça

uygunluk sebeplerini genişletmiş ve uygulamada daha esnek bir çerçeve benimsemiştir. Bknz. Gürsel, İşçinin Kişisel Verilerinin Korunması Hakkı, 243.

[517] İşverenin veri işleme yetkisini düzenleyen ilgili mevzuat hükümleri için bknz. Özer Deniz, "Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk", 116-17.

[518] Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 109.

öngörülme" şartını karşıladığını söylemek mevcut mevzuat çerçevesinde mümkün görünmemektedir[519].

Dolayısıyla, bir tele çalışanın dijital ortamdaki faaliyetlerinin bu hukuka uygunluk sebebine dayandırılarak izlenebilmesi için, o izleme yönteminin, toplanacak veri türlerinin ve izlemenin kapsamının açık, belirli ve doğrudan bir kanuni yetkiye dayanması şarttır. İşverenin genel denetim ve yönetim hakkı veya işin düzenine ilişkin soyut kanuni atıflar, özellikle tele çalışanın mahremiyet alanına giren yoğun gözetim pratikleri için bu kapsamda yeterli bir yasal zemin oluşturmamalıdır. Bu nedenle, kanunda açıkça öngörülme şartının dar yorumlanması esastır. Kanaatimize, işverenin tele çalışanı yoğun teknolojik yöntemlerle izleyebilmesi için, izleme yönteminin, kapsamının ve sınırlarının, İş Kanunu gibi genel çerçeve kanunlar aracılığıyla dolaylı olarak değil, doğrudan bu duruma yönelik özel bir yasal düzenleme ile ele alınmalıdır. Aksi bir yorum, çalışanın Anayasa ile korunan temel haklarına orantısız bir müdahalenin kapısını aralayacaktır.

4.2.1.3. İlgili Kişinin veya Üçüncü Kişilerin Hayati Menfaatinin Korunması

Kişisel verilerin işlenmesi, KVKK'nın 5. maddesinin 2. fıkrasının (b) bendi ve KVKK'nın 6. maddesinin 3. fıkrasının (a) bendi uyarınca, "*fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu"* ise, ilgili kişinin açık rızası olmaksızın hukuka uygun kabul edilecektir[520]. Benzer bir yaklaşım GDPR'da da bulunmaktadır. GDPR 6. maddesinin 1. fıkrasının (d) bendi genel nitelikteki kişisel verilerin işlenmesinin *"veri sahibinin*

[519] Kanunlarda açıkça öngörülme şartı yalnızca kanun metinlerini değil, aynı zamanda kanunun verdiği yetkiye dayanarak çıkarılan yönetmelik gibi ikincil düzenlemeleri de kapsamaktadır. Temel hak ve hürriyetleri sınırlayan çerçevenin mutlaka kanunla çizilmesi gerekmekle birlikte, bu kanunların uygulanmasına ilişkin usul ve esasların yönetmelikler aracılığıyla detaylandırılması mümkündür. Dolayısıyla, kişisel verilerin işlenmesine dair genel çerçevenin bir kanun hükmüyle belirlenmesi halinde, bu hükmün ayrıntılarının kanuna dayanılarak çıkarılan bir yönetmelikle düzenlenmesi, söz konusu işlemenin "kanunlarda açıkça öngörülme" şartına aykırılık teşkil etmez. Örneğin, 6458 sayılı Kanun'un verdiği yetkiye dayanarak çıkarılan yönetmelikle yabancılara ait parmak izi gibi biyometrik verilerin işlenmesi veya Milli Eğitim Bakanlığı yönetmelikleri ile diplomalarda yer alacak kişisel verilerin belirlenmesi bu duruma örnek olarak gösterilmiştir. Ayrıntılar için bknz. Kişisel Verileri Koruma Kurumu, *Kanunlarda Öngörülme Kişisel Veri İşleme Şartına İlişkin Bilgi Notu*, no. 62 (Kişisel Verileri Koruma Kurumu, 2025), 17-23.

[520] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 198-99.

veya başka bir gerçek kişinin hayati menfaatlerinin korunması için gerekli olması" hâlinde hukuka uygun olacağını belirtmektedir[521]. Özel nitelikli kişisel veriler açısından ise GDPR 9. maddesinin 2. fıkrasının (c) bendi, işlemenin *"veri sahibinin veya veri sahibinin fiziksel veya yasal olarak rıza veremeyecek durumda olduğu başka bir gerçek kişinin hayati menfaatlerinin korunması için gerekli olması"* durumunda, rıza aranmaksızın yapılabileceğini düzenlemektedir[522].

KVKK genel kişisel verilerin işlenmesi için dahi *"fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunma veya rızasına hukuki geçerlilik tanınmama"* şartını ihdas etmiştir. KVKK'nın 5. maddesinin gerekçesinde bu duruma örnek olarak *"hürriyeti tahdit edilen bir kişinin kurtarılması amacıyla, kendisinin veya şüphelinin taşımakta olduğu telefon, bilgisayar, kredi kartı, banka kartı veya diğer teknik bir araç üzerinden yerinin belirlenmesi için"* kişisel verilerinin işlenebileceği ifade edilmiştir[523].

GDPR ise genel veriler için bu şartı açıkça belirtmemekte; sadece işlemenin hayati menfaatleri korumak için gerekli olması yeterli sayılmaktadır. Ancak, GDPR'ın Başlangıç bölümü 46. maddesi bu noktada önemli bir yorumlama kılavuzu sunmaktadır: *"Bir gerçek kişinin hayati menfaatlerine dayanan kişisel veri işleme, ilke olarak, yalnızca işlemenin açıkça başka bir hukuki temele dayandırılamadığı durumlarda gerçekleşmelidir"*[524]. Bu, GDPR açısından hayati menfaatlerin korunması hukuka uygunluk sebebinin, genellikle diğer işleme şartlarının (örneğin, rıza alınabiliyorsa rıza, yasal bir yükümlülük varsa yasal yükümlülük) uygulanamadığı durumlarda, bir nevi "son çare" olarak devreye girebileceğini ima etmektedir. KVKK'da ise "son çare" niteliği bu kadar belirgin bir şekilde ifade edilmemiştir, ancak "zorunlu olması" şartı bu yönde bir yoruma kapı aralayabilmektedir. Her iki düzenlemede de işleme faaliyetinin hayati menfaatlerin korunması amacıyla sınırlı ve

[521] Feiler vd., The EU General Data Protection Regulation (GDPR), 79.
[522] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 92.
[523] Elbir, "Kişiliğinin Korunması Bağlamında İşçiye Ait Kişisel Verilerin Korunması", 138.
[524] Madde 9/2-b; İşleme, Birlik hukuku ya da Üye Devlet hukuku uyarınca veya Üye Devlet hukukuna dayanılarak yapılan bir toplu iş sözleşmesi çerçevesinde yetkilendirilmiş olmak kaydıyla, istihdam, sosyal güvenlik ve sosyal koruma hukukunun alanında veri sorumlusunun ya da veri sahibinin yükümlülüklerini yerine getirmesi veya belirli haklarını kullanması amacıyla gerekli olduğu ölçüde ve veri sahibinin temel hakları ile menfaatlerine yönelik uygun güvenceleri sağlamak şartıyla gerçekleştirilebilir. Feiler vd., The EU General Data Protection Regulation (GDPR), 82.

orantılı olması esastır. İşveren, bu kapsamda, örneğin iş kazası geçiren ve bilinci yerinde olmayan işçinin rızası olmaksızın, acil tıbbi müdahale için sağlık bilgilerini sağlık personeliyle paylaşabilir veya iletişime geçilebilecek yakınlarının iletişim bilgilerini işleyebilir[525].

Tele çalışma kapsamında, bu hukuka uygunluk sebebinin rutin izleme ve gözetleme faaliyetlerini meşrulaştırmak için kullanılması kural olarak mümkün değildir. İşverenin, çalışanının performansını takip etmek, verimliliğini ölçmek veya iş süreçlerini denetlemek amacıyla gerçekleştirdiği izleme faaliyetleri, hayati menfaatlerin korunması kapsamına girmez. Ancak, çok istisnai ve öngörülemeyen durumlarda, tele çalışanın evinde çalışırken ani bir sağlık sorunu yaşaması ve bu durumun örneğin (başka bir amaçla ve hukuka uygun şekilde kurulmuş) bir video konferans sırasında fark edilmesi ya da işverenin sağladığı bir giyilebilir cihazın (eğer kullanımı başka bir hukuka uygun sebebe dayanıyorsa) bir kaza veya bayılma gibi bir durumu otomatik olarak algılaması hâlinde, çalışanın bilincinin kapalı olması ve rızasının alınamaması (fiili imkânsızlık) koşuluyla, acil tıbbi yardım çağrılması veya yakınlarına haber verilmesi amacıyla o an için zorunlu olan sağlık veya konum verisinin işlenmesi bu kapsama girebilir. Burada dahi, işleme faaliyeti sadece o anki hayati tehlikeyi bertaraf etmeye yönelik, sınırlı ve ölçülü olmalıdır. Bu dar kapsam, GDPR, Başlangıç bölümü 46. maddesindeki son çare olma ve KVKK'daki zorunlu olma ilkeleriyle de uyumludur. Bu noktada altı çizilmesi gereken husus şudur: İşveren, bir çalışana sağlık verisi toplayan giyilebilir bir cihazı "olası bir acil duruma karşı hayati menfaatleri korumak" amacıyla veremez. Cihazın kullanımı, başlangıçta çalışanın geçerli bir açık rızası gibi başka bir hukuka uygunluk sebebine dayanmalıdır. Hayati menfaatlerin korunması şartı, ancak cihaz kullanılıyorken ve rıza alınmasının imkânsız olduğu fiili bir acil durum (örneğin bilinç kaybı) ortaya çıktığında, o anki müdahale için bir gerekçe oluşturabilir. Bununla birlikte, hayati tehlike riskinin işin doğası gereği sürekli yüksek olduğu belirli sektörlerde (örneğin yalnız başına tehlikeli kimyasallarla çalışanlar, tıbbi acil müdahale gerektirebilecek sağlık personeli vb.) bu tür müdahale olanaklarının önceden öngörülmesi ve iş sağlığı güvenliği politikaları kapsamında yapılandırılması, istisnai bir hukuka uygunluk zemini oluşturabilir.

[525] Ayrıntılı bilgi için bknz. Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 63-71.

4.2.1.4. Sözleşmenin Kurulması veya İfası için Gerekli Olma

KVKK'nın 5. maddesinin 2. fıkrasının (c) bendi uyarınca, *"bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması"* durumunda, ilgili kişinin açık rızası aranmaksızın işleme gerçekleştirilebilmektedir[526]. GDPR 6. maddesinin 1. fıkrasının (b) bendi hükmünde benzer bir hukuka uygunluk sebebi öngörmektedir: *"işlemenin, veri sahibinin taraf olduğu bir sözleşmenin ifası için veya sözleşme öncesinde veri sahibinin talebi üzerine adımların atılması için gerekli olması"*. Her iki düzenleme de sözleşme tarafı olan kişinin talebiyle sözleşmenin kurulması veya ifası için "gerekli" olan adımların atılması sürecini kapsamakta; dolayısıyla veri sorumlusuna, ilgili kişinin kişisel verilerini, sözleşmesel yükümlülüklerin yerine getirilebilmesi amacıyla işleme yetkisi tanımaktadır[527]. Bu kapsamda "gereklilik" kavramı dar yorumlanmakta olup, işleme faaliyetinin sözleşmenin temel bir unsuru olması ve sözleşmenin ifası için objektif olarak zorunlu olması beklenmektedir; sadece faydalı veya sözleşmede yer alıyor olması yeterli değildir[528]. Bu istisna hem KVKK hem de GDPR uyarınca, temel olarak özel nitelikli olmayan kişisel veriler için geçerlidir. Özel nitelikli kişisel verilerin (örneğin sağlık verileri) sözleşmenin ifası için işlenmesi gerektiğinde, KVKK'nın 6. maddesinin 3. fıkrası uyarınca açık rıza veya kanunda belirtilen diğer istisnai hâllerden birinin karşılanması gerekmektedir.

İş sözleşmesi kapsamında kişisel verilerin işlenmesi, genel olarak üç farklı evrede gerçekleşmektedir: işe alım süreci (sözleşme öncesi aşama), iş ilişkisinin devamı (sözleşmenin ifası) ve iş sözleşmesinin sona ermesi. İşverenin sözleşme öncesi değerlendirme ve karar alma süreçlerini yürütebilmesi açısından, iş ilişkisinin henüz kurulmadığı aşamalarda da kişisel veri işleme faaliyeti gerekli hâle gelebilmektedir.

---

[526] Güler, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Kişisel Verilerinin Korunması", 55.

[527] GDPR kapsamında toplu iş sözleşmeleri doğrudan bir sözleşmesel ilişki olarak değerlendirilmemekle birlikte, madde 88 uyarınca üye Devletlere, iş ilişkilerine özgü daha ayrıntılı düzenlemeler getirme konusunda özel hükümler öngörme yetkisi tanınmıştır. Bu kapsamda, her bir üye devletin ulusal hukukunda, toplu iş sözleşmeleri çerçevesinde kişisel verilerin işlenmesine ilişkin özel kurallar getirme imkânı saklı tutulmuştur. Bknz. Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 105.

[528] European Data Protection Board (EDPB), *Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects* (t.y.), 9-10, erişim 29 Mayıs 2025, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

Örneğin, bir iş başvurusu sürecinde adayın özgeçmişinde yer alan kimlik bilgileri, iletişim bilgileri, eğitim durumu ve mesleki yeterliliklerine ilişkin veriler, işverenin sözleşme öncesi değerlendirme yapabilmesi ve adayla mülakat organize edebilmesi için işlenebilir[529]. Bu tür bir işleme faaliyeti, doğrudan ilgili kişinin talebi üzerine sözleşmenin kurulmasına yönelik adımların atılması amacıyla gerçekleştirildiğinden, KVKK'nın 5. maddesinin 2. fıkrasının (c) bendi ve GDPR 6. maddesinin 1. fıkrasının (b) bendi) kapsamında açık rıza aranmaksızın hukuka uygun kabul edilmektedir[530]. Tele çalışmaya özgü bir pozisyon için işe alım sürecinde, adayın uzaktan çalışma yetkinliklerini teyit etmek veya sözleşmenin ifası için kritik olan teknik altyapı (örneğin, stabil internet erişimi) hakkında bilgi almak gibi durumlar, bu gereklilik kapsamında değerlendirilebilir. Ancak bu hukuka uygunluk sebebi adayın özel hayatının detaylı bir incelemesini haklı çıkarmaz. Benzer şekilde, işin ifası aşamasında işçinin görevini yerine getirebilmesi için kendisine tahsis edilen kurumsal e-posta adresi veya şirket telefon hattının veri kayıt sistemine işlenmesi; iş süreçlerinin yürütülmesi amacıyla çalışma süresi takip sistemleri, görev atama yazılımları veya iç iletişim platformlarına kişisel bilgilerinin entegrasyonu da bu kapsamda değerlendirilmektedir[531].

Tele çalışma sözleşmesinin ifası için hangi izleme ve gözetleme faaliyetlerinin gerekli olduğu sorusu ise daha titiz bir değerlendirme gerektirmektedir. Örneğin, bir tele çalışanın kurumsal sistemlere uzaktan güvenli erişimi için temel bağlantı loglarının (IP adresi, bağlantı zamanı) tutulması veya görevlerini teslim ettiği bir proje yönetim platformundaki aktivite kayıtları, sözleşmenin ifası için gerekli görülebilmektedir. Ancak, aynı tele çalışanın sürekli webcam ile izlenmesi, klavye hareketlerinin detaylı kaydedilmesi veya özel yazılımlarla tüm ekran aktivitelerinin anlık ve kapsamlı takibi gibi müdahaleci yöntemlerin, iş sözleşmesinin özünü oluşturan temel edimlerin (örneğin, bir rapor yazmak, yazılım geliştirmek, müşteri danışmanlığı yapmak) ifası

---

[529] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 454.

[530] Alman hukukunda, işe alım sürecindeki kişisel veri işleme faaliyetleri de iş ilişkisi kapsamında değerlendirilmekte olup, Bundesdatenschutzgesetz (BDSG) § 26/1 uyarınca hem çalışanların hem de iş başvurusunda bulunan adayların kişisel verilerinin işlenmesi aynı hukuki çerçevede düzenlenmiştir. Benzer şekilde, Türk hukukunda da KVKK'nın 5. maddesinin 2. fıkrasının (c) bendi uyarınca, bir sözleşmenin kurulmasına yönelik adımlar kapsamında adayın kişisel verilerinin işlenmesi ile mevcut işçinin verilerinin işlenmesi aynı hukuki dayanak altında değerlendirilmektedir. Ayrıntılı bilgi için bknz. Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 71-93.

[531] Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 185-203.

için objektif olarak zorunlu olduğu savunması genellikle zayıf kalacaktır[532]. Eğer işin temel edimi bu tür bir izleme olmaksızın da etkin bir şekilde yerine getirilebiliyorsa, söz konusu izleme faaliyeti sözleşmenin ifası için gerekli sayılamaz ve bu hukuka uygunluk sebebine dayandırılamaz. İşveren, bir izleme yönteminin sözleşmenin ifası için gerekli olduğunu iddia ediyorsa, aynı amaca daha az müdahaleci bir yolla ulaşılamayacağını da ortaya koymalıdır[533]. Bu durum, ilerleyen bölümde ayrıntılı olarak ele alınacak olan ölçülülük ilkesinin, gereklilik testinin ayrılmaz bir parçası olduğunu göstermektedir. Ayrıca, işverenlerin tele çalışma sözleşmelerine çalışanın izleneceğine dair genel bir madde eklemesi, bu izlemeyi otomatik olarak sözleşmenin ifası için gerekli kılmayacak; gereklilik değerlendirmesi objektif kriterlere göre yapılmalı, sözleşmeye keyfi olarak eklenen ve çalışanın temel haklarını orantısız şekilde kısıtlayan izleme hükümleri bu hukuka uygunluk sebebine dayandırılamayacaktır.

Sözleşmenin sona ermesinden sonra kişisel verilerin saklanmasına ilişkin yükümlülük, KVKK'nın 4. maddesinin 2. fıkrasında düzenlenen, *"kişisel verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi"* ilkesine dayanmaktadır. Bu doğrultuda, kişisel veriler ancak belirli bir süreyle sınırlı olarak saklanabilir; bu sürenin sona ermesiyle birlikte verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekmektedir[534]. Sürenin belirlenmesinde ise ilgili özel mevzuatlar dikkate alınmalıdır. Örneğin, İş Kanunu'nun Ek 3. maddesi uyarınca, iş sözleşmesinden kaynaklanan yıllık izin ücreti ile kıdem tazminatı, bildirim şartına uyulmaksızın fesih nedeniyle doğan tazminat, kötüniyet tazminatı ve eşit davranma ilkesine aykırı feshe bağlı tazminatlar bakımından zamanaşımı süresi beş yıl olarak belirlenmiştir[535].

GDPR'ın 88. maddesi ise üye devletlere iş ilişkileri bağlamında çalışanların kişisel verilerinin işlenmesine yönelik daha spesifik kurallar getirme (örneğin, toplu iş

---

[532] Jeremias Adams-Prasslt, "What If Your Boss Was An Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work", *Comp. Lab. L. & Pol'y J.* 41, sy 123 (2019): 141.
[533] Falque-Pierrotin, *Opinion 2/2017 on Data Processing at Work*, 13-15.
[534] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 264-65; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 205.
[535] Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 175.

sözleşmeleri aracılığıyla) imkânı tanımaktadır.[536]. Bu, ulusal düzeyde işçi verilerinin korunmasına yönelik ek güvenceler sağlanabileceği anlamına gelmektedir.

4.2.1.5. Hukuki Yükümlülüğün İfası için Zorunlu Olması

KVKK'nın 5. maddesinin 2. fıkrasının (ç) bendine göre, *"veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri işlemenin zorunlu olması"* bir diğer hukuka uygunluk sebebidir. Bu hüküm, işverenin, iş ilişkisinden doğan ve kamu hukuku veya özel hukuk kaynaklı çeşitli yükümlülüklerini yerine getirebilmesi adına kişisel veri işleyebilmesine hukuki dayanak sağlamaktadır[537].

GDPR 6. maddesinin 1. fıkrasının (c) bendi, işlemenin *"veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uyması için gerekli olması"* hâlinde hukuka uygun olacağını belirtmektedir. GDPR 6. maddesinin 3. fıkrası, bu yasal yükümlülüğün Birlik veya üye Devlet hukukunda belirtilmesi gerektiğini ve bu yasal dayanağın işleme amacını da belirlemesi gerektiğini ifade etmektedir. Ayrıca, söz konusu yasal düzenlemenin bir kamu yararı amacını karşılaması ve güdülen meşru amaçla orantılı olması gerekmektedir[538]. GDPR Başlangıç bölümü 45. maddesine göre her bir işleme faaliyeti için ayrı bir kanun olmasını gerektirmez; genel bir kanuni düzenleme de belirli işleme faaliyetleri için yasal zemin oluşturmaktadır[539].

Eğer yasal yükümlülük, özel nitelikli kişisel verilerin (örneğin sağlık verileri) işlenmesini gerektiriyorsa, durum daha da hassaslaşmaktadır. KVKK'nın 6. maddesinin 3. fıkrasının (f) bendi *"İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması"* hâlinde özel nitelikli verilerin işlenmesine izin vermektedir[540]. Benzer şekilde, GDPR 9. maddesinin 2. fıkrasının (b) bendi, işlemenin *"veri sorumlusunun veya veri sahibinin istihdam ve sosyal güvenlik ve sosyal koruma hukuku alanındaki yükümlülüklerinin yerine getirilmesi ve özel haklarının*

---

[536] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 304.
[537] Güler, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Kişisel Verilerinin Korunması", 55.
[538] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 79-80.
[539] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 81.
[540] Kaya, *KVKK Reformu 2024 Değişiklikleri*, 20-23.

kullanılması amacıyla gerekli olması ve Birlik veya Üye Devlet hukuku veya Üye Devlet hukukuna tabi toplu sözleşmeler tarafından veri sahibinin temel hakları ve menfaatleri için uygun güvenceler sağlanması kaydıyla yetkilendirilmiş olması halinde" özel nitelikli verilerin işlenmesine olanak tanımaktadır[541].

İşverenin yasal yükümlülükleri kapsamında veri işlemesi, özellikle iş hukukundan ve diğer ilgili mevzuatlardan doğan sorumlulukların ifası sırasında gündeme gelmektedir. Örneğin, iş sağlığı ve güvenliği önlemlerinin alınması, Sosyal Güvenlik Kurumu'na bildirim yapılması, ücret bordrosunun tutulması veya çalışma izinlerinin takibi gibi hususlar, işverenin kamu otoritelerine karşı yükümlülüklerini yerine getirmesi açısından kişisel veri işlemeyi gerekli kılmaktadır[542].

Tele çalışma bağlamında da işverenin iş sağlığı ve güvenliği önlemlerini alma, ücret ve sosyal güvenlik primlerini doğru hesaplama, veri güvenliğini sağlama gibi yasal yükümlülükleri devam etmektedir. Ancak, bu genel yasal yükümlülüklerin, İkinci Bölüm'de detaylandırılan türden müdahaleci izleme ve gözetleme yöntemlerinin (sürekli ekran kaydı, klavye hareketlerini izleme, özel yazılımlarla anlık aktivite takibi vb.) kullanılmasını zorunlu kılıp kılmadığı dikkatle değerlendirilmelidir[543]. Kural olarak, bir yasal yükümlülüğün varlığı, işverene otomatik olarak çalışanlarını her türlü yöntemle izleme hakkı vermemektedir. İzleme faaliyetinin bu hukuka uygunluk sebebine dayandırılabilmesi için, belirli bir izleme yönteminin kullanılmasının o yasal yükümlülüğün yerine getirilmesi için objektif olarak zorunlu olması ve daha az müdahaleci bir alternatifin bulunmaması gerekmektedir[544]. Örneğin, işverenin tele çalışanın iş sağlığı ve güvenliğini sağlama yükümlülüğü bulunmaktadır. Fakat bu yükümlülük, işverenin tele çalışanın ev ortamını sürekli webcam ile izlemesini veya sağlık durumunu giyilebilir cihazlarla anlık takip etmesini genellikle zorunlu kılmamaktadır[545]; işveren bu yükümlülüğünü çoğunlukla bilgilendirme, eğitim,

---

[541] Feiler vd., The EU General Data Protection Regulation (GDPR), 92.
[542] Elbir, "Kişiliğinin Korunması Bağlamında İşçiye Ait Kişisel Verilerin Korunması", 276-77; İnci Alfar, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Veri İşleme Sözleşmeleri" (Doktora Tezi, Dokuz Eylül Üniversitesi, 2024), 182.
[543] Adams-Prasslt, "What If Your Boss Was An Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work", 141.
[544] Küzeci, Kişisel Verilerin Korunması Hukuku, 236-37; Yiğit Efe Limoncuoğlu, "İşçiye Ait Kişisel Verilerin Korunması" (Yayınlanmamış Yüksek Lisans Tezi, İzmir Ekonomi Üniversitesi, 2022), 125.
[545] Falque-Pierrotin, *Opinion 2/2017 on Data Processing at Work*, 17-18.

ergonomik kontrol listeleri veya rızaya dayalı sanal değerlendirmeler gibi daha az müdahaleci yollarla yerine getirebilmektedir. Bununla birlikte, tele çalışanların hassas şirket verilerine uzaktan eriştiği durumlarda, işverenin KVKK'nın 12. maddesi kapsamındaki veri güvenliğini sağlama yükümlülüğü, belirli ve sınırlı teknik izleme tedbirlerini (örneğin, kurumsal cihazlara yönelik güvenlik yazılımları, sistem erişim loglarının tutulması, veri sızıntısı önleme (DLP) sistemlerinin kullanımı gibi) alınmasını gerektirebilmektedir[546]. Ancak bu tür bir izleme dahi, her zaman amaçla sınırlı, ölçülü ve şeffaf olmalıdır.

İşverenin yargı mercileri önünde kendini savunabilmesi için delil sunma yükümlülüğü de veri işleme faaliyetlerini meşrulaştıran bir diğer hukuki zorunluluktur[547]. Nitekim, bir işe iade davasında işçinin yıllık izinlerini kullandığını veya ücretinin eksiksiz ödendiğini ispatlamak isteyen işverenin, bu amaçlarla daha önce hukuka uygun olarak toplanmış ve saklanmakta olan kişisel verileri mahkemeye sunması, bu kapsamda değerlendirilmelidir[548]. Bu durum, mevcut kayıtların yasal bir süreçte kullanılmasına işaret etmekte, bu kayıtların en başta belirli bir izleme yöntemiyle toplanmasının yasal bir zorunluluk olduğu anlamına gelmemektedir.

---

[546] Bknz. Bölüm 3.5.1.

[547] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 246.

[548] Yeliz Bozkurt Gümrükçüoğlu, "Kişisel Verilerin Korunması Kanunu'nun İş Sağlığı Ve Güvenliği Alanındaki Etkileri", *9. Uluslararası İş Sağlığı Güvenliği Kongresi, Bildiri Tam Metinleri Kitabı* 2 (2018): 811-23. İş sağlığı ve güvenliği mevzuatında yer alan özel düzenlemeler, kişisel verilerin saklanma sürelerine ilişkin çeşitli yükümlülükler öngörmektedir. Örneğin, Kanserojen veya Mutajen Maddelerle Çalışmalarda Sağlık ve Güvenlik Önlemleri Hakkında Yönetmelik madde 17 uyarınca, bu maddelere maruziyetle ilgili kayıtlar, maruziyetin sona ermesinden sonra en az 40 yıl süre ile saklanmaktadır. Benzer şekilde, Biyolojik Etkenlere Maruziyet Risklerinin Önlenmesi Hakkında Yönetmelik uyarınca tutulan kişisel tıbbi kayıtların maruziyetin son bulmasından sonra genel olarak en az 15 yıl saklanması gerekmekte ; kalıcı veya gizli enfeksiyona neden olduğu bilinen, hastalığın gelişmesinden önce uzun kuluçka dönemi olan veya uzun süreli ciddi hasar bırakabilen enfeksiyonlara sebep olan biyolojik etkenlere maruziyet durumunda ise maruz kalan çalışanların listesi, bilinen son maruziyetten sonra en az 40 yıl boyunca saklanmaktadır. Daha genel bir yükümlülük olarak, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 86. maddesi, işverenlerin işyeri defter, kayıt ve belgelerini ilgili olduğu yılı takip eden yıl başından başlamak üzere 10 yıl süreyle saklamasını zorunlu kılmaktadır. Farklı bir alanda, Özel İstihdam Büroları Yönetmeliği'nin 25. maddesi gereğince, bu bürolar belirli belge ve bilgileri düzenleme tarihini izleyen takvim yılı başından itibaren beş yıl süreyle saklamakla yükümlü bulunmaktadır. Maden işyerlerine özgü olarak ise, Maden İşyerlerinde İş Sağlığı ve Güvenliği Yönetmeliği uyarınca, yeraltında çalışanların giriş-çıkışlarının ve bulundukları yerlerin takibine ilişkin sistem tarafından tutulan kayıtlar en az bir yıl süreyle saklanmaktadır. Ayrıntılı bilgi için bknz. Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 171-75.

4.2.1.6. İlgili Kişi Tarafından Alenileştirmiş Olması

KVKK'nın 5. maddesinin 2. fıkrasının (d) bendi kişisel verinin işçi tarafından alenileştirilmiş olması düzenlenmiş olup, özel nitelikli kişisel veriler için ise 2024 yılında yapılan değişiklikle KVKK'nın 6. maddesinin 3. fıkrasının (ç) bendinde *"ilgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması"* şeklinde düzenlenmiştir. Ancak bu istisnai düzenlemenin uygulanabilirliği, belirli ve sıkı şartların birlikte gerçekleşmesine bağlı olup, veri sorumlularına keyfî veri işleme imkânı tanımamaktadır[549]. Görüldüğü üzere, yeni düzenlemede alenileştirme iradesine uygunluk unsuru ön plana çıkarılmıştır[550]. Nitekim, önceki düzenleme döneminde de KVKK'nın 5. madde kapsamında öğretide verilerin alenileştirme iradesiyle uyumlu şekilde işlenmesinin hukuka uygunluğu savunulmakta idi[551]. Kanaatimizce bu bağlamda KVKK'nın 5. madde kapsamında işlenen genel nitelikteki verilerde de alenileştirme iradesine uygunluğun aranması gerekmektedir.

GDPR'da benzer bir istisna daha sınırlı bir kapsamda ele alınmaktadır. GDPR 9. maddesinin 2. fıkrasının (e) bendinde, yalnızca özel nitelikli kişisel verilerin işlenmesinin, *"işlemenin, veri sahibi tarafından açıkça kamuya açıklanmış (manifestly made public by the data subject) kişisel verilerle ilgili olması"* hâlinde hukuka uygun olacağını belirtilmiştir[552]. Genel nitelikli verilere ilişkin bu yönde bir düzenleme ihdas etmemiştir.

İlgili düzenlemenin temel mantığı, kişinin kendisi tarafından kamuya açıklanan verilerin artık özel bir koruma alanı içinde değerlendirilmeyeceği varsayımına dayanmaktadır. Nitekim kişi, bu verileri belirli bir amaca matuf olarak kamuya açık hâle getirdiğinde, bu verilerin belirli sınırlar dâhilinde işlenmesine kendi iradesiyle imkân tanımış sayılmaktadır[553]. Ancak burada dikkate alınması gereken ilk ve en temel koşul; alenileştirmenin bizzat ilgili kişi tarafından ve serbest irade ile gerçekleştirilmiş

---

[549] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 388; Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 247; Dülger, *Kişisel Verilerin Korunması Hukuku*, 300; Güler, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Kişisel Verilerinin Korunması", 52-54.
[550] Kaya, *KVKK Reformu 2024 Değişiklikleri*, 18.
[551] Dülger, *Kişisel Verilerin Korunması Hukuku*, 301.
[552] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 92.
[553] Ayşe Nida Günal ve Yasin Üstün, "İş İlişkilerinde Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebebi Olarak 'Meşru Menfaat'", *Kişisel Verileri Koruma Dergisi* 4, sy 2 (2022): 6-7.

olmasıdır. İşçinin bilgisi veya rızası olmadan üçüncü kişilerce kamuya ifşa edilen veriler, bu kapsamda değerlendirilemez[554].

İkinci olarak, kişisel verilerin alenileştirilmiş olması, bu verilerin her koşulda ve sınırsız biçimde işlenebileceği anlamına gelmemektedir. Veri işleme faaliyeti, alenileştirme iradesiyle sınırlı olmalı ve bu iradeyle uyumlu bir amaç doğrultusunda gerçekleştirilmelidir[555]. Aksi takdirde, veri sorumlusunun veri üzerindeki tasarrufu hukuka aykırı hâle gelir. 2024 yılında yapılan değişiklikle birlikte, özel nitelikli kişisel verilerin işlenmesinde, ilgili kişinin verisini alenileştirmiş olması tek başına yeterli sayılmamış; ayrıca bu alenileştirmenin iradesine uygun bir şekilde kullanılması gerektiği vurgulanmıştır[556]. Buna karşılık, KVKK'nın 5. maddesi kapsamında alenileştirilmiş nitelikteki kişisel verilerin işlenmesinde de benzer şekilde alenileştirme amacına sadık kalınması aranmaktadır[557].

Tele çalışma modelinde, bu hukuka uygunluk sebebi, işverenin aktif izleme ve gözetleme yöntemlerini (örneğin, özel yazılımlarla ekran kaydı alma, webcam izleme gibi) meşrulaştırmak için genellikle uygun bir dayanak değildir. Zira bu yöntemler, çalışanın alenileştirmediği, özel kabul edilen faaliyetlerine ve verilerine erişim anlamına gelmektedir. Ancak, bir tele çalışanın kendi isteğiyle kamuya açık hâle getirdiği profesyonel sosyal medya profilleri (örneğin LinkedIn), kişisel web sitesinde veya blogunda yayınladığı mesleki içerikler ya da katıldığı herkese açık çevrim içi forumlardaki işle ilgili yorumları gibi veriler, işveren tarafından alenileştirme iradesiyle uyumlu olduğu ölçüde (örneğin, çalışanın mesleki yetkinliklerini ve güncel çalışmalarını takip etmek veya sektördeki temsil yeteneğini anlamak amacıyla) işlenebilmektedir[558]. Burada dahi, KVKK 6. maddesinin 3. fıkrasının (ç) bendindeki alenileştirme iradesine uygunluk ve genel veri koruma ilkeleri kritik önem

---

[554] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 247.
[555] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 388-89.
[556] Kaya, *KVKK Reformu 2024 Değişiklikleri*, 17.
[557] Nafiye Yücedağ, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 75, sy 2 (2017): 780-81; Şehriban İpek Aşıkoğlu, "Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebepleri", içinde Türk Hukukunun Avrupa Birliği Hukukuna Uyumu Özel Hukuk-Acquis Communautaire'in Alınması-Açıklamalar, Değerlendirmeler, ed. Arslan Kaya vd. (Istanbul University Press, 2020), 1073; Küzeci, Kişisel Verilerin Korunması Hukuku, 399; KVKK, "'Alenileştirme' Hakkında Kamuoyu Duyurusu", KİŞİSEL VERİLERİ KORUMA KURUMU, 16 Aralık 2020, https://www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU.
[558] Falque-Pierrotin, Opinion 2/2017 on Data Processing at Work, 11.

taşımaktadır. Tele çalışanın kişisel ve profesyonel yaşamının dijital ortamlarda daha fazla iç içe geçtiği günümüz koşullarında, hangi sosyal medya paylaşımının veya çevrim içi aktivitenin işle ilgili alenileştirme kapsamında olduğu, hangisinin özel hayatın bir parçası olarak değerlendirilmesi gerektiği ayrımı daha da önem kazanmaktadır. İşveren, çalışanın tamamen kişisel nitelikteki ve işle doğrudan ilgisi olmayan alenileştirdiği verileri (örneğin, özel hobilere, aile yaşamına ilişkin paylaşımlar), bu hukuka uygunluk sebebine dayanarak işleyemez[559]. Örneğin, bir tele çalışanın herkese açık bir sosyal medya hesabında kişisel bir tatil fotoğrafı paylaşması, işverene bu fotoğrafı veya buradan elde edilecek konum verisini işleme hakkı vermez. Zira burada alenileştirme iradesi, işle ilgili bir amaç taşımamaktadır ve profesyonel kimliğin bir parçası değildir.

4.2.1.7. Bir Hakkın Tesisi, Kullanılması veya Korunması için Zorunlu Olması

KVKK'nın 5. maddesinin 2. fıkrasının (e) bendi ve KVKK'nın 6. maddesinin 3. fıkrasının (d) bendinde düzenlenen, "*bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması"* durumu bir başka hukuka uygunluk sebebini oluşturmaktadır[560]. Bu hüküm uyarınca, veri sorumlusunun kişisel verileri işlemesi, ancak hukuken korunmaya değer bir hakkın tesisi, kullanılması ya da korunması amacıyla ve gerçekten zorunlu olduğu ölçüde mümkündür. Söz konusu hak, yalnızca veri sorumlusuna ait olmak zorunda olmayıp, üçüncü kişilere ait hakların korunması amacıyla da veri işlenebilir[561]. Hakkın türü ya da dayandığı kaynak bakımından herhangi bir sınırlama öngörülmemiştir; önemli olan, veri işleme faaliyetinin açıkça bu amaçla bağlantılı ve gerekli olmasıdır[562].

GDPR da benzer bir amaca hizmet eden hukuka uygunluk sebepleri öngörmektedir. Ancak bu düzenlemeyi, genel ve özel nitelikli veriler için farklı maddeler altında gerçekleştirmektedir. Genel nitelikteki kişisel veriler açısından, GDPR 6. maddesinin 1. fıkrasında, KVKK'nın 5. maddesinin 2. fıkrasının (e) bendi ile birebir örtüşen ayrı

---

[559] Uncular, İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, 150.
[560] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 247; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 399-400; Dülger, *Kişisel Verilerin Korunması Hukuku*, 304-5; Günal ve Üstün, "İş İlişkilerinde Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebebi Olarak 'Meşru Menfaat'", 6.
[561] Dülger, *Kişisel Verilerin Korunması Hukuku*, 304.
[562] Manav, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", 104-5.

bir hukuka uygunluk sebebi bulunmamakla birlikte, bir hakkın tesisi, kullanılması veya korunması genellikle GDPR 6. maddesinin 1. fıkrasının (f) bendi kapsamında veri sorumlusunun meşru menfaatleri çerçevesinde değerlendirilmektedir[563]. Bu durumda, veri sorumlusunun hakkını tesis etme, kullanma veya koruma yönündeki meşru menfaati ile veri sahibinin temel hak ve özgürlükleri arasında bir denge testi yapılması gerekmektedir. Özel nitelikli kişisel veriler söz konusu olduğunda ise, GDPR 9. maddesinin 2. fıkrasının (f) bendi çok daha doğrudan bir paralellik sunmakta ve *"işlemenin, hukuki iddiaların tesisi, kullanılması veya savunulması için gerekli olması veya mahkemelerin yargısal görevlerini yerine getirmeleri durumunda"* özel nitelikli verilerin işlenmesine izin vermektedir[564]. Bu durum, KVKK'nın genel yaklaşımıyla önemli ölçüde paralellik göstermektedir.

Her iki düzenlemede de zorunlu (KVKK) veya gerekli (GDPR) olma kriteri, işleme faaliyetinin keyfi olmamasını ve amaçla sınırlı kalmasını temin etmektedir. Bu hukuka uygunluk sebebi, tele çalışma modelinde işverenin etkin ve kapsamlı izleme faaliyetleri başlatmasını genellikle tek başına meşrulaştırmamaktadır. Bir hakkın tesisi, kullanılması veya korunması amacı, çoğunlukla mevcut olan veya başka bir hukuka uygun sebebe (örneğin sözleşmenin ifası, yasal yükümlülük) dayanılarak toplanmış verilerin, belirli bir hukuki ihtilaf veya somut bir hak talebi durumunda işlenmesini (özellikle saklanmasını veya bir yasal süreçte delil olarak kullanılmasını) zorunlu kılabilir. Ancak, kanaatimizce gelecekte olası bir hukuki uyuşmazlığa karşı genel bir önlem olarak tele çalışanların sürekli ve müdahaleci yöntemlerle izlenmesi, zorunluluk, ölçülülük ve amaçla sınırlılık ilkeleriyle bağdaşmayacaktır.

Söz konusu hukuka uygunluk sebebine dayanılabilmesi için, işverenin tesis etmeyi, kullanmayı veya korumayı amaçladığı hakkın somut olması ve bu hakka yönelik gerçek veya yakın bir tehdidin bulunması gerekmektedir. Örneğin, evden tele çalışan bir işçinin günlük çalışma sürelerine veya dijital sistemlere erişim zamanlarına ilişkin daha önce başka meşru bir amaçla (örneğin, ücret hesaplaması için sözleşmenin ifası kapsamında) toplanmış ve tutulmakta olan kayıtların, işverenin ileride doğabilecek bir hukuki uyuşmazlıkta (örneğin, fazla çalışma alacağına ilişkin bir davada) savunma

[563] Feiler vd., The EU General Data Protection Regulation (GDPR), 79.
[564] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 92.

hakkını kullanabilmesi amacıyla saklanmaya devam edilmesi bu kapsamda değerlendirilebilir. Ancak, sırf olası bir alacak davasına karşı önlem almak amacıyla, normalde gerekmeyen detayda ve sıklıkta bir aktivite izleme yazılımı kullanmak bu hukuka uygunluk sebebine dayandırılamaz[565].

Benzer bir ilke, işçinin sadakat borcunu esaslı şekilde ihlal ettiğine yönelik şüphelerin ortaya çıktığı durumlarda da geçerlidir. Bir tele çalışanın ticari sırları rakip bir firmaya sızdırdığına dair güçlü ve somut şüphelerin varlığı, işveren açısından hem meşru menfaatini koruma hakkını doğurmakta hem de iş hukukunda "şüphe feshi" için zemin hazırlamaktadır. Feshin geçerli sayılabilmesi için son çare (ultima ratio) ilkesi gereği, işverenin fesih öncesinde şüpheyi aydınlatma yükümlülüğü bulunmaktadır[566]. Bu doğrultuda işverenin, ticari sırların korunması gibi yasal haklarını ispatlamak amacıyla, sadece şüpheyle sınırlı, belirli bir zaman dilimini kapsayan ve hedefe yönelik (örneğin, ilgili çalışanın kurumsal e-posta trafiğinin incelenmesi gibi) bir araştırma yapması meşru görülebilmektedir[567]. Ancak burada dahi, müdahalenin meşruiyeti tehdidin somutluğuyla orantılı olmalıdır. Soyut bir koruma amacı güderek tüm çalışanların iletişimini sürekli taramak, ölçülülük ilkesinin açık bir ihlali olacağından, bu yolla elde edilen bulgulara dayalı bir şüphe feshini geçersiz kılmaktadır.

4.2.1.8. Veri Sorumlusunun Meşru Menfaatleri için Zorunlu Olması

KVKK'da düzenlenen veri işleme şartlarından biri de 5. maddenin 2. fıkrasının (f) bendi uyarınca, *"ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlemenin zorunlu olması"* hâlidir. GDPR 6. maddesinin 1. fıkrasının (f) bendiyle doğrudan paralellik göstermektedir[568]. GDPR'ın ilgili hükmü, işlemenin *"veri sorumlusunun veya üçüncü bir tarafın meşru menfaatlerinin amaçları için gerekli olması, ancak veri sahibinin kişisel verilerinin*

---

[565] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 209.
[566] Ulaş Baysal, "Şüphe Feshi Kavramı ve Bu Konuda Yargıtay Kararlarının Hukuki Değerlendirilmesi", *Sicil İş Hukuku Dergisi*, sy 35 (2016): 86; Ece Sıla Hafizoğlu, "İş İlişkisinde Şüphe ve Şüphe Feshi (Alman Hukuku ile Karşılaştırmalı)" (Doktora Tezi, Dokuz Eylül Üniversitesi, 2022), 15.
[567] Bknz. *Case of Libert V. France*.
[568] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 248; Ömer Ekmekçi vd., *Anayasa Mahkemesine bireysel başvurunun temel esasları ve iş ve sosyal güvenlik hukukuna ilişkin kararlar* (On İki Levha Yayıncılık, 2022), 215.

korunmasını gerektiren menfaatlerinin veya temel hak ve özgürlüklerinin, özellikle veri sahibi bir çocuk ise, bu menfaatlere üstün gelmemesi kaydıyla" hukuka uygun olacağını belirtmektedir[569]. Her iki düzenleme de bu hukuka uygunluk sebebini iş ilişkilerinde sıkça başvurulan bir dayanak olarak kabul etmekle birlikte, uygulanmasını katı koşullara bağlamıştır. Özellikle işverenin yönetim hakkını kullanırken çalışma düzenini sağlamak, verimliliği artırmak, mal varlığını korumak veya hukuki riskleri yönetmek gibi menfaatlerini gerçekleştirmek amacıyla gerçekleştirdiği kişisel veri işleme faaliyetleri, çoğu zaman bu hüküm çerçevesinde gerekçelendirilmektedir[570]. İşverenin meşru menfaatine dayanarak kişisel veri işlemesi, ona sınırsız ve mutlak bir yetki tanımaz; bu hukuka uygunluk sebebine başvurulabilmesi, için ayrıca veri koruma ilkelerine de uyulması gerekmektedir[571]. Ek olarak veri işleme süreci, ilgili kişinin temel hak ve özgürlüklerine ölçüsüz bir müdahaleye yol açmamalı ve Anayasa ile güvence altına alınan kişilik haklarıyla bağdaşır nitelikte olmalıdır. Bu kapsamda, işverenin meşru menfaati ile işçinin temel hak ve özgürlükleri arasında makûl, adil ve orantılı bir denge kurulması zorunludur. Aksi hâlde, yani işçinin hak ve özgürlükleri işverenin menfaatine üstün geldiği durumda, veri işleme faaliyeti hukuka aykırı sayılacak ve hem KVKK hem de GDPR kapsamında korunmayacaktır[572].

İşverenin ekonomik varlığını sürdürebilmesi, işyerinde güvenliğin sağlanması (örneğin, GDPR, Başlangıç bölümü 47. maddesinde dolandırıcılığın önlenmesi meşru bir menfaat olarak geçer), mülkiyetinin korunması ve ticari sırlarının açığa çıkmasının önlenmesi gibi amaçlar, meşru menfaat kapsamında değerlendirilebilir. Meşru menfaati "hayali veya spekülatif" olmamalı, gerçek ve mevcut bir tehlikeye

---

[569] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 216; Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 79.
[570] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 248-50.
[571] Örnek olarak Kurul bir kararında, 5015 sayılı Petrol Piyasası Kanunu kapsamındaki yasal yükümlülük çerçevesinde işlenen araç plaka verilerinin, meşru menfaat gerekçesiyle ikinci bir amaç olan "Araç Tanıma Projesi" kapsamında kullanılmasına ilişkin başvuruyu değerlendirirken; veri işleme faaliyetinin meşru menfaate dayandırılabilmesi için zorunluluk, temel haklarla denge ve genel ilkelere uygunluk gibi şartların birlikte sağlanması gerektiğini vurgulamıştır. Somut olayda hatalı yakıt dolumlarının önlenmesinin şirketin meşru ve orantılı menfaatleri kapsamında olduğuna karar verilmiş ve açık rıza olmaksızın kullanımına, aydınlatma yükümlülüğünün yerine getirilmesi şartıyla izin verilmiştir. Bknz. Kişisel Verileri Koruma Kurulu, 25.03.2019 tarih ve 2019/78 sayılı karar, erişim 09.06.2026, https://www.kvkk.gov.tr/Icerik/5434/2019-78.
[572] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 248.

dayanmalıdır[573]. GDPR, Başlangıç bölümü 47. maddesi ayrıca, veri sahibi ile veri sorumlusu arasında, veri sahibinin veri sorumlusunun bir müşterisi veya çalışanı olduğu durumlar gibi ilgili ve uygun bir ilişkinin bulunduğu hâllerde meşru menfaatin söz konusu olabileceğini belirtmektedir[574]. Ancak bu çıkarların gerçekten korunmaya değer olup olmadığı ve denge testini geçip geçmediği somut olayın özelliklerine göre değerlendirilmeli, işçinin temel hak ve özgürlükleriyle orantılı olmalıdır. Nitekim sadece ekonomik nitelikli yararların, özellikle işçinin özel hayat hakkına müdahale söz konusu olduğunda, kendiliğinden üstün meşru yarar olarak kabul edilmeyeceği her iki hukuki çerçevede de geçerli bir yaklaşımdır. Bu noktada işçinin korunması ilkesi ve özel hayat hakkının temel hak niteliği birlikte değerlendirilmelidir.

İşverenin özel hayata müdahale içeren uygulamalarının meşru sayılması için sadece ekonomik gerekçelerin yeterli görülmemesi gerekmektedir. Müdahalenin hukuka uygunluğu, ekonomik nedenlerin yanı sıra, işçinin sadakat borcu ve dürüstlük kuralı kapsamında bu tür müdahalelere katlanmasının beklenip beklenemeyeceği açısından da değerlendirilmesi gerekmektedir[575]. Aksi hâlde, işverenin ekonomik çıkarlarının kamu yararı kisvesi altında genişletilmesi ve işçinin özel hayatına ölçüsüz bir müdahaleye zemin hazırlanması söz konusu olacaktır. Bu sebeple müdahale, amacına ulaşmak için gerekli, uygun ve işçinin özel hayatını mümkün olduğunca az etkileyen biçimde (yani, orantılılık ve veri minimizasyonu ilkelerine uygun olarak) gerçekleştirilmelidir[576].

Tele çalışma modelinde ise bu hukuka uygunluk sebebinin uygulanması daha da karmaşık ve hassas bir hâl almaktadır. İşverenler, tele çalışanların verimliliğini denetlemek, iş süreçlerinin etkinliğini sağlamak, kurumsal veri ve sistem güvenliğini korumak gibi meşru menfaatlere dayanabilmektedirler. Ancak, bu menfaatlerin özellikle evde tele çalışanın özel hayat alanında gerçekleştirilen izleme ve gözetleme faaliyetleriyle dengelenmesi kritik bir önem taşımaktadır. Tele çalışanın, fiziksel işyerine kıyasla evinde daha yüksek bir makûl gizlilik beklentisi bulunmaktadır. Bu nedenle, işçi ile işveren arasındaki menfaat dengesinin korunmasında çalışanın temel

[573] European Data Protection Board (EDPB), *Guidelines 3/2019 on Processing of Personal Data Through Video Devices*, Version 2.0 (2020), 10.
[574] Feiler vd., The EU General Data Protection Regulation (GDPR), 82.
[575] Sevimli, *İşçinin Özel Yaşamına Müdahalenin Sınırları*, 199-200.
[576] Ayrıntılı bilgi için bknz. Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 248-50.

hak ve özgürlükleri daha ağır basma eğiliminde olabilmekte ve işverenin meşru menfaatinin bu haklara üstün geldiğini ispatlaması daha da zorlaşmaktadır.

Tele çalışanın verimliliğini ölçmek amacıyla, sürekli aktif olan ve klavye hareketlerini, fare tıklamalarını, ziyaret edilen web sitelerini ve kullanılan uygulamaları detaylı bir şekilde kaydeden bir aktivite izleme yazılımının kullanılması, işverenin verimliliği artırma meşru menfaatine dayandırılsa bile, çalışanın özel hayatına ve veri minimizasyonu ilkesine orantısız bir müdahale teşkil etmektedir[577]. Bu tür bir izleme, çalışanda sürekli gözetlenme hissi yaratarak psikolojik baskı oluşturabilir ve gereklilik/zorunluluk testini geçmekte zorlanabilir; zira verimlilik genellikle daha az müdahaleci yöntemlerle (proje bazlı çıktı değerlendirmesi, belirli aralıklarla yapılan ilerleme toplantıları, net hedefler ve teslim tarihleri belirleme vb.) de ölçülebilir[578]. Buna karşılık, tele çalışanın şirket tarafından sağlanan bir cihaz üzerinden hassas müşteri verilerine veya ticari sırlara eriştiği durumlarda, işverenin veri güvenliğini sağlama ve veri sızıntılarını önleme yönündeki meşru menfaati, söz konusu cihaz üzerinde belirli ve sınırlı güvenlik izleme yazılımlarının kullanılmasını daha gerekçelendirilebilir kılabilir[579]. Her ne kadar bu düzenleme öncesinde de çalışanın sır saklama yükümlülüğü kapsamında işletme verilerini koruması gerektiği kabul edilmekteydiyse de Uzaktan Çalışma Yönetmeliği 11. maddesiyle bu duruma açık bir hukuki zemin kazandırmıştır. Bu durum, artık Yönetmelik kapsamında da bir hukuka uygunluk nedeni olarak kabul edilmektedir[580]. Ancak bu durumda dahi, izlemenin kapsamı (örneğin, sadece iş saatleri içinde ve işle ilgili aktivitelerle sınırlı olması), süresi, toplanan verilerin niteliği ve çalışanların bu konuda KVKK'nın 10. maddesi ve GDPR 13. ile 14. maddeleri uyarınca şeffaf bir şekilde bilgilendirilmesi ve özellikle GDPR 35. maddesi kapsamında bir Veri Koruma Etki Değerlendirmesi (DPIA) yapılması kritik önem taşımaktadır. Tele çalışmada sürekli webcam veya mikrofon kaydı gibi yöntemlerin meşru menfaate dayandırılması ise, bu yöntemlerin aşırı müdahaleci doğası ve çalışanın ev mahremiyetine yönelik kaçınılmaz ve ciddi ihlal

[577] Adams-Prasslt, "What If Your Boss Was An Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work", 141.
[578] Aída Ponce Del Castillo, *Artificial Intelligence, Labour and Society* (ETUI, 2024), 105.
[579] Falque-Pierrotin, Opinion 2/2017 on Data Processing at Work, 13.
[580] Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 17; Kandemir, *İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma*, 111; Ünal Adınır, "Tele çalışmada verilerin korunması", 991-93.

potansiyeli nedeniyle, denge testinde çalışanın haklarına açıkça üstün gelecek ve hukuka uygun bulunmayacaktır[581].

GDPR'ın Başlangıç bölümü 48. maddesi, bir teşebbüs grubuna veya merkezi bir kuruluşa bağlı kurumlara ait veri sorumlularının, grup içinde iç idari amaçlarla (müşteri veya çalışan verilerinin işlenmesi dâhil) kişisel veri aktarımında meşru menfaati olabileceğini de belirtmekte; ancak bu durumun da Tüzüğün diğer kurallarına uygun olmasını şart koşmaktadır[582]. Örneğin, iş ilişkileri kapsamında izleme ve gözetleme faaliyetleri söz konusu olduğunda, GDPR 25. madde uyarınca genellikle bir Veri Koruma Etki Değerlendirmesi yapılması ve GDPR 13. ve 14. maddelerinde düzenlenen şeffaflık ilkesi gereği çalışanların detaylı bir şekilde bilgilendirilmesi beklenmektedir[583].

4.2.1.9. Özel Nitelikli Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebepleri

Özel nitelikli kişisel veriler; bireylerin ırkı, etnik kökeni, siyasi düşüncesi, sağlığı ve cinsel hayatı gibi son derece hassas bilgilerini içermeleri ve işlenmeleri hâlinde kişiler hakkında ayrımcılık veya mağduriyete yol açma riski barındırmaları nedeniyle genel nitelikli kişisel verilerden daha sıkı bir koruma rejimine tabi tutulmuştur. Bununla birlikte, 12 Mart 2024 tarih ve 7499 sayılı Kanun ile KVKK'nın 6. maddesinde yapılan kapsamlı değişiklikler, uygulamada yaşanan sorunları gidermek ve Genel Veri Koruma Tüzüğü ile uyumu artırmak amacıyla özel nitelikli kişisel verilerin işlenme şartlarını yeniden düzenlemiştir. Bu reform, özel nitelikli kişisel veri işleme faaliyetlerini neredeyse tamamen açık rıza şartına sınırlayan eski yapıyı değiştirerek, alternatif hukuka uygunluk sebepleri ihdas etmiştir[584].

Yapılan değişiklik neticesinde, özel nitelikli kişisel verilerin işlenmesi yasağı ilkesi muhafaza edilmekle birlikte, bu verilerin işlenmesini mümkün kılan hukuki işleme

---

[581] Falque-Pierrotin, Opinion 2/2017 on Data Processing at Work, 21.
[582] Feiler vd., The EU General Data Protection Regulation (GDPR), 82.
[583] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 255, 367.
[584] Kaya, *KVKK Reformu 2024 Değişiklikleri*, 8 vd.; Gamze Turan Başara, "Kişisel Verilerin Korunması Kanunu'nun 6. Maddesinde Yapılan Değişiklik Bağlamında Özel Nitelikli Kişisel Verilerin İşlenmesi", *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 28, sy 4 (2024): 62 vd., 4.

sebepleri önemli ölçüde genişletilmiştir.[585] Yeni düzenleme uyarınca, ilgili kişinin açık rızasının yanı sıra; kanunlarda açıkça öngörülme, fiili imkânsızlık, ilgili kişi tarafından alenileştirme, bir hakkın tesisi, kullanılması veya korunması için zorunluluk gibi hâller, tüm özel nitelikli kişisel veriler için geçerli hukuki işleme sebepleri olarak kabul edilmiştir. Kanun koyucu bu değişikliklerle, KVKK'nın 5. ve 6. maddeleri arasında bir uyum sağlamış ve özel nitelikli olan ve olmayan veriler için benzer hukuki işleme temelleri oluşturmuştur[586].

Bu reformun getirdiği en önemli yeniliklerden biri, özellikle iş hukuku uygulamasında yaşanan tıkanıklıkları gidermeye yöneliktir. Bu kapsamda 6. maddenin 3. fıkrasında yapılan düzenlemeyle birlikte, *"(f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması"* hâlinde kişisel verilerin işlenmesi, açık rıza aranmaksızın hukuka uygun kabul edilmektedir[587]. Örneğin, bir işverenin, işçinin çalışma yeterliliğini denetleme yükümlülüğü kapsamında sağlık verilerini işlemesi veya işçinin adli sicil kaydını temin etmesi bu hukuka uygunluk sebebine dayandırılabilecektir. GDPR 9. maddesinin 2. fıkrasının (b) bendindeki benzer istisna ile paralellik göstermektedir ve işverenlerin bu tür verileri işlerken rızaya dayanma ihtiyacını azaltmaktadır, ancak her zaman temel veri koruma ilkelerine uyulması şarttır[588].

---

[585] Kaya, *KVKK Reformu 2024 Değişiklikleri*, 10 vd.; Turan Başara, "Kişisel Verilerin Korunması Kanunu'nun 6. Maddesinde Yapılan Değişiklik Bağlamında Özel Nitelikli Kişisel Verilerin İşlenmesi", 62 vd.

[586] Kanaatimizce bu paralellik, kanun koyucunun özel nitelikli kişisel verilere tanıdığı varsayılan "özel koruma" zırhını önemli ölçüde zayıflatmaktadır. Değişiklik sonrası, Kanun'un 5. ve 6. maddeleri arasındaki fark neredeyse tamamen ortadan kalkmış, bu durum özel nitelikli veri ayrımının pratik önemini büyük ölçüde azaltmıştır. Dahası, kanun yapma tekniği açısından bakıldığında, eğer amaç iki madde arasında tam bir uyum sağlamak idiyse, 6. maddenin yeni halinde 5. maddedeki şartların neredeyse birebir tekrar edilmesi yerine, doğrudan 5. maddeye atıf yapılması daha yalın ve etkili bir yöntem olabilirdi. Mevcut haliyle metin, gereksiz bir tekrara düşerek kanunun sistematiğini ve okunabilirliğini olumsuz etkilemektedir.

[587] Kaya, *KVKK Reformu 2024 Değişiklikleri*, 14.

[588] GDPR 9. maddesinin 2. fıkrasının (b) bendi; *"İşleme, Birlik hukuku ya da Üye Devlet hukuku uyarınca veya Üye Devlet hukukuna dayanılarak yapılan bir toplu iş sözleşmesi çerçevesinde yetkilendirilmiş olmak kaydıyla, istihdam, sosyal güvenlik ve sosyal koruma hukukunun alanında veri sorumlusunun ya da veri sahibinin yükümlülüklerini yerine getirmesi veya belirli haklarını kullanması amacıyla gerekli olduğu ölçüde ve veri sahibinin temel hakları ile menfaatlerine yönelik uygun güvenceleri sağlamak şartıyla gerçekleştirilebilir."* şeklinde düzenlenmiştir.

4.3. Temel İlkeler

Daha önce de ifade ettiğimiz üzere, veri işleme faaliyetinin hukuka uygun kabul edilebilmesi için yukarıda değerlendirilen hukuka uygunluk nedenlerinin varlığı, tek başına yeterli değildir. Ayrıca KVKK'nın 4. maddesinde sayılan ilkelere uyum sağlanması gerekmektedir. GDPR açısından da benzer bir durum geçerlidir. Tüzüğün 5. maddesinde düzenlenen temel ilkelere riayet edilmesi zorunludur. Gerek KVKK'nın 4. maddesi gerekse GDPR'ın 5. maddesi kişisel verilerin işlenmesine rehberlik eden ve uyulması zorunlu olan temel ilkeleri ortaya koymaktadır. Bu ilkeler, veri işleme faaliyetlerinin hukuki çerçevesini ve etik sınırlarını belirlemektedir.

KVKK'da sayılan ilkeler; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmedir. GDPR 5. maddesinin 1. fıkrasında belirtilenler de bu ilkelere büyük ölçüde paralellik göstermektedir. Bu düzenlemede sayılan ilkeler şunlardır:

> *(a) Hukuka uygunluk, dürüstlük ve şeffaflık (lawfulness, fairness and transparency),*
> *(b) Amaç sınırlaması (purpose limitation),*
> *(c) Veri minimizasyonu (data minimisation),*
> *(d) Doğruluk (accuracy),*
> *(e) Saklama sınırlaması (storage limitation),*
> *(f) Bütünlük ve gizlilik (integrity and confidentiality*).

GDPR, KVKK'dan farklı olarak *"hesap verebilirlik"* (accountability) ilkesini de açıkça düzenlemektedir[589]. Bu ilke, veri sorumlusunun yukarıda sayılan ilkelere uyduğunu ve bundan sorumlu olma yükümlülüğünü ifade etmektedir. KVKK'da "hesap verebilirlik" bu şekilde ayrı bir ilke olarak ifade edilmese de Kanun'un genel ruhundan ve veri sorumlusunun yükümlülüklerinden bu yönde bir beklenti doğurmaktadır[590]. Ayrıca, KVKK'nın 4. maddesinde düzenlenen genel "hukuka ve dürüstlük kurallarına uygun olma" ilkesinin ve 12. maddedeki veri güvenliği

[589] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 73.
[590] Serdar Çelikel, "Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri" (Doktora Tezi, Ankara Üniversitesi, 2021), 101-2.

yükümlülüklerinin, GDPR'da daha spesifik olarak ifade edilen şeffaflık, bütünlük ve gizlilik gibi temel ilkeleri de bünyesinde barındırmaktadır. Aşağıda veri işleme faaliyetinin hukuka uygun kabul edilmesi bakımından uyulması gereken ilkeler ayrı başlıklar altında tek tek incelenecektir.

4.3.1. Dürüstlük Kuralına ve Hukuka Uygun Olma

Kişisel verilerin işlenmesine ilişkin temel ilkelerden biri olan "dürüstlük kuralına ve hukuka uygun olma" ilkesi KVKK'nın 4. maddesinin 2. fıkrasının (a) bendinde düzenlenen ve tüm veri işleme faaliyetlerinin dayanmak zorunda olduğu genel ilkelerdendir. Bu ilke, yalnızca diğer veri işleme kurallarına kaynaklık etmekle kalmamakta, aynı zamanda kişisel veri koruma hukukunun normatif çatısını da oluşturmaktadır[591]. İş ilişkisinde ise bu ilke, işverenin işçiyi gözetme yükümlülüğü ile eşit davranma borcunun veri işleme süreçlerine yansıması açısından belirleyici bir işlev üstlenmektedir[592].

Hukuka uygun şekilde kişisel verilerin işlenmesi, yürürlükteki hukuki düzenlemelere, Anayasa'ya, KVKK'ya ve ilgili diğer kanunlara uygun hareket edilmesini gerektirmektedir[593]. Anayasa 20. maddesinin 3. fıkrasında açıkça belirtildiği üzere, kişisel veriler ancak kanunda öngörülen hâllerde veya kişinin açık rızasına dayanılarak işlenebilir. KVKK'da düzenlenen hukuka uygunluk sebepleri, anayasal çerçevenin bir yansımasıdır[594]. Ancak belirtelim ki, hukuka uygunluk yalnızca KVKK'ya uyum ile sınırlı değildir. İşverenin, işçilerin kişisel verilerini işlerken İş Kanunu, Türk Borçlar Kanunu, sosyal güvenlik mevzuatı gibi ilgili tüm normatif kaynaklara uyum göstermesi gerekmektedir. Örneğin, bir çalışanın sağlık verisinin işlenmesi KVKK'nın yanı sıra kişisel sağlık verilerine ilişkin diğer mevzuata ve iş sağlığı ve güvenliğine

---

[591] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 206; Dülger, *Kişisel Verilerin Korunması Hukuku*, 173; Furkan Güven Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 2. Baskı (On İki Levha Yayıncılık, 2017), 48.

[592] Sevimli, "Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419", 128; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 149.

[593] Gürsel, İşçinin Kişisel Verilerinin Korunması Hakkı, 211-12; Dülger, Kişisel Verilerin Korunması Hukuku, 173-74; Çekin, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 69-70; Küzeci, Kişisel Verilerin Korunması Hukuku, 206-7; Yiğit, İş İlişkisinde Kişisel Verilerin Korunması, 19.

[594] Berat Duman, "Anayasa Hukukunda Kişisel Verilerin Korunması" (Doktora Tezi, Selçuk Üniversitesi, 2020), 145-52.

ilişkin düzenlemelere uyumu zorunlu kılmaktadır. GDPR 5. maddesinin 1. fıkrasının (a) bendinde kişisel verilerin "hukuka uygun, dürüst ve şeffaf bir şekilde" (lawfully, fairly and in a transparent manner) işlenmesi gerektiğini belirterek benzer bir temel ilkeyi benimsenmiştir[595]. GDPR kapsamında kişisel verilerin işlenmesi GDPR 6. maddesi (genel veriler için) veya GDPR 9. maddesi (özel nitelikli veriler için) belirtilen hukuka uygunluk sebeplerinden en az birine dayanması gerekmektedir. Ayrıca, bu işlem GDPR'ın diğer ilgili hükümlerine ve yürürlükteki diğer Birlik veya üye devlet düzenlemelerine de uygunluk göstermelidir[596].

Tele çalışma modelinde, bir izleme faaliyetinin belirli bir hukuka uygunluk sebebine dayanması, onun her durumda hukuka uygun olduğu anlamına gelmemektedir. Eğer kullanılan izleme yöntemi (örneğin, çalışanın bilgisi ve rızası dışında evdeki özel konuşmaları da dolaylı olarak kaydedebilen sürekli mikrofon analizi veya özel yazışmalarına erişim sağlayan bir sistem)[597] aynı zamanda Anayasa ile korunan haberleşmenin gizliliğini veya özel hayatın gizliliğini orantısız bir şekilde ihlal ediyorsa ya da işçinin temel kişilik haklarına zarar veriyorsa, bu durum genel hukuka uygunluk ilkesine aykırılık teşkil edecektir[598].

Dürüstlük kurallarına uygun veri işleme ise TMK'nın 2. maddesinde yer alan dürüstlük kuralı ile yakından ilişkili olup, veri sorumlusunun makûl, öngörülebilir ve iyi niyetli davranmasını gerektirmektedir. GDPR 5. maddesinin 1. fıkrasının (a) bendindeki dürüstlük (fairness) ilkesi de benzer bir anlayışı yansıtmaktadır. Kişisel veri işlemenin veri sahipleri için beklenmedik, haksız veya aldatıcı olmaması gerektiğini ifade etmektedir[599]. Bu ilke doğrultusunda işverenin veri işlemesi; ilgili işçinin makûl beklentilerine uygun olmalı, öngörülebilir bir çerçevede gerçekleşmeli, temel hak ve özgürlüklerine zarar vermemelidir.

---

[595] Feiler vd., The EU General Data Protection Regulation (GDPR), 73.
[596] Dülger, Kişisel Verilerin Korunması Hukuku, 179-81; Dilanur Demir, "Kişisel Verilerin Korunması Kapsamında Unutulma Hakkı" (Yayınlanmamış Yüksek Lisans Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, 2023), 56.
[597] Annette Bernhardt vd., "The Data-Driven Workplace and the Case for Worker Technology Rights", *ILR Review* 76, sy 1 (2023): 19.
[598] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 61-66.
[599] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 73.

Tele çalışanın ev ortamında, işveren tarafından önceden tam olarak içeriği ve kapsamı açıklanmayan veya çalışanın makûl beklentilerinin ötesinde bir yoğunlukta (Örneğin, bireyin özel hayatına dair çıkarımlar yapabilen, iş dışındaki zamanlarını da kapsayan ve özel yazışmalarını tarayan yapay zekâ tabanlı gözetleme uygulamaları) bir dijital gözetim uygulanması, dürüstlük ilkesine aykırı olacaktır[600]. Çalışanın, evinde çalışırken dahi belirli bir mahremiyet beklentisi içinde olması makûldür ve işverenin bu beklentiyi zedeleyen, aldatıcı veya baskıcı izleme yöntemleri dürüstlük kuralını ihlal eder. Makûl beklenti, bir çalışanın, iş ilişkisinin doğası gereği hangi tür izlemelere katlanmayı beklemesi gerektiğiyle ilgilidir. Örneğin bir satış temsilcisi, satış rakamlarının takip edilmesini makûl olarak bekleyebilirken, aynı temsilci evindeki çalışma masasından sürekli webcam ile izlenmeyi makûl olarak beklememelidir[601].

Veri sorumlusunun şeffaf davranması ise dürüstlük ilkesinin doğal bir sonucudur. Şeffaflık, veri işlemenin ilgili kişiye önceden bildirilmesi, işleme amacının açıkça belirtilmesi ve ilgili kişinin haklarını kullanabilmesi için gerekli bilgilerin sunulması anlamına gelir[602]. KVKK'dan farklı olarak, GDPR 5. maddesinin 1. fıkrasının (a) bendi şeffaflık ilkesini açıkça ifade etmiştir[603] .Bununla birlikte, KVKK'da da şeffaflık, dürüstlük kuralının bir sonucu ve veri sorumlusunun aydınlatma yükümlülüğünün bir yansıması olarak değerlendirilebilmektedir. Şeffaflık, GDPR, Başlangıç bölümü 39. maddesi uyarınca, kişisel verileri işlenen gerçek kişilere, verilerinin toplandığı, kullanıldığı, danışıldığı veya başka bir şekilde işlendiği ve kişisel verilerin ne ölçüde işlendiği veya işleneceği konusunda bilgi verilmesi anlamına gelmektedir[604]. Ayrıca bilgi ve iletişimin kolayca erişilebilir ve anlaşılır olması, açık ve sade bir dil kullanılması gerekmektedir. Bu bilgi ve iletişimin kolayca erişilebilir ve anlaşılır olmasının yanı sıra açık ve sade bir dil kullanılarak sunulması

[600] European Data Protection Board (EDPB), *Guidelines 3/2019 on Processing of Personal Data Through Video Devices*, 13; Valerio De Stefano ve Mathias Wouters, *AI and Digital Tools in Workplace Management and Evaluation: An Assessment of the EU's Legal Framework* (European Parliamentary Research Service, 2022), 52-53, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4144899.
[601] Franca Salis Madinier, A Guide to Artificial Intelligence at the Workplace (European Economic and Social Committee, 2021), 23.
[602] Gürsel, İşçinin Kişisel Verilerinin Korunması Hakkı, 210-11; Küzeci, Kişisel Verilerin Korunması Hukuku, 207-8; Mesut Serdar Çekin vd., Veri Hukuku (On İki Levha Yayıncılık, 2023), 70; Dülger, Kişisel Verilerin Korunması Hukuku, 174-79.
[603] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 73.
[604] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 74.

esastır. Dolayısıyla, şeffaflığın temel gereklilikleri, aydınlatma yükümlülüğünün kapsamıyla doğrudan örtüşmektedir.

Şeffaflık ilkesi, işverenlerin tele çalışma modelinde kullanılan izleme teknolojileri hakkında çalışanları net ve kapsamlı bir şekilde bilgilendirme yükümlülüğünü de beraberinde getirmektedir. Günümüzde tele çalışma modelinde kullanılan yeni izleme teknolojilerinin karmaşıklığı göz önüne alındığında, işverenin şeffaflık ilkesi gereği çalışanları sadece genel olarak izleme yapıldığı konusunda değil, izlemenin teknik detayları, kapsamı, süresi, verilerin kimlerle paylaşılabileceği ve olası sonuçları hakkında da açık, anlaşılır ve kolay erişilebilir bir dille bilgilendirmesi zorunludur. Sadece "performans ve güvenlik amacıyla izleme yapılmaktadır" gibi genel bir ifade, özellikle müdahaleci izleme yöntemleri için şeffaflık ilkesini karşılamayacaktır.

4.3.2. Belirli, Açık ve Meşru Amaçlar için İşlenme

Kişisel verilerin işlenmesinde uyulması gereken temel ilkelerden biri olan "belirli, açık ve meşru amaçlar için işlenme" ilkesi, KVKK'nın 4. maddesinin 2. fıkrasının (c) bendi ve GDPR 5. maddesinin 1. fıkrasının (b) bendinde düzenlenmiştir. Öğretide bu ilke, kişisel veri işleme faaliyetinin yönünü ve sınırlarını belirleyen temel normatif çerçeve olarak kabul edilmektedir[605]. Veri sorumlusunun keyfî, belirsiz veya kötü niyetli veri işleme uygulamalarına başvurmasını önlemeyi amaçlamakta; böylece veri işleme sürecinin şeffaflık, hesap verebilirlik ve birey haklarına saygı ilkeleriyle uyumlu hâle gelmesini sağlamaktadır. Bu temel ilke belirlilik, açıklık ve meşruiyet olmak üzere üç ana unsurdan oluşmaktadır. Aşağıda her bir unsur ayrı başlıklar altında kısaca incelenecektir.

4.3.2.1. Belirlilik

Belirlilik ilkesi gereğince, veri işleme faaliyeti, kesin ve net olarak tanımlanmış bir amaca dayanmalıdır. KVKK'da ve GDPR'da (özellikle Başlangıç bölümü 39. maddesi) veri işleme amaçlarının veri toplama anında belirlenmesi gerektiği

[605] Dülger, *Kişisel Verilerin Korunması Hukuku*, 181; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 208.

vurgulanmıştır. Bu çerçevede gelecekte herhangi bir amaçla kullanılmak üzere veri toplanması hukuka aykırı kabul edilecektir. Kişisel veriler, yalnızca belirli bir ihtiyacı karşılamak veya belirli bir işlemi yürütmek için toplanmalıdır. Belirsiz, soyut ya da gelecekte muhtemel olabilecek varsayımsal amaçlarla işlenmemelidir[606]. Bu çerçevede "ileride gerekebilir" düşüncesiyle veri işlenmesi veya "her ihtimale karşı" veri toplanması, sözü geçen ilkenin açık ihlali niteliğindedir[607].

Tele çalışma özelinde belirlilik ilkesi değerlendirildiğinde, işveren "personel yönetimi" veya "tele çalışma süreçlerinin optimizasyonu" gibi muğlak amaçlarla veri toplamamalıdır. Veri toplama anında veri işleme amacı açıkça tanımlanmalı ve işleme faaliyetinin tüm aşamaları bu amaçla uyumlu olacak şekilde yürütülmelidir[608]. Tele çalışma modelinde, işverenin çalışanlarını izleme ve gözetleme yöntemleriyle izlemesi durumunda, her bir faaliyet için veri toplama amacı önceden, kesin ve net olarak tanımlanmalıdır[609]. Örneğin, "çalışan performansını artırmak" gibi soyut bir amaç yerine, "tele çalışan müşteri temsilcilerinin çağrı yanıtlama sürelerini analiz ederek hizmet kalitesini X standardına getirmek" veya "hassas proje verilerine uzaktan erişen tele çalışanların sadece yetkili sistemlere ve işle ilgili uygulamalara erişim sağladığını teyit etmek amacıyla erişim loglarını ve uygulama kullanımını sınırlı ölçüde tutmak" gibi daha spesifik amaçlar belirlenmelidir.

4.3.2.2. Açıklık

Veri işleme amacının yalnızca veri sorumlusu tarafından belirlenmiş olması da yeterli değildir. Ayrıca ilgili kişi tarafından da anlaşılabilir ve öngörülebilir nitelikte olması gereklidir[610]. Açıklık unsuru, veri işlemenin şeffaf bir şekilde yürütülmesini temin etmeyi amaçlamaktadır ve GDPR 5. maddesinin 1. fıkrasının (a) bendinde vurgulanan şeffaflık ilkesiyle yakından ilişkilidir. Bu kapsamda, ilgili kişi, hangi verilerinin hangi amaçlarla işlendiğini ve işleneceğini önceden, açıkça ve yeterli şekilde bilmelidir[611].

---

[606] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 212; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 209; Dülger, *Kişisel Verilerin Korunması Hukuku*, 182; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 151; Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 21.
[607] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 209.
[608] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 213.
[609] Bknz. Bölüm 3.3.2.
[610] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 213.
[611] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 129.

Belirsiz, teknik ifadeler içeren veya yoruma açık genel tanımlar, açıklık ilkesini zedelemektedir. Nitekim, açık amaç ilkesine uygunluk, veri sorumlusunun aydınlatma yükümlülüğünün de ayrılmaz bir parçasıdır; çünkü aydınlatma yükümlülüğünün özü, hangi verinin hangi spesifik amaçla işlendiğinin ilgili kişiye bildirilmesidir. Bu bildirim ise ancak amacın kendisi en baştan açık ve meşru bir şekilde tanımlanmışsa geçerlilik kazanır.

Tele çalışan, hangi dijital araçla (örneğin, kullanılan izleme yazılımının adı, temel işlevleri ve veri toplama yetenekleri), hangi verilerinin (klavye hareketleri mi, ekran görüntüleri mi, uygulama kullanım süreleri mi, ağ trafiği mi), ne sıklıkta (sürekli mi, rastgele mi, belirli olaylara veya zaman dilimlerine bağlı mı), ne kadar süreyle ve tam olarak hangi amaçla izlendiği konusunda açık, anlaşılır ve yanıltıcı olmayan bir şekilde bilgilendirilmelidir[612]. Sadece "iş süreçlerinin takibi ve güvenliği amacıyla izleme yapılmaktadır" gibi genel bir ifade, özellikle müdahaleci izleme yöntemleri söz konusu olduğunda, bu ilkeyi karşılamakta yeterli sayılmayacaktır.

4.3.2.3. Meşruiyet

Meşruiyet, veri işleme faaliyetinin kanunlara ve anayasal düzenlemelere uygun olmasını, bireyin kişilik haklarına zarar vermemeyi ve veri sorumlusunun çıkarlarının bireyin temel haklarıyla orantılı olmasını ifade etmektedir[613]. Bu kapsamda veri işleme amacının yalnızca belirli ve açık olması yeterli değildir. Aynı zamanda hukuken korunmaya değer bir menfaate dayanması, kamu düzenine, temel hak ve özgürlüklere aykırı olmaması da gerekir[614].

Tele çalışmada işverence kullanılan izleme yönteminin de amacı kişisel veri işleme söz konusu ise meşru olmalıdır[615]. Örneğin, bir işverenin tele çalışanın evindeki özel hayatını merak saikiyle gözetlemesi ya da sendikal faaliyetlerini takip etmek veya

---

[612] Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 122.
[613] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 214-15; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 209; Meşru olma ile yasal olma arasındaki ayrıntılı farklar için bknz. Dülger, *Kişisel Verilerin Korunması Hukuku*, 187.
[614] Savaş, "İş Hukukunda 'Siber Gözetim'", 107.
[615] Falque-Pierrotin, Opinion 2/2017 on Data Processing at Work, 22-24.

çalışanı yıldırmak gibi bir amaçla kişisel veri işlemesi meşru kabul edilemez. Benzer şekilde, tele çalışanın her anını insan onurunu zedeleyici bir şekilde kontrol altında tutarak aşırı strese sokacak veya kesintisiz çalışmayı dayatacak bir izleme amacı da meşru kabul edilemez[616]. İşverenin verimlilik artışı veya veri güvenliği gibi meşru bir amacı olsa dahi, bu amaca ulaşmak için seçilen izleme yönteminin çalışanın temel hak ve özgürlüklerine, özellikle de ev ortamındaki mahremiyetine orantısız bir müdahale teşkil etmemesi gerekmektedir[617].

4.3.3. İşlendikleri Amaçla Sınırlı ve Ölçülü Olma

Kişisel verilerin işlenmesinde uyulması gereken temel ilkelerden biri olan işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi, KVKK'nın 4. maddesinin 2. fıkrasının (ç) bendinde açıkça düzenlenmiştir. Bu ilke uyarınca, kişisel verilerin işlenmesi yalnızca önceden belirlenmiş, açık ve meşru amaçlarla sınırlı tutulmalı; belirlenen amaçla ilgisi bulunmayan, gereksiz veya aşırı nitelikteki veri işleme faaliyetlerinden kaçınılmalıdır[618]. Bu ilke, GDPR 5. maddesinin 1. fıkrasının (c) bendinde "veri minimizasyonu" (data minimization) olarak adlandırılmakta ve kişisel verilerin işlendikleri amaçlar için yeterli, ilgili ve gerekli olanla sınırlı olması (adequate, relevant and limited to what is necessary) gerektiğini ifade etmektedir[619]. Öğretide söz konusu ilke, farklı kaynaklarda veri asgarileştirme veya yeterlilik ilkesi gibi kavramlarla da ifade edilmektedir[620].

İşlendikleri amaçla sınırlı ve ölçülü olma ilkesi, KVKK ve GDPR'ın yanı sıra 108+ sayılı Sözleşme gibi uluslararası hukuk belgelerinde de temel bir veri koruma ilkesi olarak kabul edilmektedir[621]. Sözü geçen ilke, kişisel verilerin yalnızca belirli, açık ve

---

[616] Valerio De Stefano, "'Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection", *41 COMP. LAB. L. & POL'y J. 15*, advance online publication, 2019, 14, https://doi.org/10.2139/ssrn.3178233.
[617] Bernhardt vd., "The Data-Driven Workplace and the Case for Worker Technology Rights", 13.
[618] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 215-16; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 213-19; Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 21; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 152.
[619] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 73.
[620] Akgül, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, 133; Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 51; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 214.
[621] Bkz. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, modernised by CETS No. 223), Article 5.

meşru amaçlarla işlenmesini ve bu işleme faaliyetlerinin amaca uygun ve ölçülü olmasını gerekli kılmaktadır. Avrupa Sosyal Tarafları arasında 2002 yılında imzalanan Uzaktan Çalışma Çerçeve Anlaşması'nın (European Framework Agreement on Telework, 2002) mahremiyete ilişkin 6. maddesi de bu ilkeye vurgu yapmaktadır. İlgili madde, işverenlerin uzaktan çalışanların mahremiyetine saygı gösterme yükümlülüğünü açıkça düzenlemekte ve herhangi bir izleme sisteminin uygulanması hâlinde bu sistemlerin mutlaka ölçülülük ilkesi doğrultusunda tasarlanması gerektiğini belirtmektedir[622]. Bu bağlamda ölçülülük ilkesi, izleme faaliyetlerinin yalnızca meşru bir amaca ulaşmak için zorunlu, gerekli ve uygun olan araçlarla sınırlandırılmasını ve çalışanların özel hayatına gereksiz ya da aşırı müdahalede bulunulmamasını öngörmektedir[623]. Kişisel verilerin korunmasına ilişkin hem ulusal hem de uluslararası hukuk sistemlerinde ortak bir normatif çerçeve olarak da kabul edilmektedir. Sözü geçen ilkeye göre, eğer belirtilen amaca başka, daha az müdahaleci araçlar vasıtasıyla veya daha az kişisel veri işleyerek ulaşılabiliyorsa, mevcut veri işleme faaliyeti gerçekleştirilmemeli veya kapsamı daraltılmalıdır. Kişisel verilerin işlenmesi belirlenen amacın kapsamını aşmayacak biçimde ölçülü ve sınırlı tutulmalıdır. Bir başka ifadeyle veri sorumlusu, hedeflenen amaca ulaşmak için gerekli olan en az miktarda veriyi kullanmalıdır[624]. Bu noktada ispat yükü, veri sorumlusu olan işverendedir. Yani, topladığı her bir veri türünün, belirlediği meşru amaca ulaşmak için neden gerekli olduğunu ve daha azının neden yeterli olmayacağını gerekçelendirmek zorundadır[625]. Ayrıca kişisel verilerin birden fazla amaç için kullanılması söz konusu ise her kullanım amacı bakımından ayrı ayrı gereklilik ve ölçülülük kriterine uyum sağlanmalıdır[626].

Bu konuda Yargıtay 9. Hukuk Dairesi'nin 22.02.2024 tarihi ve E. 2024/1311, K. 2024/3381 sayılı kararına konu olayda, işçilerin konum ve hareketlerini takip eden ve

---

[622] Madinier, *A Guide to Artificial Intelligence at the Workplace*, 23.
[623] Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 11; Akın, "Türk Çalışma Yaşamında Pandemi Sürecinde Uzaktan/Evden Çalışma ve Olası Sonuçları", 279; Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 200-201; Dulay Yangın, "Bilgi ve İletişim Teknolojilerinde Yaşanan Gelişimin İş Hukuku Üzerindeki Etkileri: Tele Çalışmaya İlişkin Tespit ve Öneriler", 253; Ünal Adınır, "Tele çalışmada verilerin korunması", 971.
[624] Savaş, "İş Hukukunda 'Siber Gözetim'", 107; Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 81.
[625] Bahar Çakmak, "İnsan Hakları Temelli Yaklaşım Çerçevesinde Yapay Zekâ Teknolojilerinde Kişisel Verilerin Korunması" (Yayınlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi, 2024), 102.
[626] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 214.

kısa süreli hareketsizlikte titreşimle uyarı veren RFID cihazlarının kullanımı tartışılmıştır. İşveren, uygulamanın İSG amaçlı olduğunu savunurken, davacı sendika uygulamanın kişilik haklarını ihlal ettiğini ve KVKK'ya aykırı olduğunu belirtmiştir. Yargıtay, kararı eksik inceleme nedeniyle bozarak; cihazın teknik özellikleri, çalışan sağlığına etkileri ve KVKK kapsamında rıza alınıp alınmadığı gibi konuların uzman bilirkişilerce tespit edilmesi gerektiğine hükmetmiştir. Bizim de katıldığımız karşı oyda ise, uygulamanın ölçülülük ilkesine ve temel insan haklarına açıkça aykırı olduğu ifade edilmiştir[627].

---

[627] Bizim de katıldığımız karşı oy yazısında "*6098 sayılı Kanun'un 417'nci maddesi "İşçinin kişiliğinin korunması" başlığını taşımakta olup maddenin birinci fıkrasında "İşveren hizmet ilişkisinde işçinin kişiliğini korumak ve saygı göstermek ve işyerinde dürüstlük ilkelerine uygun bir düzeni sağlamakla özellikle işçilerin psikolojik ve cinsel tacize uğramamaları ve bu tür tacizlere uğramış olanların daha fazla zarar görmemeleri için gerekli önlemleri almakla yükümlüdür." denilmektedir. 6098 sayılı Kanun'un 419 uncu maddesi ise "İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir." hükmünü içermektedir. 6098 sayılı Kanun'un 396 ncı maddesine göre de "İşçi yüklendiği işi özenle yapmak ve işverenin haklı menfaatinin korunmasında sadakatle davranmak zorundadır." İşverenlerin iş dünyasında rekabet edebilmek ve ayakta kalabilmek için çalışanları hakkında düzenli bilgilere ihtiyaç duyması ve onları üretim sahasında kontrol etmesi doğaldır. Bu kontrol bazen kanuni zorunluluk ve sorumluluklardan kaynaklanabilir; bazen de performans değerlendirme verimlilik ölçümü ve iş güvenliği sebeplerinden kaynaklanabilir. İşveren bu sebeplere dayanarak gerekli izlemelerde bulunabilir. Ancak bu izlemeler gerçekleştirilirken her zaman orantılılık ilkesine uygun davranmak zorundadır. Aksi durumda işçilerin özel hayatlarının ihlali söz konusu olacaktır. İzlenmenin işçiler üzerinde oluşturacağı etki yoğunlukla strestir. İzlenme, işçiler üzerinde depresyon ve anksiyete artışlarına sebep olabilecektir. 6698 sayılı Kanun kişisel veriyi kimliği belirli yada belirlenebilir gerçek kişiye ilişkin "her türlü bilgi" olarak tanımlar. 6698 sayılı Kanunun 4 üncü maddesinde yer alan kişisel verilerin işlenmesine ilişkin temel ilkeler her türlü kişisel veri işleme faaliyetlerinin içinde bulunmalı ve veri işleme faaliyetleri bu ilkelere uygun olarak yürütülmelidir. Bu ilkeler; hukuka ve dürüstlük kurallarına uygun davranma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhaza edilme olarak düzenlemiştir. Kanun'un 5 inci maddesi ise kişisel verilerin işlenme şartlarını düzenlenmiş olup birinci fıkrası kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğini, ikinci fıkrası rızanın aranmayacağı ayrık durumları düzenlemiş; ancak somut olayda ikinci fıkrada sayılan durumların söz konusu olmadığı anlaşılmıştır. İşçinin taraf tanık anlatımlarına göre her on dakikada, hareketsiz kalması hâlinde bu durumun sisteme kaydedilerek titreşim gönderilmesi ve arkasından işlem yapılmasa bile ekip başları tarafından uyarılması ya da tutanak tutulması, 6698 sayılı Kanun kapsamında özel nitelikte kişisel veri olarak kabul edilmelidir. Bu hâliyle sürekli şekilde izlenmek doğaldır ki işçiyi stres altına sokarak işçi sağlığını olumsuz etkilemekte, kişilik haklarını zedelemektedir. Davalı işyerinde işçilerin başlangıçta açık rızası alınmadan uygulamaya konulan Hassas Konum Tabanlı Personel Etiketi kısaca RFID adı verilen bu takip sistemi ister davacı tarafın ileri sürdüğü gibi işçilerin performans denetimine ilişkin olsun, ister davalı tarafın ileri sürdüğü gibi ihtilaflı dönemde yürürlükte bulunan toplu iş sözleşmesinin 27 nci maddesinin (a) bendinden hareketle üyenin çalışma süresini tespiti yanında birincil amaç olarak iş sağlığı ve güvenliği için kullanılmış olsun -ki işçilerin iş sağlığı ve güvenliğinin takip sistemi dışında başka yöntemlerle sağlanması mümkün iken- her on dakikada bir yerlerinde olup olmadıklarının, hareketsiz kalıp kalmadıklarının kontrolü insan psikolojisine, orantılılık ilkesine 6098 sayılı Kanun'un 417 ve 419 uncu maddelerine, 6698 sayılı Kanun'a ve temel insan haklarına aykırılık oluşturmaktadır. Açıklanan nedenlerle RFID takip cihazı uygulamasının mevzuata ve toplu iş sözleşmesine aykırı olduğunun tespitine ilişkin İlk Derece Mahkemesi kararı ve davalı tarafın istinaf talebini esastan reddeden istinaf kararı usul ve kanuna uygun olmakla onanması gerekirken çoğunluğun bozma yönündeki kararına iştirak edilememiştir."* şeklinde belirtilmiştir. Kanaatimizce karşı oyda belirtilen nedenlerle, davalı işverence kurulan takip sisteminin, iş sağlığı ve güvenliğini sağlama amacı ile çalışanın temel hak ve özgürlüklerine yaptığı müdahale

GDPR 25. maddesinde belirtilen gizliliğin tasarım aşamasından itibaren gözetilmesi ve başlangıçtan itibaren gizliliği esas alan yapılandırma ilkesi de bu ilkeyi destekler nitelikte[628], veri sorumlularının hem işleme araçlarını belirlerken hem de işleme sırasında veri minimizasyonu gibi ilkeleri etkin bir şekilde uygulayacak teknik ve organizasyonel tedbirleri almasını ve varsayılan olarak sadece her bir özel amaç için gerekli olan kişisel verilerin işlenmesini sağlamasını zorunlu kılmaktadır[629]. İşverenler, tele çalışma için kullanılacak yazılım ve donanımları seçerken veya geliştirirken, GDPR 25. maddesi uyarınca, varsayılan olarak en az miktarda kişisel veriyi işleyen ve gizlilik ayarları en yüksek seviyede olan araçları tercih etmelidir[630]. Örneğin, bir video konferans yazılımının varsayılan olarak kamera ve mikrofonu kapalı başlatması veya bir aktivite izleme yazılımının sadece işverenin aktif talebiyle ve sınırlı bir süre için, önceden tanımlanmış minimum veri setini toplaması bu ilkeye uyumlu olacaktır.

İlkenin önemli bir yönü, veri sorumlusunun yalnızca mevcut amaç doğrultusunda değil, aynı zamanda gelecekteki olası amaçlar doğrultusunda da veri toplamasını engellemesidir. İleride gerekebilir düşüncesiyle işlenen veriler, bu ilkenin ihlaline neden olacaktır[631]. Verilerin ilk toplandığı anda belirlenen amaçla uyumsuz bir yeni amaç için işlenmesi durumunda, yeni bir hukuka uygunluk nedenine dayanılması veya açık rıza alınması gerekmektedir. Aksi hâlde, işleme faaliyeti gerek KVKK gerekse GDPR'ın belirlediği temel ilkelere aykırılık teşkil edecektir[632]. Dolayısıyla bu ilke, yalnızca veri toplama anında değil, verinin işlenmeye devam ettiği tüm süreçlerde dikkate alınmalı ve veri sorumlusu tarafından dinamik biçimde gözden geçirilmelidir.

---

arasında bariz bir orantısızlık bulunmaktadır. İşçinin sürekli gözetim altında tutulması, özel hayatının gizliliğini ve kişilik haklarını ihlal etmekle kalmayıp, 6698 sayılı Kanun'da güvence altına alınan kişisel verilerin korunması ilkesini de açıkça çiğnemektedir. Hukuka uygunluğun temel ölçütlerinden olan orantılılık ilkesi göz ardı edilerek, daha az müdahaleci yöntemler mevcutken bu yola başvurulması kabul edilemez. Bu sebeple, alt derece mahkemelerinin haklı ve yerinde olan kararının onanması gerektiği görüşündeyiz. Karar için bknz., https://www.lexpera.com.tr/ictihat/yargitay/e-2024-1311-k-2024-3381-t-22-02-2024, erişim 05.05.2025.

[628] Valerio De Stefano, "Algorithmic Bosses and What to Do About Them: Automation, Artificial Intelligence and Labour Protection", içinde Economic and Policy Implications of Artificial Intelligence, ed. Domenico Marino ve Melchiorre A. Monaca (Springer International Publishing, 2020), n. 3, https://doi.org/10.1007/978-3-030-45340-4_7.

[629] Feiler vd., The EU General Data Protection Regulation (GDPR), 145.

[630] De Stefano, "Algorithmic Bosses and What to Do About Them", n. 3.

[631] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 209.

[632] Kanunda amaç değişikliği konusunun açık bir şekilde düzenlenmemiş olmasına yönelik eleştiriler için bknz. Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 75-76.

Amaçla sınırlılık ilkesi, AB Yapay Zekâ Tüzüğü kapsamında da değerlendirilmektedir. Buna göre, Tüzük çerçevesinde işveren, yapay zekâ destekli izleme araçlarının kullanımı bakımından Tüzük'ün 3. maddesinin 4. fıkrası Başlangıç bölümü 13. maddesi kapsamında dağıtıcı (deployer) olarak konumlandırılmakta[633] ve bu araçları yalnızca sağlayıcı (provider) tarafından belirlenmiş olan "amaçlanan kullanım" (intended purpose) doğrultusunda kullanmakla yükümlü kılınmaktadır[634]. İşverenin, örneğin yalnızca sistem güvenliğini sağlamaya yönelik tasarlanmış bir aracı, asıl amacı dışında, çalışanların verimliliğini ölçmek gibi ek ve daha müdahaleci bir amaçla kullanması, amaçla sınırlılık ilkesine açıkça aykırılık teşkil etmekte ve bu ikincil amaçla yapılan işlemeyi hukuka aykırı hâle getirmektedir. Çünkü aracın orijinal risk değerlendirmesinde öngörülmeyen bu ikincil kullanım şekli, çalışanların mahremiyetine daha büyük bir müdahaleyi beraberinde getirmektedir. İşverenin bir yapay zekâ sisteminin amaçlanan kullanımını değiştirmesi durumunda, kendisinin bir "sağlayıcı" olarak kabul edileceği ve çok daha ağır yükümlülüklere tabi olacağı da öğretide belirtilmektedir[635].

Ölçülülük ilkesi gereğince, doğrudan ve sürekli izleme yöntemleri yerine, aynı amaca ulaşmayı sağlayacak daha az müdahaleci yollarla başvurulması gerekmektedir. Örneğin, çalışanların sürekli internet kullanımını izlemek yerine, yalnızca belirli web sitelerine erişimini teknik olarak engellemek, daha ölçülü ve uygun bir çözüm olarak değerlendirilmektedir[636]. Öte yandan, ölçülülük ilkesi, yalnızca verinin içeriği ve miktarıyla değil, aynı zamanda verilerin ne kadar süreyle saklandığıyla da doğrudan ilişkilidir. İşleme amacı sona erdiğinde, verilerin artık saklanmaya devam etmesi ölçüsüzlük oluşturmaktadır. Kişisel veriler, yalnızca işleme amacıyla sınırlı süre boyunca muhafaza edilmeli; süre sona erdiğinde silinmeli, imha edilmeli veya anonim hâle getirilmelidir[637]. Bu yönüyle "işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" ilkesiyle sıkı bir bağ içerisindedir[638].

---

[633] Voigt ve Hullen, *The EU AI Act*, 26.
[634] Voigt ve Hullen, The EU AI Act, 114.
[635] Voigt ve Hullen, The EU AI Act, 29-30.
[636] Falque-Pierrotin, *Opinion 2/2017 on Data Processing at Work*, 13-15.
[637] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 264-65; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 205.
[638] Duygu Maya, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Çerçevesinde Bulut Bilişim Sistemleri" (Yayınlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, 2023), 47.

İş ilişkileri bağlamında ise TBK 419. maddesinde işçinin verilerinin işe yatkınlığıyla ilgili veya iş sözleşmesinin ifası için zorunlu olduğu ölçüde işlenebileceği düzenlenmiştir[639]. İşçinin kişisel verilerinin, yalnızca iş görme ediminin amacına uygun olarak işlenmesini öngören bu düzenleme, sosyal ve ekonomik açıdan zayıf konumdaki işçiyi işverene karşı korumayı ve kural olarak kişisel verilerin kaydedilmesini yasaklamayı amaçlamaktadır[640]. Bu çerçevede örneğin bir iş sözleşmesinin kurulması için gerekli olan temel iletişim bilgileri dışındaki verilerin toplanması, bu ilkeye aykırılık oluşturacaktır. Aynı şekilde, bir işverenin bordro düzenlemek amacıyla çalışanlara ait bazı verileri işlemesi makûl kabul edilebilirken, bu kapsamın ötesinde özel nitelikli verilerin toplanması ve kullanılması ölçüsüzlük teşkil edecektir. TBK 419. maddesinde düzenlenen *"işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde"* veri işleme ilkesi, tele çalışanın özel hayat alanında gerçekleşen izleme faaliyetleri sonucu elde edilecek veriler için daha da sıkı yorumlanmalıdır. İşverenin, tele çalışanın ev ortamındaki her hareketini veya tüm dijital izlerini iş sözleşmesinin ifası için zorunlu olarak nitelendirmesi ise bu ilkeyle bağdaşmayacaktır.

Amaçla sınırlılık ve ölçülülük ilkesi, iş ilişkilerinde izleme ve gözetleme uygulamaları kapsamında ele alınması gereken temel ilkelerden biri olarak karşımıza çıkmaktadır. Teknolojik gelişmelerle birlikte, izleme ve gözetleme araçları ile elde edilen veriler, internet aracılığıyla uzaktan erişilebilir hâle gelmiş; buna ek olarak yüz tanıma ve hareket analizi gibi müdahale düzeyi yüksek yeni yöntemlerin kullanımı da yaygınlaşmıştır[641]. Böylelikle çalışanların özel hayatına yönelik müdahalelerin kapsamı genişlemiş, kişisel verilerin korunması açısından daha büyük riskler ortaya çıkmıştır. Örneğin, işçilerin dinlenme alanları, duşlar ve soyunma odaları gibi kişisel alanlarında kamera ile gözetlenmeleri suretiyle veri toplanması, iş görme ediminin ifası açısından zorunluluk taşımadığı gibi, açık bir veri ihlaline neden olmaktadır. Bu

[639] Manav, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", 104-5.
[640] K. Ahmet Sevimli, "Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419", *Sicil İş Hukuku Dergisi, Yıl* 4, sy 24 (2011): 134 vd.; A. Eda Manav, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 19, sy 2 (2015): 104-5; Yeliz Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", içinde *İş Hukukunda Yeni Yaklaşımlar* (İstanbul: Beta Yayınları, 2017), 31 vd.
[641] Falque-Pierrotin, *Opinion 2/2017 on Data Processing at Work*, 19-20.

tür uygulamalar aynı zamanda işçinin mahremiyet hakkının ihlali niteliğinde olup[642], işçi bakımından taciz boyutuna varan ciddi bir hak ihlali olarak değerlendirilmektedir[643]. Benzer şekilde, tele çalışanın evinde, özellikle çalışma alanı dışındaki özel hayat alanlarını (örneğin, yatak odası, mutfak gibi) veya aile bireylerinin de bulunduğu ortamları kapsayacak şekilde webcam veya mikrofon aracılığıyla izleme yapılması, ya da çalışanın çalışma saatleri dışındaki veya kişisel mola zamanlarındaki aktivitelerinin takip edilmesi, bu ilkenin ve genel mahremiyet hakkının açık bir ihlalidir[644]. Eğer bir izleme yazılımı, belirtilen meşru amaca ulaşmak için gereğinden fazla veri kategorisi topluyorsa (örneğin, sadece çalışma süresi takibi veya görev tamamlanma durumunu teyit için konum verisi, özel uygulama kullanım detayları veya sürekli webcam görüntüsü)[645], bu durum veri minimizasyonu ve ölçülülük ilkelerine açıkça aykırılık teşkil etmektedir. Böyle bir durumda işçi, iş sözleşmesini haklı nedenle derhâl feshetme hakkına sahip olmakla birlikte, söz konusu ihlal nedeniyle uğradığı zararlardan dolayı maddi ve manevi tazminat talebinde de bulunabilecektir[646]. Ayrıca işçinin sürekli biçimde görüntü ve ses kaydına maruz bırakılması, psikolojik baskı ve çeşitli rahatsızlıklara yol açabileceği için iş sağlığı ve güvenliği yönünden de hukuka aykırılık oluşturmaktadır[647].

Yapay zekâ tabanlı izleme ve gözetleme uygulamalarının kullanılması bağlamında ise ölçülülük ilkesinin uygulanmasında AB Yapay Zekâ Tüzüğü çerçevesinde somut bazı örneklerle sınırlandırılmıştır. Bu bağlamda Tüzük, işyerlerinde ve eğitim kurumlarında duygu tanıma sistemlerinin kullanılmasını genel prensip olarak yasaklamaktadır[648].

---

[642] Emine Tuncay Kaplan, "İşverenin Koruma ve Gözetme Borcunun Kapsamı", *Kamu-İş, C* 2 (2003): 145; Erdemir Ve Çeliktaş, "Örgütsel ve Hukuki Açıdan İşyeri İzleme: Karşılaştırmalı Bir İnceleme", 99.

[643] Köksal Büyük ve Uğur Keskin, "Panoptikon'un Elektronik Dirilişi: Etik Bir Sorun Olarak İşyeri İzleme", *İş Ahlakı Dergisi* 5, sy 10 (2012): 58; Erdoğan, *Kişilik Hakkı Kapsamında İşçilerin İzlenmesi ve Gözetlenmesi*, 44.

[644] Jeremias Adams-Prassl vd., "Regulating Algorithmic Management: A Blueprint", *European Labour Law Journal* 14, sy 2 (2023): 129. İşverenin, işçinin evinde iş için ayrılan bölümün özel kullanımını sınırlaması durumunda kira giderinin bir kısmını üstlenip üstlenmeyeceği yönündeki değerlendirmeler için bknz. Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", 195.

[645] Bernhardt vd., "The Data-Driven Workplace and the Case for Worker Technology Rights", 19.

[646] Erdoğan, *Kişilik Hakkı Kapsamında İşçilerin İzlenmesi ve Gözetlenmesi*, 163-64; Kahraman Akgül, "İşçinin İşyerinde İzlenmesi ve Gözetlenmesinin Hukuki Sonuçları", 103-11.

[647] Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 10; Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 166; Kahraman Akgül, "İşçinin İşyerinde İzlenmesi ve Gözetlenmesinin Hukuki Sonuçları", 55.

[648] Voigt ve Hullen, *The EU AI Act*, 54-55.

Ancak Tüzük, tıbbi veya güvenlik gibi özel amaçlar için bu yasağa son derece sınırlı istisnalar tanımaktadır. Örneğin, profesyonel pilotların veya sürücülerin yorgunluk düzeylerini ölçen sistemler, güvenlik amaçlı olduğu gerekçesiyle bu istisna kapsamına girmekte ve bu sayede yasaklanmış kategorisinden çıkarılarak sınırlı biçimde izin verilen teknolojiler arasında kabul edilmektedir[649]. Böylelikle, genel olarak fazla müdahaleci bir yöntem şeklinde kabul edilen duygu tanıma sistemleri, belli durumlarda istisnai olarak değerlendirilmektedir.

4.3.4. Saklama Süresi ile Sınırlı Olma

KVKK'nın 4. maddesinde, kişisel verilerin *"ilgili mevzuatta öngörülen ve işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi*" gerektiği belirtilmektedir. Bu ilkeye göre, kişisel veriler ancak işlenme amacı doğrultusunda gerekli olduğu sürece saklanabilmekte; amaç ortadan kalktığında ise verilerin saklanmaya devam edilmesi hukuka aykırılık teşkil etmektedir[650]. GDPR'ın 5. maddesinin 1. fıkrasının (e) bendinde yer alan saklama sınırlaması (storage limitation) ilkesi, temel bir kural ortaya koymaktadır. Bu kurala göre kişisel veriler, *"işlendikleri amaçlar için gerekli olandan daha uzun bir süre boyunca kimliği belirli veya belirlenebilir bir şekilde saklanmamalıdır"*. Bununla birlikte aynı ilke, bu temel kurala bir istisna getirerek, GDPR 89. maddesinin 1. fıkrası uyarınca bu verilerin, *"veri sahibinin hak ve özgürlüklerini korumak için uygun teknik ve organizasyonel tedbirlerin alınması koşuluyla, yalnızca kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiksel amaçlar için daha uzun süreler boyunca saklanabileceğini"* de belirtmektedir[651].

İlkenin özü, kişisel verilerin süresiz biçimde kayıt altında tutulmasının, bireylerin mahremiyetini tehdit etmesi ve kişisel alanlarına sürekli bir müdahale olasılığı yaratması nedeniyle hukuka aykırı olmasıdır[652]. Bu ilke, kişisel verilerin belirli bir

---

[649] Voigt ve Hullen, *The EU AI Act*, 55.
[650] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 220; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 244-45; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 152; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 221.
[651] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 306.
[652] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 220; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 244-45; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 152-54; Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 21; Dülger, *Kişisel Verilerin Korunması Hukuku*, 194-98.

amaçla toplandığı andan itibaren zamansal olarak sınırlı süreyle saklanmasını zorunlu kılmaktadır. Veriler, işleme amacının gerçekleşmesinden veya bu amacın sona ermesinden sonra, artık gereksinim duyulmaması hâlinde, silinmeli, yok edilmeli ya da kişisellik niteliği ortadan kaldırılarak anonim hâle getirilmelidir[653]. GDPR 5. maddesinin 2. fıkrasındaki "hesap verebilirlik" ilkesi uyarınca, veri sorumluları bu ilkeye uyumu göstermek adına, saklama sürelerini belirlemeli ve bu sürelere uyumu sağlamak için politikalar ve prosedürler geliştirmelidir. Süresiz veri saklama, bireylerin verilerinin sürekli bir gözetim altında olduğu hissine kapılmasına yol açmakta ve bu durum, kişisel verilerin korunması hukukunun özünü oluşturan bireysel özerklik ilkesini, bireyin maddi ve manevi bütünlüğü ile özel hayatın gizliliği hakkını zedelemektedir[654].

Verilerin silinmesi, yok edilmesi ya da anonimleştirilmesi, hem bireyin hak ve özgürlüklerini koruma işlevi görmekte hem de veri sorumlusu açısından bir yükümlülük oluşturmaktadır[655]. Bu yükümlülüğün yerine getirilmemesi, yalnızca KVKK bağlamında idari yaptırımlarla sınırlı kalmamakta, ayrıca Türk Ceza Kanunu bakımından da ceza sorumluluğuna yol açabilmektedir[656]. Özellikle verileri yok etmeme fiili, belirli koşulların gerçekleşmesi hâlinde suç teşkil edebilmektedir. Bu nedenle, veri sorumlularının düzenli aralıklarla veri envanterlerini gözden geçirmeleri, işleme amacı sona ermiş verileri tespit etmeleri ve gerekli imha işlemlerini gerçekleştirmeleri gerekmektedir[657].

Saklama süresi belirlenirken öncelikle tabi olunan özel mevzuattaki hükümler dikkate alınmalıdır. Örneğin, İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği 7. maddesinin 1. fıkrasının (b) bendi uyarınca, işverenin çalışanın sağlık dosyasını işten ayrılma tarihinden itibaren en az 15 yıl boyunca saklaması gerekmektedir. Bu tür açık mevzuat hükümleri, veri sorumluları açısından bağlayıcıdır ve bu süre dolmadan ilgili kişinin

---

[653] Anonim hale getirme ile ilgili ayrıntılı bilgi için bknz. Bölüm 4.5.1.9. Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 264-65; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 205.
[654] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 221.
[655] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 220; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 222.
[656] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 477-94.
[657] KVKK, Kişisel Veri İşleme Envanteri Hazırlama Rehberi, no. 61 (Ankara, 2025), 14.

verilerinin silinmesi mümkün değildir. Böyle bir durumda veri sorumlusunun, ilgili kişinin silme talebini reddetme yükümlülüğü bulunmaktadır[658].

Bazı durumlarda, saklama süresi mevzuatta düzenlenmemiş olabilir. Bu gibi hâllerde verilerin "işlendikleri amaç için gerekli olan süre" kadar saklanması esastır. Fakat bu sürenin nasıl belirleneceği, birçok durumda belirsizlik yaratmaktadır. Bu çerçevede, farklı kategorilere ait kişisel verilerin ne kadar süreyle saklanacağı hususu, açık ve belirli kurallara dayanan bir veri koruma politikası ile önceden belirlenmelidir[659]. Aksi hâlde, saklama sürelerine ilişkin belirsizlikler, veri sorumlusunun keyfî uygulamalarına zemin hazırlayabilir. Kurulun sektörel rehberler veya kararlarla standart süreler öngörmesi, uygulamada tutarlılık sağlanması açısından önemlidir[660].

İş ilişkisi bakımından düşünüldüğünde, işverenin kişisel verileri, olası yargı süreçlerinde delil olarak kullanabilmesi için zamanaşımı süresi boyunca saklaması mümkündür. Ancak burada dikkat edilmesi gereken husus; işverenin bu verileri yalnızca savunma veya hak arama amacıyla saklı tutabilmesi; bunları yeniden işleyerek yeni amaçlar doğrultusunda kullanmaması gerektiğidir[661]. Bu ayrım, veri saklama ile yeni veri işleme arasında çizilmesi gereken sınırı da göstermektedir.

Tele çalışma modelinde, çeşitli izleme ve gözetleme yöntemleriyle (örneğin, aktivite izleme yazılımları, ekran kayıtları, webcam görüntüleri, iletişim logları, uygulama kullanım verileri) toplanan kişisel verilerin saklanma süresi, bu verilerin toplanma amacıyla sıkı sıkıya bağlı olmalıdır. Bu tür veriler genellikle anlık durum tespiti, anlık performans değerlendirmesi veya belirli bir güvenlik olayının incelenmesi gibi kısa vadeli amaçlarla toplanmaktadır. Dolayısıyla, bu amaçlar gerçekleştikten sonra verilerin uzun süreler boyunca saklanması sınırlı süreyle tutulma ilkesine aykırılık teşkil edecektir[662]. Tele çalışmada kullanılan izleme yazılımlarının ürettiği büyük

---

[658] Özer Deniz, "Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk", 20.
[659] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 222.
[660] Bknz. Kişisel Verileri Koruma Kurumu, *Kişisel Veri Saklama ve İmha Politikası* (Kişisel Verileri Koruma Kurumu, 2017).
[661] Manav, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", 129-30.
[662] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 220; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 244-45; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 152; Arslan, "Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması", 221.

miktardaki veri[663] (örneğin, her gün kaydedilen klavye aktivite logları, saatlik ekran görüntüleri) göz önüne alındığında, işverenlerin bu veriler için çok kısa ve net saklama süreleri belirlemeleri ve sürenin sonunda otomatik silme veya mümkünse güvenilir anonimleştirme mekanizmaları uygulamaları bu ilkenin temel bir gereğidir[664]. Zira sürekli izleme ile üretilen terabaytlarca verinin manuel olarak yönetilmesi ve işlenme amacı ortadan kalkanların tek tek tespit edilip silinmesi fiilen imkânsızdır. Bu nedenle, gizliliğin tasarım aşamasından itibaren gözetilmesi ve başlangıçtan itibaren gizliliği esas alan yapılandırma ilkesi gereği, bu tür verileri belirli aralıklarla (örneğin, 72 saat sonra) otomatik olarak silecek şekilde yapılandırılmış sistemlerin kullanılması, bu ilkeye uyum için kritik öneme sahiptir[665]. Örneğin, günlük aktivite raporu oluşturulduktan ve çalışana geri bildirim verildikten sonra ham aktivite loglarının 24-48 saat içinde silinmesi veya bir proje tamamlandıktan sonra o projeyle ilgili anlık izleme verilerinin en geç 1 hafta içinde anonimleştirilmesi gibi politikalar benimsenebilir[666]. Tele çalışma kapsamında toplanan izleme verilerinin saklama sürelerinin, işlenme amacı doğrultusunda belirlenmesi, büyük bir titizlik gerektirmektedir. İşverenler, bu süreyi keyfi olarak uzatma eğiliminde olmamalıdır. Bu verilerin çalışanın özel hayat alanında üretildiği ve müdahaleci nitelikte olabileceği dikkate alındığında, gerekli sürenin mümkün olan en kısa zaman dilimi olarak yorumlanması ve bu sürenin somut, objektif ve önceden belirlenmiş kriterlere dayanması esastır. Sadece genel performans takibi gibi soyut bir amaç, bu verilerin aylarca veya yıllarca saklanmasını meşrulaştırmamaktadır. Fiziksel işyerlerindeki İSG kayıtlarının uzun süreli saklanması yasal bir gereklilik olsa da bu durum tele çalışanın evindeki sürekli izleme verilerinin de benzer şekilde uzun süre saklanabileceği anlamına gelmez; her veri türü ve toplanma amacı için ayrı bir değerlendirme yapılmalıdır.

Son olarak, unutulma hakkı da dolaylı olarak bu ilkeyle ilişkilidir. Özellikle çevrim içi ortamda geçmişte yaşanan bir olayın, aradan uzun bir süre geçmesine rağmen bireyin

---

[663] Valerio De Stefano ve Simon Taes, "Algorithmic Management and Collective Bargaining", *Transfer: European Review of Labour and Research* 29, sy 1 (2023): 23, https://doi.org/10.1177/10242589221141055.
[664] Falque-Pierrotin, Opinion 2/2017 on Data Processing at Work, 11.
[665] Zeynep Öğretmen Kotil, *Kişisel Verilerin Korunması Çerçevesinde Yapay Zeka* (Oniki Levha Yayıncılık, 2022), 232.
[666] Anonimleştirmeye yönelik 3.5.1.8. Bölümdeki açıklamalarımız dikkate alınarak bu işlemin gerçekleştirilmesi gerekmektedir.

aleyhine hatırlatılması, bireyin toplumsal itibarı ve kişilik hakkı üzerinde ağır bir yük oluşturabilir[667].Veri sahibinin, hakkındaki kişisel verilerin silinmesi veya yok edilmesi yönündeki talebi, sınırlı süreyle saklama ilkesi kapsamında değerlendirilmelidir. Gerek KVKK'nın 7. maddesinin 1. fıkrası gerek GDPR 17. maddesinin 1. fıkrasının (a) bendi, verilerin toplandığı veya işlendiği amaçlar için artık gerekli olmaması durumunda silinmesi gerektiğini açıkça belirtmektedir. Bir tele çalışan da hakkında toplanan ve artık işlenme amacı ortadan kalkmış olan (veya en baştan hukuka aykırı olarak toplanmış olan) izleme verilerinin (örneğin, geçmişe dönük detaylı aktivite kayıtları, eski webcam görüntüleri) silinmesini veya yok edilmesini talep edebilir. İşverenin bu talebi etkin bir şekilde değerlendirip geçerli bir istisna bulunmuyorsa yerine getirmesi gerekir. Aksi takdirde, veri sahibinin Kişisel Verileri Koruma Kuruluna şikâyet hakkı doğacak ve işveren idari ve cezai yaptırımlarla karşı karşıya kalabilecektir.

4.3.5. Doğru ve Güncel Olma

KVKK'nın 4. maddesinin 2. fıkrasının (b) bendine düzenlenen "doğru ve gerektiğinde güncel olma" ilkesi kişisel verilerin işlenmesinde uyulması gereken temel ilkelerden biridir. Bu ilke, kişisel veri işleme faaliyetlerinin yalnızca belirli, meşru ve hukuka uygun amaçlarla değil, aynı zamanda gerçekliğe uygun ve güncelliği korunmuş veriler üzerinden yürütülmesini zorunlu kılmaktadır[668]. GDPR 5. maddesinin 1. fıkrasının (d) bendinde "doğruluk" (accuracy) ilkesi benzer şekilde düzenlenmiştir. Buna göre, kişisel veriler *"doğru ve gerektiğinde güncel olmalıdır; işlendikleri amaçlar göz önüne alındığında, yanlış olan kişisel verilerin gecikmeksizin silinmesini veya düzeltilmesini sağlamak için her türlü makûl adım atılmalıdır"*[669]. Veri sorumlusunun, işleme faaliyetlerinin her aşamasında doğruluk ve güncellik ilkesine riayet etmesi, gerek ilgili

[667] Ayrıntılı bilgi için bknz. Damla Kaynar ve İştar Urhanoğlu, "İşçinin Ulaşılamama Hakkı", *Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi* 21, sy Özel Sayı (2024): 319-82; İştar Urhanoğlu vd., "İşçinin Unutulma Hakkı", içinde *İnsana Yakışır İş Serisi: 1. Cilt* (İbn Haldun Üniversitesi Yayınları, 2025), 1:211-43; KVKK, *Unutulma Hakkı (Unutulma Hakkının Arama Motorları Özelinde Değerlendirilmesi)*, no. 73 (Ankara, 2025), 11-35.
[668] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 218-19; Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 81; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 219-21.
[669] Feiler vd., The EU General Data Protection Regulation (GDPR), 73.

kişinin haklarının etkin korunması gerekse veri işleme faaliyetinin hukuka uygunluğunu sürdürebilmesi açısından KVKK ve GDPR uyarınca zorunludur[670].

Veri sorumlusunun işlediği kişisel verilerin doğru olması, bir diğer deyişle gerçeği yansıtması gerekmektedir. Özellikle bireyin kimliğine, sosyal statüsüne, mali durumuna veya sağlık verilerine ilişkin yanlış bir bilgiye dayanarak yapılan işlem, ilgili kişi açısından ağır sonuçlar doğurabilir. Bu tür hatalı veri işleme faaliyetleri, sadece kişilik hakkı ihlali oluşturmakla kalmaz; aynı zamanda veri sorumlusunun hukuki ve cezai sorumluluğunu da doğurabilir[671]. GDPR'ın "her türlü makûl adım atılmalıdır" ifadesi, veri sorumlusuna verilerin doğruluğunu sağlamak için etkin bir yükümlülük getirildiğini göstermektedir. Bu çerçevede, kişisel veriler yalnızca toplandıkları anda değil, işleme sürecinin devamında da doğruluğunu korumalıdır[672].

Tele çalışmada izleme ve gözetleme yazılımları (örneğin, aktivite takip araçları, klavye hareketlerini kaydeden yazılımlar, yapay zekâ tabanlı analiz sistemleri) tarafından toplanan veya üretilen verilerin doğru olması, bu ilke açısından zorunludur. Ancak, bu araçlar teknik hatalar içerebilir, yanlış ölçümler yapabilir veya verileri hatalı yorumlayabilir. Örneğin, bir aktivite izleme yazılımı, tele çalışanın uzun bir dokümanı okuduğu, bir telefon görüşmesi yaptığı veya bir konsept üzerinde derinlemesine düşündüğü sırada klavye/fare hareketi olmamasını, pasiflik veya çalışmama olarak yanlış kaydedebilir[673]. Benzer şekilde, yapay zekâ destekli bir duygu analiz aracı, kültürel farklılıkları, alaycı ifadeleri veya sadece yorgunluktan kaynaklanan bir ses tonunu yanlış yorumlayarak çalışanın iletişimini hatalı bir şekilde olumsuz veya ilgisiz olarak etiketleyebilir[674]. İşverenin, bu tür teknik olarak yanlış veya bağlamdan kopuk, dolayısıyla doğru olmayan verilere dayanarak çalışan hakkında karar alması (örneğin, düşük performans değerlendirmesi, prim kesintisi, disiplin işlemi), doğru veri işleme ilkesinin ihlali anlamına gelecektir. Ayrıca, tele çalışmada toplanan izleme verileri, genellikle çalışanın ev ortamının karmaşık bağlamından yoksundur. Örneğin, bir ekran

[670] Nafiye Yücedağ, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", *Kişisel Verileri Koruma Dergisi* 1, sy 1 (2019): 50-52, 1; Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 110-11.
[671] Akgül, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, 132; Yücedağ, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", 50.
[672] Yaren Sena Öztürk, "Kişisel Verilerin Korunmasında Yapay Zekânın Rolü" (Yüksek Lisans Tezi, Antalya Bilim Üniversitesi, 2024), 55.
[673] De Stefano ve Taes, "Algorithmic Management and Collective Bargaining", 24.
[674] De Stefano ve Taes, "Algorithmic Management and Collective Bargaining", 24.

görüntüsünde görünen ve işle ilgisiz gibi duran bir web sitesi, aslında çalışanın kısa bir mola sırasında kişisel bir ihtiyacını gidermek için ziyaret ettiği bir sayfa olabilir veya işle ilgili bir araştırmanın dolaylı bir parçası olabilir[675]. Bu nedenle, verilerin sadece teknik olarak doğruluğu değil, aynı zamanda bağlamsal doğruluğu da gözetilmelidir. İşveren, izleme verilerini yorumlarken bağlamı dikkate almak ve çalışana bu konuda açıklama yapma veya veriyi düzeltme imkânı sunmak için her türlü makûl adımı atmalıdır[676]. Eğer izleme verileri, çalışanın motivasyonu, bağlılığı veya stresi gibi sübjektif çıkarımlar yapmak için kullanılıyorsa, bu çıkarımların doğruluğu son derece şüpheli olabilir ve bu tür kesin olmayan verilere dayanılarak önemli kararlar alınması bu ilkeye aykırılık teşkil edecektir[677].

Bununla birlikte veri sorumlusunun kişisel verileri güncel ve doğru tutma yükümlülüğü, her durumda ilgili kişinin bilgilerini sürekli araştırma veya periyodik olarak güncelleme zorunluluğu doğurmaz. Ancak verinin güncel olmaması ilgili kişi üzerinde ciddi sonuçlar doğurabilecekse, bu durumda veri sorumlusunun doğruluk ve güncelliği düzenli biçimde denetlemesi gerekir[678]. Bununla birlikte işçinin de temel kişisel verilerinde (adres, medeni hâl vb.) meydana gelen değişiklikleri zamanında ve doğru şekilde işverene bildirme yükümlülüğü bulunmaktadır[679].

Tele çalışma bağlamında elde edilen izleme verileri, çalışanın davranış ve performansına ilişkin dinamik ve sürekli güncellenen kişisel veriler niteliğinde olabilmektedir. Bu tür verilerin işlenmesinde, güncellik ve doğruluk ilkelerine uygun hareket edilmesi gereklidir. Örneğin, bir çalışanın geçmiş döneme ait düşük performans göstergeleri, sonraki dönemlerdeki performans iyileşmelerine rağmen sistem üzerinde belirleyici olmamalıdır; işleme faaliyetleri güncel ve doğru veriler esas alınarak sürdürülmelidir. Ayrıca bu ilke, yukarıda değerlendirdiğimiz unutulma hakkı, silme hakkı ve depolama yasağı ile de yakından ilişkilidir. Zira geçmişte doğru

---

[675] Abigail M Kagan, *Big Data and Employment Law: What Employers and Their Legal Counsel Need to Know*, 2018, 198.
[676] Del Castillo, Artificial Intelligence, Labour and Society, 99; Bernhardt vd., "The Data-Driven Workplace and the Case for Worker Technology Rights", 18.
[677] De Stefano ve Wouters, AI and Digital Tools in Workplace Management and Evaluation, 16.
[678] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 220; Uncular, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, 135; Yücedağ, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", 51.
[679] Ayşe Şahin Yunak, "İş Hukukunda Kişisel Verilerin Korunması" (Yayınlanmamış Yüksek Lisans Tezi, KTO Karatay Üniversitesi, 2023), 44.

ve güncel olarak toplanmış bir kişisel veri, zamanla bireyin hukuki veya toplumsal statüsünde meydana gelen değişiklikler nedeniyle artık gerçeği yansıtmayan veya işleme amacı açısından yanlış bir duruma dönüşebilir[680]. Örneğin, bir ceza davasında sanığın beraat etmesi hâlinde, daha önce ceza aldığına ilişkin verilerin hâlen işlenmesi, artık güncelliğini ve doğruluğunu (o bağlamda) kaybetmiş bir verinin kullanılmasına neden olacaktır. GDPR 17. maddesinin 1. fıkrasının (d) bendi, kişisel verilerin hukuka aykırı olarak işlenmesi durumunda (ki, buna yanlış veri işleme de dâhildir) silinmesini gerektirir[681].

Tele çalışanın, hakkında toplanan ve yanlış olduğuna inandığı izleme verilerini (örneğin, hatalı bir üretkenlik skoru, yanlış kaydedilmiş bir aktivite, yapay zekâ tarafından yapılan hatalı bir çıkarım) KVKK'nın 11. maddesi ve GDPR 16. maddesi uyarınca düzelttirme hakkı vardır. Ancak, özellikle algoritmik sistemler tarafından üretilen karmaşık verilerin veya yorumların nasıl düzeltileceği pratik zorluklar içerebilmektedir[682]. İşveren, bu tür talepleri etkin bir şekilde karşılamak ve çalışanın veriler üzerindeki kontrolünü sağlamak için şeffaf, anlaşılır ve erişilebilir mekanizmalar kurmakla yükümlüdür. Zira izleme araçları tarafından üretilen veriler üzerinde çalışanın doğrudan bir kontrolü veya müdahale imkânı genellikle bulunmamaktadır. Bu da işverenin bu verilerin doğruluğunu temin etme sorumluluğunu artırmaktadır[683].

---

[680] Çekin vd., *Veri Hukuku*, 81; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 151-52; Yücedağ, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", 51; Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 20.
[681] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 199.
[682] Abudureyimu ve Ogurlur, "Yapay Zekâ Uygulamalarının Kişisel Verilerin Korumasına Dair Doğurabileceği Sorunlar ve Çözüm Önerileri", 766.
[683] Adams-Prassl vd., "Regulating Algorithmic Management", 128.

4.4. Veri Koruma Hukukunun İş İlişkisinin Taraflarına Getirdiği Hak ve Yükümlülükler

4.4.1. Genel Olarak

İş sözleşmesi taraflara karşılıklı hak ve borçlar getiren sinallagmatik bir sözleşmedir[684]. Bu sözleşmenin işçi ve işverene yüklediği borçlar bazı hâllerde kişisel verileri korumayı da içerebilmektedir. Ancak kişisel verilerin korunmasına ilişkin mevzuat taraflara veri sorumlusu ve ilgili kişi sıfatı ile yeni bazı hak ve yükümlülükler getirmiştir. İş ilişkilerinin sürdürülebilirliği ve tarafların temel haklarının güvence altına alınması açısından kişisel verilerin korunmasının önemi her geçen gün artmaktadır. Zira iş sözleşmesinin kişisel ilişki kuran niteliği kişisel verilerin yoğun şekilde işlenmesine yol açmaktadır. Atipik çalışma biçimlerinde işverenin kontrol ihtiyacındaki artış ve buna bağlı olarak geliştirilen yeni izleme ve gözetleme yöntemleri ile bu yöntemlere yapay zekânın entegre edilmesi işlenen kişisel veri miktarını ve niteliğini daha da artırmıştır. Bu çerçevede iş sözleşmesinin taraflarının kişisel verilerin korunması hukuku bağlamındaki hak ve yükümlülüklerinin ortaya konulması gerekmektedir.

Kişisel Verilerin Korunması Kanunu ile Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında iş ilişkisinin taraflarına yüklenen hak ve yükümlülükler aşağıda sistematik olarak ele alınacaktır. Veri sorumlusunun yükümlülükleri ile ilgili kişinin hakları Kişisel Verilerin Korunması Kanunu'nun "Haklar ve Yükümlülükler" başlıklı üçüncü bölümünde düzenlenmiştir. Üç maddeden oluşan bu bölümün ilk düzenlemesi "aydınlatma yükümlülüğü" kenar başlıklı 10. maddesidir. 11. madde ilgili kişinin haklarına ilişkin düzenleme getirmekte olup, 12. madde de ise "veri güvenliğine ilişkin yükümlülükler" hükme bağlanmıştır.

[684] Süzek ve Başterzi, *İş Hukuku*, 357-541; Çelik vd., *İş Hukuku Dersleri*, 302-457; Sümer, *İş Hukuku*, 67-95.

4.4.2. Veri Sorumlusunun Yükümlülükleri

4.4.2.1. Aydınlatma Yükümlülüğü

Veri sorumlusunun yerine getirmesi gereken en temel yükümlülüklerden biri, KVKK'nın 10. maddesinde açıkça düzenlenen aydınlatma yükümlülüğüdür[685]. İşverenin işçiye ait kişisel verileri işlerken KVKK 10. maddesinde belirtilen bu yükümlülüğü eksiksiz şekilde yerine getirmesi, hem işçinin KVKK 11. maddesinde sayılan haklarını etkin bir şekilde kullanabilmesi hem de veri işleme faaliyetinin meşruiyetinin sağlanması açısından büyük önem arz eder[686]. Belirtmek gerekir ki, KVKK 10. maddesinin 1. fıkrasına göre aydınlatma yükümlülüğü, kişisel verilerin elde edilmesinden önce veya en geç elde edildiği anda yerine getirilmelidir[687]. Veri sorumlusu, bu yükümlülüğü ilgili kişinin herhangi bir talebi olmaksızın, kendiliğinden ifa etmek zorundadır[688]. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'e göre, *"Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine bağlı değildir"*[689]. Başka bir deyişle, bu yükümlülük ilgili kişinin rıza göstermesine, bilgilendirilmeyi talep etmesine veya işlemeye açıkça itiraz etmesine bağlı olmayan, mutlak ve objektif bir yükümlülüktür[690].

---

[685] Ayrıntılı bilgi için bkmz. Özlem Acar Ünal, "Veri Sorumlusunun Aydınlatma Yükümlülüğü", *Banka ve Finans Hukuku Dergisi* 8, sy 32 (2019): 1325-78; Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 256; Ali Demirbaş, *Kişisel Verileri Koruma Hukukunda Veri Sorumlusu ve Yükümlülükleri* (Oniki Levha Yayıncılık, 2023), 59.

[686] Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 39; Demirbaş, *Kişisel Verileri Koruma Hukukunda Veri Sorumlusu ve Yükümlülükleri*, 65.

[687] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 248; Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 40; Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 253-54.

[688] Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 42.

[689] Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, Resmî Gazete, 10.03.2018, Sayı: 30356. Kurul, çevrim içi bir platform aracılığıyla iş başvurusu alan bir veri sorumlusu şirketler topluluğu hakkında re'sen inceleme başlatarak verdiği kararda, aydınlatma yükümlülüğünün yerine getirilmesinin herhangi bir onaya tabi olmadığını açıkça belirtmiştir. Kararda şu ifadelere yer verilmiştir: "Aydınlatma yükümlülüğünün yerine getirilmesindeki amaç, kişisel verilerin işlenmesi bakımından ilgili kişinin bilgi sahibi olmasını sağlamaktır. Buna karşın açık rıza alınmasının amacı, veri sorumlusunun kişisel veri işleme faaliyetini hukuka uygun hâle getirecek bir gerekçeye dayanmasıdır. Dolayısıyla, ilgili kişi aydınlatma metni sayesinde veri işleme faaliyeti hakkında bilgi edinmiş olsa da, bu metinde yer alan hususlara açık rıza vermek zorunda değildir." "Veri sorumlusu tarafından aydınlatma yükümlülüğü ve açık rıza onayı alınması süreçlerinin ayrı ayrı yerine getirilmesi gerektiği ile ilgili" Kişisel Verileri Koruma Kurulunun Kararı, No. 2018/90 (26 Temmuz 2018), https://www.kvkk.gov.tr/Icerik/5420/2018-90.

[690] Mesut Serdar Çekin, *Yapay Zekâ Teknolojilerinin Hukuki İşlem Teorisine Etkileri* (Onikilevha Yayıncılık, 2021), 178; Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 255.

KVKK'nın 10. maddesi ve Tebliğ'in 4. maddesi uyarınca, kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere en azından şu hususlarda bilgi vermekle yükümlüdür: veri sorumlusunun ve varsa temsilcisinin kimliği; kişisel verilerin hangi amaçla işleneceği, kişisel verilerin kimlere ve hangi amaçla aktarılabileceği; veri toplamanın yöntemi ve hukuki sebebi ile KVKK 11. maddesinde sayılan diğer haklar[691]. Buna karşılık GDPR ise aydınlatma yükümlülüğünü, verinin toplandığı kaynağı esas alarak daha detaylı bir yaklaşımla düzenlemektedir. Bu çerçevede, GDPR'ın 13. maddesi verilerin doğrudan ilgili kişiden toplandığı durumları, 14. maddesi ise dolaylı yollarla başka kaynaklardan elde edildiği durumları ele alarak farklı bilgilendirme içerikleri öngörmüştür. Bu bilgilendirmenin zamanlaması da kritik bir öneme sahiptir. GDPR, aydınlatmanın veri işleme başlamadan, özellikle de bireyin haklarını derinden etkileyebilecek otomatik karar verme süreçleri devreye girmeden önce yapılmasını zorunlu kılmaktadır[692].

Önemle belirtilmelidir ki, KVKK 10. maddesi kapsamındaki aydınlatma yükümlülüğü ile KVKK 5. maddesinin 1. fıkrası ve KVKK 6. maddesinin 3. fıkrasının (a) bendi kapsamındaki açık rıza alma işlemleri birbirinden bağımsızdır ve ayrı ayrı yerine getirilmelidir. Tebliğ'in 5. maddesinin 1. fıkrasının (f) bendinde yer alan düzenlemede *"Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir"* ifadesine yer verilmiştir. Bu ifade, açık rıza alınması sırasında yapılan aydınlatmanın aynı metin içinde sunulması şeklindeki yaygın uygulamanın geçersiz olduğunu açıkça ortaya koymaktadır[693].

---

[691] Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 175-76.

[692] GDPR kapsamındaki bilgilendirme yükümlülüğü, KVKK ile kıyaslandığında daha ayrıntılı ve bağlam temelli bir yapıdadır. Özellikle GDPR'da, veri koruma görevlisinin (DPO) iletişim bilgileri, verilerin saklama süresi, otomatik karar alma süreçleri, rıza geri çekme hakkı ve denetim makamına şikâyette bulunma hakkı gibi unsurların da açıkça bildirilmesi zorunlu tutulmuştur. KVKK'da bu gibi hususlara doğrudan yer verilmese de Tebliğ, aydınlatma yükümlülüğünün detaylarını belirlemiştir. Tebliğ uyarınca bilgilendirmenin "anlaşılır, açık ve sade bir dil" kullanılarak yapılması, "genel nitelikte ve muğlak ifadelere" yer verilmemesi ve işleme amacının "belirli, açık ve meşru" olması zorunludur. Ayrıca, veri işlemenin hukuki sebebinin, Kanun'un 5. ve 6. maddelerindeki işleme şartlarından hangisine dayandığının açıkça belirtilmesi gerekir. Ayrıntılı bilgi için bknz. Çekin, *Yapay Zekâ Teknolojilerinin Hukuki İşlem Teorisine Etkileri*, 178, 207-10; Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 254-268,364-367; Sandra Wachter vd., "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR", *Harv. JL & Tech.* 31 (2017): 869-70.

[693] Cem Sarıkabadayı, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri" (Yayınlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi, 2024), 54.

Aydınlatma yükümlülüğünün rızadan bağımsız ve kendiliğinden yerine getirilmesi gereken temel bir yükümlülük olması, bu bilgilendirmenin şekil ve içerik olarak da belirli standartlara tabi olmasını gerektirmektedir. Aydınlatmanın şekli de KVKK 10. maddesi ve ilgili Tebliğ açısından önem taşımaktadır. Tebliğ uyarınca bu yükümlülük, yazılı (elektronik ortam dâhil), sözlü (ispat yükümlülüğü veri sorumlusuna ait olmak üzere), ses kaydı gibi çeşitli fiziksel veya elektronik yöntemlerle ve hatta iş sözleşmesine eklenen hükümler aracılığıyla yerine getirilebilmektedir[694]. Hangi yöntem seçilirse seçinsin, bilgilendirme metinlerinin "anlaşılır, açık ve sade bir dil" ile hazırlanması; muğlak, genel geçer veya yanıltıcı ifadelerden kaçınılması esastır[695]. Ayrıca, iş süreçlerindeki değişikliklere paralel olarak bu metinlerin periyodik olarak güncellenmesi, veri işleme faaliyetinin şeffaflığının sürdürülebilirliği açısından gereklidir[696].

Bu genel usul ve esasların ötesinde, aydınlatma yükümlülüğünün içeriği, özellikle yapay zekâ destekli teknolojilerin ve otomatik karar verme mekanizmalarının yaygınlaşmasıyla yeni ve daha karmaşık bir boyut kazanmaktadır. Profilleme dâhil olmak üzere otomatik karar verme mekanizmalarının varlığı hâlinde, bu mekanizmaların işleyiş mantığı, amacı ve veri sahibi açısından öngörülen sonuçları hakkında anlamlı ve anlaşılabilir bilgiler verilmesi gerekmektedir. Bu gereklilik, özellikle yapay zekâ destekli izleme ve karar verme süreçlerinde daha da karmaşık ve önemli bir hâl almaktadır. Bu noktada, algoritmik şeffaflık kavramı merkezi bir önem kazanmaktadır[697]. Algoritmik şeffaflık, bir sistemin sonuçlarını kullanıcıların anlayabileceği şekilde açıklayabilmesi ve bu sistemlerden etkilenen kişilerin, kararların hangi faktörlere dayandığını anlamasını sağlamasıdır[698]. Zira bu şeffaflık sağlanmadan, çalışanın bir karara etkin bir şekilde itiraz etmesi ya da olumsuz etkilendiğini kanıtlaması neredeyse imkânsız hâle gelmektedir[699]. Bu doğrultuda,

---

[694] GDPR 12. maddesinde de benzer şekilde bilgilendirmenin "öz, şeffaf, anlaşılır ve kolay erişilebilir bir biçimde, açık ve sade bir dil kullanılarak" yapılmasını şart koşar. Bu metinlerin iş süreçlerindeki değişikliklere göre periyodik olarak güncellenmesi, veri işleme faaliyetinin şeffaflığı bakımından gereklidir. Ayrıntılı bilgi için bknz. Hüseyin Can Aksoy, "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme", *Kişisel Verileri Koruma Dergisi* 4, sy 2 (2022): 12, 2.
[695] Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 39-42.
[696] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 257.
[697] Del Castillo, *Artificial Intelligence, Labour and Society*, 131.
[698] Çekin, *Yapay Zekâ Teknolojilerinin Hukuki İşlem Teorisine Etkileri*, 179.
[699] Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 92-93; Bozkurt Gümrükçüoğlu ve Yakacak, "Yapay Zekânın İşe Alım Süreçlerinde Kullanımı ve Algoritmik Ayrımcılık", 1726.

çalışanlara sadece KVKK'nın gerektirdiği temel bilgileri sunmak yeterli görülmemektedir. Kanaatimizce GDPR uyarınca da belirtilen anlamlı bilgi sağlama yükümlülüğü getirilmektedir. Bu ilkeyi daha da somutlaştıran AB Yapay Zekâ Tüzüğü ise, sistemi kullanan işverene (dağıtıcı), çalışanlarını kullandığı sistem hakkında bilgilendirme ve özellikle yüksek riskli sistemlerde, talep üzerine kararın nasıl alındığına dair açık ve anlamlı bir açıklama sunma yükümlülüğü getirmekte; çalışanlara ise bu açıklamayı talep etme hakkı tanımaktadır[700]. Bu yaklaşım, aydınlatma yükümlülüğünü, verinin işlendiği bilgisinden kararın nasıl üretildiği bilgisine doğru genişleten önemli bir adımı teşkil etmekte ve hukukumuzda da benzer bir düzenlemenin benimsenmesi isabetli görülmektedir.

İş ilişkisi bağlamında değerlendirildiğinde, işverenin işçinin verisini işleme niyetinin bulunduğu her durumda, işleme faaliyeti başlamadan önce işçiyi KVKK 10. maddesinde belirtilen hususlarda bilgilendirmesi gerekmektedir[701]. Tele çalışma özelinde ise aydınlatma yükümlülüğünün, işverenin yalnızca izleme yapıldığına dair genel bir bildirimde bulunmasının ötesinde, detaylı ve spesifik bilgiler içermesi zorunludur. İşveren, bir izleme yazılımı kullanıp kullanmadığı, kullanıyorsa izleme yazılımının adını, hangi verileri (klavye hareketleri, ekran görüntüleri, uygulama kullanımı vb.) ne sıklıkta ve ne kadar süreyle topladığını; bu verileri analiz eden bir yapay zekâ algoritması varsa bu algoritmanın temel çalışma mantığını ve bu analizin çalışanın performansı veya geleceği hakkında ne gibi sonuçlar (örneğin, otomatik olarak düşük performans uyarısı üretme) doğurabileceğini açık ve anlaşılır bir dille anlatmakla yükümlüdür. Sadece performans takibi gibi genel bir amaç beyanı, bu ilkenin ve şeffaflık beklentisinin açık bir ihlalini teşkil etmektedir.

4.4.2.2. İlgili Kişinin Başvurularının Alınması ve Sonuçlandırılması Yükümlülüğü

Kişisel verilerin korunması hukukunda, ilgili kişinin başvurularını alma ve sonuçlandırma yükümlülüğü, veri sorumlusunun temel arasında yer almaktadır. Bu yükümlülük, ilgili kişinin KVKK ve GDPR kapsamında düzenlenen haklarını etkin ve

[700] Voigt ve Hullen, *The EU AI Act*, 118-21.
[701] Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 209-11.

anlamlı bir biçimde kullanabilmesini sağlamak bakımından merkezi bir önem taşımaktadır[702]. Veri sorumlusunun bu yükümlülüğü ihlal etmesi, yalnızca usule ilişkin bir eksiklik olarak değil, aynı zamanda ilgili kişinin temel haklarının ihlali olarak da değerlendirilmesi gerekmektedir[703]. Veri sorumlusunun bu yükümlülüğü, yalnızca taleplerin alınmasını değil, aynı zamanda bu taleplere süresi içinde ve hukuka uygun şekilde cevap verilmesini de kapsamaktadır. İlgili kişinin veri sorumlusuna başvuru süreci KVKK 13. madde ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ[704] ile düzenlenmiştir[705].

---

[702] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 341; Dülger, *Kişisel Verilerin Korunması Hukuku*, 353.

[703] Dülger, *Kişisel Verilerin Korunması Hukuku*, 354. GDPR'ın 12. maddesinin 2. fıkrasına göre, veri sorumlusu, GDPR'ın 15 ile 22. maddeleri arasında sıralanan haklarını kullanabilmesi için her türlü kolaylığı sağlamak zorundadır.

[704] Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, Resmî Gazete, 10.03.2018, Sayı: 30356.

[705] Veri sorumlusunun talep karşısındaki tutumu, hukuka uygunluk ilkesine bağlı olarak şekillenmelidir. İlgili kişi tarafından yapılan taleplerin açıkça temelsiz ya da orantısız olması hâlinde veri sorumlusu bu talepleri KVKK 13. maddesinin 3. fıkrası uyarınca gerekçesini açıklayarak reddedebilir. GDPR 12. maddesinin 5. fıkrasında da benzer bir düzenleme yer alır ve bu durumda ispat yükümlülüğü veri sorumlusuna aittir. Ancak, bu durum istisnadır ve veri sorumlusu, ret kararında hukuka ve dürüstlük kuralına uygun, açık ve ölçülü bir gerekçe sunmakla yükümlüdür. Aksi takdirde, ilgili kişi KVKK 14. maddesi uyarınca Kurul'a şikâyet yoluna başvurabilir ve bu başvuru sonucunda veri sorumlusu hakkında idari yaptırımlar (KVKK 18. madde) uygulanabilir. GDPR kapsamında da veri sahibi, 77. madde uyarınca bir denetim makamına şikâyette bulunma ve 79. madde uyarınca etkili bir yargısal yola başvurma hakkına sahiptir. İlgili kişinin başvuru usulü, "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ" ile ayrıntılı olarak düzenlenmiştir. Tebliğ'e göre başvurunun Türkçe yapılması zorunludur. Başvuru; yazılı olarak, kayıtlı elektronik posta (KEP), güvenli elektronik imza, mobil imza veya veri sorumlusunun sisteminde kayıtlı olan e-posta adresi üzerinden yapılabilir. Başvuruda; ad, soyad, imza (yazılı başvuruda), T.C. kimlik numarası (yabancılar için uyruk/pasaport numarası), tebligat adresi, varsa iletişim bilgileri ve talep konusunun bulunması zorunlu tutulmuş, ayrıca ilgili bilgi ve belgelerin de eklenmesi gerektiği belirtilmiştir. Taleplerin sonuçlandırılmasına ilişkin olarak ise veri sorumlusu, başvuruyu en geç otuz gün içinde ve kural olarak ücretsiz sonuçlandırmakla yükümlüdür. GDPR'ın 12. maddesinin 3. fıkrasında da benzer şekilde "bir aylık" bir süre öngörülmekte, ancak bu sürenin talebin karmaşıklığına göre gerekçesi bildirilerek iki ay daha uzatılabileceği düzenlenmektedir. KVKK kapsamında, işlemin ayrıca bir maliyet gerektirmesi halinde ücret talep edilebilmektedir. Bu çerçevede, yazılı cevabın on sayfayı aşması durumunda her sayfa için 1 Türk Lirası işlem ücreti alınabilir; yanıtın CD veya flash bellek gibi bir ortamda verilmesi halinde ise ücret, ortamın maliyetini geçemez. Ancak, talebin veri sorumlusunun hatasından kaynaklandığı hallerde alınan ücret iade edilmek zorundadır. GDPR'ın 12. maddesinin 5. fıkrası ise, yalnızca "açıkça temelsiz veya aşırı" taleplerde veri sorumlusuna makul bir ücret talep etme veya talebi yerine getirmeyi reddetme imkânı tanır. Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 348-51; Mehmet Bedii Kaya, "Kişisel Verilerin İşlenmesi ve Korunması Arasındaki Denge", içinde *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku*, ed. Ali Cem Bilgili ve Leyla Keser Berber, Marmara Hukuk Bilimsel Toplantılar Serisi – 1 (On İki Levha Yayıncılık, 2020), 48-52; Demirbaş, *Kişisel Verileri Koruma Hukukunda Veri Sorumlusu ve Yükümlülükleri*, 142. Öte yandan, bazı durumlarda KVKK Madde 28 kapsamındaki istisnalar gereği, veri sorumlusunun ilgili kişinin taleplerini karşılama yükümlülüğü doğmayabilir. Örneğin, kişisel verilerin millî güvenlik, kamu düzeni, suç soruşturması gibi amaçlarla işlendiği hâllerde veri sorumlusunun bu taleplere yanıt verme yükümlülüğü bulunmayabilir. GDPR Madde 23 de benzer şekilde, Birlik veya Üye Devlet hukukunun, belirli gerekçelerle (ulusal güvenlik, savunma, kamu güvenliği, suçların önlenmesi veya soruşturulması vb.) veri sahibi haklarının kapsamını kısıtlayabileceğini öngörür; ancak bu kısıtlamaların temel hak ve özgürlüklerin özüne saygı göstermesi ve demokratik bir toplumda gerekli ve orantılı bir tedbir olması şarttır. Her iki düzenlemede de bu

Tele çalışma bağlamında bu haklar, çalışanın işverenine başvurarak belirli konularda bilgi talep etmesini kapsamaktadır. Çalışan bu kapsamda; kendisi hakkında hangi izleme yazılımlarının kullanıldığını, bu yazılımlar aracılığıyla hangi kişisel verilerinin (ör. ekran görüntüleri, klavye hareketleri, web sitesi geçmişi) toplandığını, bu verilerle üretilen performans puanı veya analiz raporlarının bir kopyasını, verilerinin kimlerle paylaşıldığını ve ne kadar süreyle saklandığını sorgulama hakkına sahip bulunmaktadır. İşveren, bu talebe 30 gün içinde ücretsiz olarak yanıt vermekle yükümlü olup, bu yanıtta topladığı her bir veri kategorisini ve işleme amacını açıkça belirtmesi gerekmektedir. Talebin açıkça dayanaktan yoksun veya orantısız olmadığı müddetçe reddedilmesi ise hukuka aykırılık teşkil etmektedir.

4.4.2.3. Veri Güvenliğini Sağlama Yükümlülüğü

Kişisel verilerin korunması hukukunda veri güvenliğine ilişkin yükümlülük, veri sorumlusunun en temel ve sürekli nitelikteki yükümlülüklerinden birini oluşturmaktadır[706]. Bu yükümlülük, KVKK 12. maddesinde açıkça düzenlenmiştir. KVKK Madde 12(1), veri sorumlusunun; *"(a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, (b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, (c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda"* olduğunu belirtmektedir[707]. Bu yükümlülüğün amacı, kişisel verilerin hukuka aykırı biçimde işlenmesini, yetkisiz erişime maruz kalmasını ve izinsiz şekilde ifşa edilmesini önlemek ve bu verilerin bütünlük, gizlilik ve erişilebilirlik çerçevesinde muhafaza edilmesini güvence altına almayı amaçlamaktadır[708].

---

istisnaların dar yorumlanması gerektiği hususunda öğretide genel bir görüş birliği bulunmaktadır. Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 265-66; Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 182-83.

[706] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 228; Demirbaş, *Kişisel Verileri Koruma Hukukunda Veri Sorumlusu ve Yükümlülükleri*, 663 vd.

[707] Bu kapsamda alınacak teknik ve idari tedbilere ilişkin Kurum bir rehber yayınlamıştır. Bknz. Kişisel Verileri Koruma Kurumu, *Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)*, no. 72 (Kişisel Verileri Koruma Kurumu, 2025).

[708] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 315; Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 185-87; Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 228.

GDPR da veri güvenliğine büyük önem atfetmektedir. GDPR 5. maddesinin 1. fıkrası, temel işleme ilkelerinden biri olarak kişisel verilerin *"yetkisiz veya hukuka aykırı işlemeye ve kazara kayba, yok olmaya veya hasara karşı koruma dahil olmak üzere uygun teknik veya organizasyonel tedbirler kullanılarak kişisel verilerin uygun güvenliğini sağlayacak şekilde işlenmesi gerektiğini"* belirtmektedir. Bu ilke, GDPR madde 32'de (İşlemenin Güvenliği) detaylandırılmıştır. GDPR 32. maddesinin 1. fıkrası, veri sorumlusu ve veri işleyenin, "*riske uygun bir güvenlik düzeyini sağlamak için uygun teknik ve organizasyonel tedbirleri uygulamasını"* gerektirmektedir. Bu tedbirler belirlenirken, teknolojinin mevcut durumu, uygulama maliyetleri, işlemenin niteliği, kapsamı, bağlamı ve amaçları ile gerçek kişilerin hak ve özgürlükleri açısından değişen olasılık ve ciddiyetteki risklerin dikkate alınması gerekmektedir.[709]. GDPR, bu tedbirlere örnek olarak kişisel verilerin takma adla anonimleştirilmesi ve şifrelenmesi; işleme sistemlerinin ve hizmetlerinin süregelen gizliliğini, bütünlüğünü, kullanılabilirliğini ve dayanıklılığını sağlama yeteneği gibi unsurları saymaktadır.

Dolayısıyla, hem KVKK madde 12 hem de GDPR madde 32, veri sorumlularına, işledikleri kişisel verilerin güvenliğini sağlamak üzere etkin bir şekilde "gerekli" ve "uygun" teknik ve idari tedbirleri alma yükümlülüğü getirmektedir[710]. GDPR'ın yaklaşımında, "riske uygun bir güvenlik düzeyi" ifadesiyle risk temelli bir yaklaşımın açıkça benimsendiği görülmekteyken, KVKK'nın "uygun güvenlik düzeyi" ifadesi de benzer bir bağlamsal değerlendirmeyi işaret etmektedir[711]. Her iki düzenlemenin de temel hedefi, kişisel verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini koruyarak veri ihlallerini önlemektir. Bu yükümlülük, GDPR Madde 24 (Veri sorumlusunun sorumluluğu) ve Madde 25 (Tasarım ve varsayılan ayar olarak veri koruma) ile de desteklenmektedir.

Tele çalışma modeli, veri güvenliği yükümlülüğünü işveren açısından daha da karmaşık hâle getirmektedir. Çalışanların, güvenliği işveren tarafından tam olarak kontrol edilemeyen ev ağlarından kurumsal sistemlere bağlanması; hassas verilerin, üzerinde hem kişisel hem de kurumsal bilgilerin bulunduğu cihazlarda işlenmesi ve

---

[709] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 315.
[710] Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 186-87.
[711] Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 186-87.

izleme yazılımları tarafından toplanan verilerin (ekran görüntüleri, iletişim kayıtları) aktarımı ve saklanması gibi süreçler, özel güvenlik riskleri doğurmaktadır[712]. Bu nedenle işverenin uygun güvenlik düzeyini belirlerken, bu özel riskleri (örneğin, çalışanın evindeki modem güvenliği, cihazın aile bireyleri tarafından kullanılma ihtimali) dikkate alması ve aşağıda belirtilen teknik tedbirleri uygulaması gerekmektedir.

4.4.2.4. Kurul Kararlarını Yerine Getirme Yükümlülüğü

Kişisel verilerin korunması hukukunda, veri sorumlularının denetim makamlarının kararlarına uyma yükümlülüğü, yasal rejimlerin etkinliğinin temelini oluşturmaktadır. KVKK kapsamında Kişisel Verileri Koruma Kurulu, veri işleme faaliyetlerinin hukuka uygunluğunu denetleyerek ihlallerin giderilmesine yönelik bağlayıcı kararlar alma yetkisine sahip bulunmaktadır[713]. Bu yapıya paralel olarak, GDPR da üye devletlerin denetim makamlarına (Supervisory Authorities) benzer şekilde geniş düzeltici yetkiler tanımış; bu kapsamda hukuka aykırı işlemeyi durdurma, veri silme veya işlemeyi kısıtlama gibi emredici kararlar alma gücü vermiştir[714].

Bu kararların icrasını teminat altına alan en önemli mekanizmayı ise yaptırımlar oluşturmaktadır. Hem KVKK hem de GDPR, denetim makamlarının emirlerine uyulmaması durumunda caydırıcı nitelikte ve yüksek meblağlara ulaşabilen idari para cezaları öngörmektedir. Ayrıca, her iki düzenlemede de kararların yerine getirilmesi

---

[712] Falque-Pierrotin, *Opinion 2/2017 on Data Processing at Work*, 16.

[713] KVKK'nın 15. maddesi, Kurul'un inceleme ve karar alma süreçlerini düzenler. Bu madde uyarınca Kurul, şikâyet üzerine veya bir ihlal iddiasını öğrenmesi durumunda resen yaptığı inceleme sonucunda bir ihlalin varlığını tespit ederse, hukuka aykırılıkların veri sorumlusu tarafından giderilmesi yönünde karar alabilir. Bu karar, ilgili veri sorumlusuna resmî tebligat yoluyla bildirilir. Kararın niteliğine göre, veri sorumlusu tarafından derhâl veya Kurulca belirlenen süre içinde yerine getirilmesi zorunludur. KVKK 15. maddesinin 6. fıkrası uyarınca, Kurul'un ihlalin yaygın olması durumunda alabileceği ilke kararları ise, yalnızca belirli bir olaya özgü olmayıp, benzer durumlarda yol gösterici nitelik taşıması bakımından tüm veri sorumluları için bağlayıcıdır. Kurul, bir ilke kararı tesis etmeden önce ihtiyaç duyması durumunda, ilgili kamu kurumları ve diğer yetkili kuruluşlardan görüş talep edebileceği düzenlenmiştir. Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 354-56; Güler, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Kişisel Verilerinin Korunması", 92.

[714] GDPR 58. maddesinin 2. fıkrası, denetim makamlarının sahip olduğu düzeltici yetkileri sıralar. Bu yetkiler arasında, veri sorumlusuna veya veri işleyene *"işleme faaliyetlerini Tüzük hükümlerine uygun hale getirmesi için belirli bir şekilde ve belirli bir süre içinde emir verme"*, "*işlemeye geçici veya kesin bir yasaklama dahil olmak üzere sınırlama getirme"* veya *"kişisel verilerin düzeltilmesini veya silinmesini ya da işlenmesinin kısıtlanmasını emretme"* gibi kararlar alma yetkisi bulunur. Veri sorumluları ve veri işleyenler, bu kararlara uymakla yükümlüdür. Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 244.

için niteliklerine göre farklılık gösteren net süreler belirlenmiştir. Dolayısıyla, kararlara uyma yükümlülüğü ve bu yükümlülüğün ihlaline bağlanan ciddi sonuçlar, modern veri koruma rejimlerinin işlerliği için merkezi bir rol oynamaktadır[715].

4.4.2.5. Veri Sorumluları Siciline Kayıt Yükümlülüğü

Kişisel verilerin korunması hukukunda Veri Sorumluları Siciline (VERBİS) kayıt yükümlülüğü, KVKK 16. maddesinde düzenlenmiş olup, veri sorumlularına getirilen temel yükümlülüklerden birini oluşturmaktadır[716]. VERBİS, Kurum'un gözetiminde tutulan ve KVKK madde 16. maddesinin 1.fıkrası uyarınca kamuya açık olan elektronik bir kayıt sistemidir[717]. Sicilin amacı; kişisel veri işleme faaliyetlerinin izlenebilirliğini sağlamak, veri sorumlularını hukuka uygun veri işleme noktasında KVKK madde 12'deki veri güvenliği yükümlülükleri gibi sorumluluklar altına almak ve ilgili kişilerin verileri üzerinde denetim hakkını etkin şekilde kullanmasına yardımcı olmaktır[718]. KVKK 16.maddenin 2. fıkrası kural olarak kişisel verileri işleyen gerçek ve tüzel kişilerin, veri işlemeye başlamadan önce VERBİS'e kaydolmak zorunda olduğunu belirtmekte, ancak Kurul'un belirli objektif kriterlere göre istisnalar getirebileceğini de eklemektedir[719].

---

[715] Özellikle kişisel verilerin hukuka aykırı olarak işlendiği ve bu işlemelerin telafisi güç veya imkânsız zararlara yol açabileceği durumlarda Kurul, KVKK 15. maddesinin 7. fıkrası uyarınca veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar verebilir ve bu tür kararlar derhâl uygulanmayı gerektirir. Diğer kararlar için ise, örneğin verilerin silinmesi, yok edilmesi, anonimleştirilmesi veya ilgili kişilere yönelik aydınlatma eksikliklerinin giderilmesi gibi işlemleri içeren kararlar, KVKK 15. maddesinin 5. fıkrası gereğince, gecikmeksizin ve en geç tebliğ tarihinden itibaren otuz gün içinde yerine getirilmelidir. GDPR'da ise denetim makamları, GDPR 58. maddesinin 2. fıkrasının (d) bendi uyarınca emirlerini "belirli bir süre içinde" yerine getirilmesini isteyebilir; acil durumlarda derhal etkili olacak yasaklamalar da getirebilirler. Kurul kararlarına uymamanın yaptırım KVKK 18. maddesinin 1. fıkrasının (c) bendinde idari para cezası olarak düzenlenmiştir. Benzer şekilde, GDPR 83. maddesinin 5. fıkrasının (e) bendi ve GDPR 83. maddesinin 6. fıkrası, denetim makamının emirlerine uyulmaması durumunda çok yüksek meblağlara varabilen idari para cezaları öngörür. Çelikel, "Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri", 194; Özdemir Coşkun, "Kişisel Verilerin Korunması ve İşlenmesi", 135; Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 244, 292.

[716] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 259; Demirbaş, *Kişisel Verileri Koruma Hukukunda Veri Sorumlusu ve Yükümlülükleri*, 113.

[717] Ekmekçi vd., *Anayasa Mahkemesine bireysel başvurunun temel esasları ve iş ve sosyal güvenlik hukukuna ilişkin kararlar*, 287-93.

[718] Güler, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Kişisel Verilerinin Korunması", 103.

[719] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 259; Demirbaş, *Kişisel Verileri Koruma Hukukunda Veri Sorumlusu ve Yükümlülükleri*, 113.

GDPR ise, VERBİS gibi merkezi ve kamuya açık bir veri sorumluları sicili tutulmasını genel bir yükümlülük olarak öngörmemektedir. GDPR, Yönerge'nin 18. maddesinde yer alan kayıt zorunluluğunu yürürlükten kaldırarak, yerine 35. maddede risk değerlendirmesine ilişkin yeni düzenlemelere yer vermiştir[720]. yrıca GDPR'ın bu konudaki temel mekanizmasını, madde 30'da düzenlenen "işleme faaliyetlerinin kaydı" (records of processing activities) yükümlülüğü oluşturmaktadır. GDPR madde 30 uyarınca, her veri sorumlusu (ve varsa temsilcisi), sorumluluğu altındaki işleme faaliyetlerinin bir kaydını tutmakla yükümlü bulunmaktadır. Benzer bir yükümlülük veri işleyenler için de geçerli olmaktadır. Bu kayıtların yazılı (elektronik format dâhil) olması ve denetim makamının talebi üzerine sunulması gerekmektedir[721].

4.5. İlgili Kişinin Hakları

4.5.1. Genel Olarak

İlgili kişi kişisel verileriyle ilgili olarak KVKK 11. maddesinin 1. fıkrası uyarınca:

> *"Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;*
> *a) Kişisel veri işlenip işlenmediğini öğrenme,*
> *b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,*
> *c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,*
> *ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,*
> *d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,*
> *e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,*
> *f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,*
> *g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,*
> *ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir".*

---

[720] Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*.
[721] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 155.

Aşağıda, ilgili kişinin sahip olduğu; bilgi edinme hakkı, düzeltme talep etme hakkı, kişisel verilerin silinmesini ve yok edilmesini talep etme hakkı, otomatik kararlara itiraz etme hakkı, algoritmik karar süreçlerine ilişkin bilgi edinme hakkı, alternatif senaryo açıklamaları ve zararın tazminini isteme hakkı ayrı başlıklar altında incelenecektir.

4.5.2. Bilgi Edinme Hakkı / Erişim Hakkı

Kişisel verilerin korunması hukukunda ilgili kişinin veri üzerindeki denetimini ve kontrolünü sağlamaya yönelik en temel haklardan birini, KVKK'nın 11. maddesinde düzenlenen bilgi edinme hakkı oluşturmaktadır[722]. Sözü geçen düzenleme uyarınca ilgili kişiye; kişisel verilerinin işlenip işlenmediğini öğrenme, işlenmişse buna ilişkin bilgi talep etme, işleme amacını ve amaca uygun kullanılıp kullanılmadığını öğrenme ile yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme hakları tanınmaktadır. GDPR 15. maddesinin 1. fıkrası ise ilgili kişiye; veri işleme amaçları, veri kategorileri, alıcılar, saklama süresi, düzeltme, silme, işleme kısıtlama ve itiraz hakları, şikâyet hakkı, verilerin kaynağı ve varsa otomatik karar verme süreçlerine ilişkin mantık ve sonuçlara dair anlamlı bilgiler gibi unsurları öğrenme imkânı sağlayarak daha kapsamlı bir erişim hakkı tanımaktadır[723].

Aynı zamanda "erişim hakkı" (right of access)[724] olarak da anılan bu hak, bireyin kendisine ait kişisel verilerin işlenip işlenmediğini öğrenmesini, işlendiği takdirde bu verilerle ilgili detaylara erişmesini ve bu bilgilere dayanarak gerektiğinde diğer haklarını kullanmasını mümkün mümkün kılmaktadır[725].

Bilgi edinme hakkı, kişisel verilerin korunması hukukunun yalnızca şekli değil, aynı zamanda özüne de temas eden temel bir unsuru oluşturmaktadır[726]. Zira bireyin

---

[722] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 377.
[723] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 378.
[724] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 248.
[725] Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 203; Uncular, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, 66; Aydın Akgül, *Kişisel Verilerin Korunması* (Beta, 2014), 141; Öğretmen Kotil, *Kişisel Verilerin Korunması Çerçevesinde Yapay Zeka*, 132-35.
[726] Çekin, *Yapay Zekâ Teknolojilerinin Hukuki İşlem Teorisine Etkileri*, 150-53; Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, 88; İbrahim Korkmaz, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", *TBB Dergisi*, sy 124 (2016): 131; Çelikel, "Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri", 101.

kendisine ait veriler hakkında bilgi sahibi olmaması, düzeltme, silme, işleme faaliyetlerine itiraz ve rızayı geri çekme gibi diğer haklarını da etkin bir şekilde kullanmasını fiilen imkânsız hâle getirmektedir[727]. Bu nedenle bilgi edinme hakkı, yalnızca verilerin işlendiğine dair genel bir bildirim almayı değil, aynı zamanda bu süreçlerin detaylarına ulaşma ve onları denetleme imkânını da kapsamaktadır[728]. Aynı zamanda, veri sorumlusunun verileri doğru, eksiksiz ve güncel tutma yükümlülüğünün denetlenebilmesi bakımından da araçsal bir işlev üstlenmektedir[729].

GDPR 15. maddesinin 3. fıkrası, veri sorumlusunun, işlenen kişisel verilerin bir kopyasını veri sahibine sunma yükümlülüğünü açıkça düzenlemektedir[730]. Böylece, veri sahibi yalnızca işlenen veriler hakkında bilgi almakla kalmaz, bu verilerin içeriğine doğrudan erişim hakkını da elde etmektedir. Buna karşılık, KVKK 11. maddesinin 1. fıkrasının (b) bendinde düzenlenen "bilgi talep etme" hakkı, veri kopyasına erişimi doğrudan ve açık şekilde öngörmemekte, daha çok genel nitelikte bilgilendirme yükümlülüğünü ifade etmektedir. Kanaatimizce işlenen verinin bir kopyasının talep edilebilmesi Türk Hukuku açısından da yasal bir düzenleme ile kabul edilmesi gerekmektedir.

KVKK'dan farklı olarak GDPR 15. maddesinin 1. fıkrasının (h) bendi kapsamında *"profilleme de dâhil olmak üzere 22(1) ve (4) maddelerinde atıfta bulunulan otomatik*

---

[727] Oğuz Şimşek, *Anayasa hukukunda kişisel verilerin korunması* (İstanbul: Beta, 2008), 88; İbrahim Korkmaz, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", *TBB Dergisi*, sy 124 (2016): 131; Serdar Çelikel, "Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri", 101.

[728] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 253.

[729] Bu çerçevede değerlendirilen bir diğer temel hak ise bilgi üzerinde bireyin kendi kendini belirleme hakkıdır (informational self-determination). Bu hak, bireyin kişisel verileri üzerinde hangi bilgilerin hangi amaçlarla toplanacağı, ne şekilde işleneceği, saklanacağı ve kimlerle paylaşılacağı hususlarında karar verebilme ve bu süreçleri denetleyebilme yetkisini ifade eder. Dijitalleşmenin hızla artmasıyla birlikte, özel yaşamın korunmasının modern bir yansıması olarak gelişen bu kavram, bireyin kişisel veriler üzerindeki aktif kontrolünü esas alan bir anlayışı benimsemiştir. Özellikle Avrupa ve Amerika Birleşik Devletleri arasında, söz konusu hakkın kapsamı ve uygulama biçimi bakımından önemli farklılıklar bulunmaktadır. Avrupa hukukunda bireyin kendi kendini belirleme hakkı oldukça geniş yorumlanmakta; bu kapsamda kişisel verilere erişim, işlenen veriler hakkında bilgi edinme, yanlış verilerin düzeltilmesini talep etme, verilerin silinmesini isteme (right to erasure) ve veri işlemeye itiraz etme gibi haklar güçlü bir şekilde korunmaktadır. Buna karşılık, Amerika Birleşik Devletleri hukukunda bu hak daha dar kapsamda ele alınmakta; kişisel verilerin korunmasına ilişkin talepler büyük ölçüde sektör bazlı düzenlemeler veya sözleşme ilişkileri çerçevesinde değerlendirilmekte ve ifade özgürlüğü başta olmak üzere diğer anayasal hak ve değerlerle dengelenmektedir. Roberto Fernández Fernández, "Big Data as a Tool to Enhance Recruitment Processes", *E-Journal of International and Comparative Labour Studies*, 2022, 101, https://ejcls.adapt.it/index.php/ejcls_adapt/article/view/1168/1339.

[730] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 379.

*karar almanın varlığı ve en azından bu hâllerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işlemenin veri öznesi açısından önemi ve öngörülen sonuçları"*na ilişkin bilgi talep etme hakkı tanınmıştır[731]. Madde 29 Çalışma Grubu'nun rehberlerine göre bu yükümlülük, işverenin algoritmanın karmaşık yapısını veya kaynak kodunu ifşa etmesini gerektirmemektedir. Bunun yerine amaç, veri sahibine işleme faaliyetleri hakkında geniş kapsamlı ve herkesin anlayabileceği şekilde, genel bir bakış açısı sunulması amaçlanmaktadır. Bu genel bakış açısı, genellikle profil oluşturmada kullanılan veri kategorileri, bu verilerin neden ilgili görüldüğü ve profilin karar sürecindeki rolü gibi bilgileri içerir[732]. Dolayısıyla GDPR, kararın nasıl alındığına dair teknik bir açıklamadan ziyade, kararın hangi temellere dayandığına dair genel bir çerçeve sunulmasını yeterli görmektedir. Bu durum, veri sahibinin, hakkında verilen spesifik bir kararın nedenlerini tam olarak anlaması bakımından bir boşluk yaratabilmektedir. İşte bu noktada, ilerleyen bölümlerde ele alınan alternatif senaryo açıklamaları, bu boşluğu doldurmak için ideal bir araç olarak öne çıkmaktadır. Her ne kadar GDPR tarafından açıkça zorunlu kılınmasa da alternatif senaryo açıklamaları sunmak, veri sorumlusunun "anlamlı bilgi" sağlama yükümlülüğünü yerine getirmesinin ötesine geçerek, şeffaflık ilkesinin ruhunu tam anlamıyla karşılamaktadır. Bir çalışana, sadece "düşük performans puanınız nedeniyle prim alamadınız" gibi genel bir bilgi vermek yerine, "eğer son bir ayda tamamladığınız görev sayısı 10 değil de 15 olsaydı, prim almaya hak kazanacaktınız" gibi bir karşı olguya dayalı açıklama sunmak, kararın mantığı hakkında çok daha somut, kişiselleştirilmiş ve "anlamlı" bir bilgi sağlamaktadır[733]. Bu yaklaşım, aynı zamanda erişim hakkının temel sınırlamalarından biri olan ticari sırların korunması (GDPR Başlangıç bölümü 63. maddesi) ile de uyumluluk göstermektedir. Çünkü karşı alternatif senaryo açıklamaları, algoritmanın kendisini veya tescilli mantığını ifşa etmeden, sadece girdi ve çıktı arasındaki ilişkiyi göstermektedir. Bu yaklaşım sayesinde işveren, hem çalışanın erişim hakkına saygı göstermiş olmakta hem de ticari sırlarını korumaktadır[734].

---

[731] Wachter vd., "Counterfactual Explanations Without Opening the Black Box", 878-79.
[732] Wachter vd., "Counterfactual Explanations Without Opening the Black Box", 868-69.
[733] Wachter vd., "Counterfactual Explanations Without Opening the Black Box", 843.
[734] Wachter vd., "Counterfactual Explanations Without Opening the Black Box", 881-84.

Bilgi edinme hakkı, mutlak nitelikte olmayıp, bazı sınırlamalara tabi bulunmaktadır. Bu açıdan KVKK 28. maddesinde ve GDPR 23. maddede belirtilen istisnai durumlar saklı tutulmaktadır. Her ne kadar bireyin kendi kişisel verilerine erişim hakkı bulunsa da bu hak sınırsız bir nitelik taşımamaktadır. Özellikle üçüncü kişilerin hak ve özgürlüklerinin (örneğin, ticari sırlar veya fikri mülkiyet hakları) olumsuz etkilenmemesi, devletin güvenliği ve kamu düzeni gibi meşru nedenlerle bilgi edinme hakkı sınırlandırılabilmektedir. Bu nedenle veri sorumlusunun, başvurunun kapsamını değerlendirirken hem ilgili kişinin erişim hakkını hem de bu tür meşru kısıtlama gerekçelerini birlikte gözetmesi gerekmektedir[735].

B Yapay Zekâ Tüzüğü, yüksek riskli yapay zekâ sistemlerinden etkilenen kişilere daha somut bir "açıklama hakkı" (Right to an Explanation) tanımıştır. Örneğin, bir tele çalışanın performansı, yüksek riskli bir izleme aracı tarafından otomatik olarak düşük puanlanırsa, bu çalışan sadece karara itiraz etmekle kalmamakta, aynı zamanda işvereninden bu kararın üretiminde sistemin rolü, kullanılan ana parametreler ve temel mantığı hakkında açık ve anlamlı bir açıklama da talep edebilmektedir. Bu hak, çalışanın itirazını daha bilinçli ve etkili bir şekilde yapabilmesi için gerekli zemini hazırlamaktadır[736].

Tele çalışanın izlenmesi ve gözetlenmesi bağlamında erişim hakkı, çalışanın işverenine başvurarak, "Hakkımda kullandığınız aktivite izleme yazılımı tarafından son bir ay içinde oluşturulan tüm performans raporlarını, alınan ekran görüntülerini ve hakkımda üretilen verimlilik puanlarını görmek istiyorum" şeklinde bir talepte bulunmasını sağlamaktadır. Bu sayede çalışan, kendisi hakkında hangi verilerin işlendiğini doğrudan görebilmekte ve bu verilerin doğruluğunu veya hukuka uygunluğunu KVKK 11. maddesi kapsamında denetleyebilmektedir[737].

---

[735] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 379; İrem Kaya, "Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) Kapsamında Ortak Veri Sorumluluğu" (Yayınlanmamış Yüksek Lisans Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, 2023), 104-5.
[736] Voigt ve Hullen, *The EU AI Act*, 45-46.
[737] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 259-63.

4.5.3. Değişiklik / Düzeltme Talep Etme Hakkı

İlgili kişinin kişisel verileri üzerinde sahip olduğu temel haklardan biri de değişiklik (düzeltme) talep etme hakkıdır oluşturmaktadır[738]. Bu hak, özellikle verilerin doğruluğunun ve güncelliğinin temini açısından hayati bir önem taşımakta ve yalnızca bireyin veri üzerindeki kontrolünü sağlamakla kalmamakta; aynı zamanda veri sorumlusunun KVKK 4. maddesinin 2. fıkrasının (b) bendi ve GDPR 5. maddesinin 1. fıkrasının (d) bendi uyarınca doğru ve güncel veri işleme yükümlülüğünü de tamamlayıcı bir nitelik arz etmektedir[739].

KVKK 11. maddesinin 1. fıkrasının (d) bendi uyarınca, ilgili kişi veri sorumlusuna başvurarak kendisine ait kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini talep etme hakkına sahip bulunmaktadır[740]. Bu bağlamda, değişiklik talep etme hakkı, veri sorumlusunun işlediği verinin gerçeği yansıtması gerekliliğine dayanmaktadır. GDPR 16. maddesinde "düzeltme hakkı" (right to rectification) başlığı altında benzer bir hak tanımaktadır: *"Veri sahibi, veri sorumlusundan kendisiyle ilgili yanlış kişisel verilerin gecikmeksizin düzeltilmesini isteme hakkına sahiptir. İşlemenin amaçları dikkate alındığında, veri sahibi, ek bir beyan sunmak da dahil olmak üzere eksik kişisel verilerin tamamlanmasını isteme hakkına sahiptir"*[741]. Söz konusu düzenleme, yalnızca verinin maddi hatalardan arındırılmasını değil, aynı zamanda bireyin kişilik haklarını etkileyebilecek içeriklerin denetlenmesini ve eksik bilgilerin tamamlanmasını da kapsamaktadır[742].

Değişiklik hakkı, özellikle iş ilişkileri bağlamında işçilerin verilerinin zamanında ve doğru şekilde güncellenmesini sağlamak açısından da önem arz etmektedir[743]. Bu kapsamda örneğin, işçinin medeni durumu, ikametgâh adresi veya iletişim bilgileri gibi kişisel verileri, değişiklik olması hâlinde veri sorumlusunca zamanında

---

[738] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 263-65.
[739] Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 154.
[740] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 386.
[741] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 18; Adams-Prassl vd., "Regulating Algorithmic Management", 144.
[742] Feiler vd., *The EU General Data Protection Regulation (GDPR)*, 115.
[743] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 247.

güncellenmesi gerekmektedir[744]. Bununla birlikte, işveren bu güncellemeyi yapmak adına sürekli ve kendi inisiyatifiyle araştırma yükümlülüğü altında olmayıp, aksine bu değişikliklerin ilgili kişi tarafından bildirilmesi gerekmektedir[745]. Ancak bu durum, veri sorumlusunun GDPR 5. maddesinin 1. fıkrasının (d) bendi kapsamında düzenlenen *"yanlış olan kişisel verilerin gecikmeksizin silinmesini veya düzeltilmesini sağlamak için her türlü makûl adımı atma"* yükümlülüğünü ortadan kaldırmamakta; işverenin, çalışanların bilgilerini güncelleyebilmeleri için kolaylaştırıcı mekanizmalar sunması gerekmektedir[746]. Daha önce kişisel verilerin doğru ve gerektiğinde güncel olması ilkesi altında açıkladığımız üzere, bir izleme yazılımının çalışanın uzun bir belgeyi okumasını "pasiflik" olarak yanlış kaydettiği bir senaryoda, çalışan bu hakkını kullanarak söz konusu hatalı verinin düzeltilmesini ve performans raporunun bu doğrultuda güncellenmesini talep edebilmektedir. Bu talep hakkı, özellikle algoritmik sistemler tarafından yapılan hatalı çıkarımlara karşı önemli bir güvence mekanizması işlevi görmektedir.

4.5.4. Kişisel Verilerin Silinmesi ve Yok Edilmesini Talep Etme Hakkı

İlgili kişinin kişisel verileri üzerinde sahip olduğu haklardan biri de silme ve yok edilmesini talep etme oluşturmaktadır[747]. Belirtelim ki, "unutulma hakkı" (right to be forgotten), "unutma hakkı" (right to oblivion) ve "diziden çıkarmak hakkı" (right to delisting) olarak da anılmaktadır[748]. Bu hak, KVKK'nın 11. maddesinin 1. fıkrasının (e) bendinde, Kanun'un 7. maddesinde öngörülen şartlar çerçevesinde

---

[744] Şahin Yunak, "İş Hukukunda Kişisel Verilerin Korunması", 44.
[745] Küzeci, *Kişisel Verilerin Korunması Hukuku*, 243-44; Şahin Yunak, "İş Hukukunda Kişisel Verilerin Korunması", 44; Cem Sarıkabadayı, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri", 36.
[746] Yılmaz, "Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması", 100.
[747] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 264-65; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 205.
[748] Unutulma hakkı, esasen, kişisel verilerin silinmesi hakkıdır. Ancak, kişisel verilerin korunması mevzuatı unutulma hakkının ne olduğunu tanımlamaz ve bu hak Avrupa içtihatlarında da doğrudan yer almaz. Bununla birlikte, bazı kararlar dolaylı olarak bu hakkın varlığına işaret edebilir. Bu kararlar, bir doğal kişinin isminin arama kriteri olarak kullanıldığı durumlarda, sonuçlar listesindeki bağlantıların kaldırılmasını içeren bir içeriğe atıfta bulunur. Ayrıntılı bilgi için bknz. Kaynar ve Urhanoğlu, "İşçinin Ulaşılamama Hakkı", 319-82; Urhanoğlu vd., "İşçinin Unutulma Hakkı", 211-43; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 256-57; Arama motorları, web paylaşımları vb. sanal aktiviteler bağlamında unutulma hakkına ilişkin bknz. Oleksandr Pastukhov, "The right to oblivion: what's in the name", *Computer and*, 2013, 14, https://www.academia.edu/download/62248500/Right_to_oblivion20200302-46205-1qfuknw.pdf; Fernández, "Big Data as a Tool to Enhance Recruitment Processes", 103-4.

düzenlenmiştir[749]. Bu şartlar, temel olarak kişisel verilerin işlenmesini gerektiren hukuki sebeplerin ortadan kalkmasını ifade etmektedir. Dolayısıyla, işleme amacı ortadan kalkan veriler için ilgili kişi, silme veya yok edilmesini talep etme imkânına sahip bulunmaktadır. GDPR 17. maddede ise bu hak daha genel olarak silme hakkı (right to erasure) kapsamında düzenlenmiştir[750].

Kanun'da tesis edilen bu temel yükümlülüğün usul ve esasları, 7. maddenin verdiği yetkiyle çıkarılan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik aracılığıyla detaylandırılmıştır. Yönetmelik, veri imha yöntemlerini net bir şekilde tanımlamaktadır: Silme, kişisel verilerin, "*ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir"*. Yok etme, kişisel verilerin, "*hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir"*. Anonim hale getirme ise, verilerin *"başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemidir"*. İlgili Yönetmeliğe göre veri sorumlusu, Kurul tarafından aksine bir karar alınmadıkça bu yöntemlerden uygun olanını seçmekte serbesttir. Ancak ilgili kişinin talebi hâlinde, seçtiği yöntemin gerekçesini açıklamakla yükümlüdür. Ayrıca, silme, yok etme ve anonim hâle getirme ile ilgili yapılan bütün işlemler kayıt altına alınmakta ve bu kayıtlar en az üç yıl süreyle saklanmaktadır[751].

Gerek KVKK gerekse GDPR, kişisel verilerin silinmesini talep hakkını yalnızca verinin veri sorumlusunun sisteminden çıkarılması ile sınırlı görmemektedir. Aynı zamanda verinin aktarıldığı üçüncü taraflar nezdinde de etkili kılmayı hedeflemektedir[752]. GDPR 19. maddesi uyarınca, verilerin aktarıldığı tüm alıcılara silme işleminin bildirilmesi gerekmektedir. Benzer şekilde, KVKK 11. maddesinin 1.

---

[749] KVKK kapsamında kişisel verilerin anonimleştirilmesi, veri sorumlusunun yükümlülükleri arasında yer almakla birlikte, mevzuatta veri sahibine kişisel verilerinin anonimleştirilmesini talep etme hakkı açıkça tanınmamıştır. Bu durum, veri sahibinin verileri üzerindeki kontrolünü sınırlayan bir eksiklik olarak yorumlanabilir. Zira ilgili kişi, verilerinin istatistiksel veya bilimsel amaçlarla kullanılmaya devam etmesini tercih ederek anonimleştirilmesini isteyebilecekken, Kanun bu yönde bir talep hakkı sunmamaktadır. Kanaatimizce bu yönde bir düzenlemenin getirilmesi yerine olacaktır.
[750] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 264.
[751] Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 206-7.
[752] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 398; Ayşe Nur Akıncı, *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler Ve Türk Hukuku Bakımından Değerlendirilmesi* (T.C. Kalkınma Bakanlığı, 2017), 20; Yılmaz, "Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması", 183.

fıkrasının (f) bendine dayanarak düzenlenen Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 12. maddesi uyarınca, kişisel verileri işleme şartları ortadan kalkmış ve veriler üçüncü kişilere aktarılmışsa, veri sorumlusu bu durumu üçüncü kişiye bildirmekle ve üçüncü kişi nezdinde gerekli işlemlerin yapılmasını temin etmekle yükümlüdür[753].

GDPR 17. maddesinin 2. fıkrası uyarınca, kişisel veriler kamuya açıklanmışsa, veri sorumlusu sadece verileri silmekle kalmaz, aynı zamanda bu verilerin işlendiği tüm bağlantıların kaldırılması için makûl teknik önlemleri alması gerekmektedir[754]. KVKK'da bu boyut açıkça düzenlenmemiş olsa da verilerin aktarıldığı tüm üçüncü kişilere bildirimde bulunma ve gereğinin yapılmasını sağlama yükümlülüğü, benzer bir koruma mekanizması sunmaktadır[755]. Eğer veri sorumlusu kişisel verileri alenileştirmişse ve ilgili kişi, söz konusu kişisel verilere yönelik tüm bağlantıların, bu verilerin her türlü kopyasının ve çoğaltılmış hâlinin silinmesini talep ederse, veri sorumlusu mevcut teknolojiyi ve uygulama maliyetlerini de göz önünde bulundurarak makûl adımları atmakla yükümlüdür[756].

Bu hak, tele çalışanın izlenmesi ve gözetlenmesi bağlamında hayati bir rol oynamaktadır. Örneğin, bir projenin tamamlanmasının ardından, o projeye özgü toplanmış olan detaylı aktivite logları veya ekran görüntüleri için işleme amacı ortadan kalkmaktadır. Bu durumda tele çalışan, işverenine başvurarak bu verilerin silinmesini veya yok edilmesini talep edebilmektedir. Benzer şekilde, bir performans değerlendirme dönemi kapandıktan ve olası itiraz süreleri dolduktan sonra, o döneme ait ham izleme verilerinin saklanması için meşru bir gerekçe kalmayabilmektedir. Çalışanın bu verilerin silinmesini talep etmesi, sınırlı süreyle tutulma ilkesinin bir gereği ve kişisel verilerin silinmesi ve yok edilmesini talep etme hakkının somut bir yansımasını oluşturmaktadır.

---

[753] Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik Resmî Gazete Tarihi: 28.10.2017 Resmî Gazete Sayısı: 30224

[754] Fernández, "Big Data as a Tool to Enhance Recruitment Processes", 103.

[755] Çelikel, "Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri", 112.

[756] Dilanur Demir, "Kişisel Verilerin Korunması Kapsamında Unutulma Hakkı" (Yayınlanmamış Yüksek Lisans Tezi, Hacettepe Üniversitesi, 2023), 104-5.

4.5.5. Otomatik Kararlara İtiraz ve Tabi Olmama Hakkı

4.5.5.1. Genel Olarak

Günümüzde, pek çok karar otomatik sistemler vasıtasıyla insan müdahalesi olmaksızın alınabilmektedir. Yapay zekâ sistemleri geliştikçe otomatik karar sistemlerin etkinliği artmaya devam etmesi beklenmektedir. Bu sistemler büyük ölçüde kişisel veri işlenmesine dayalı olarak çalışmaktadır. Anılması gereken bir diğer ilişkili kavram ise profillemedir. Profilleme ve otomatik karar alma süreçleri birbiriyle yakından ilişkili kavramlar olmakla birlikte, ayrıştırılması gereken teknik farklılıklar barındırır. Profilleme, bireylerin özelliklerini, davranışlarını ya da eğilimlerini tahmin etmek amacıyla yapay zekâ algoritmaları ve veri madenciliği tekniklerinin kullanılmasını ifade etmektedir. Otomatik karar alma ise, profilleme sonucu elde edilen bilgiler doğrultusunda, bir insan müdahalesi olmaksızın karar verilmesidir[757]. Örneğin, bir iş başvurusunda bulunan adayın özgeçmişinde yer alan eğitim kurumu, yaşadığı semt ve önceki iş deneyimlerine ilişkin verilerin, tamamen otomatik bir algoritma tarafından analiz edilerek "düşük başarı potansiyeli" etiketiyle değerlendirilmesi ve bu sebeple mülakata dahi çağrılmaması, otomatik karar vermeye dayalı tipik bir uygulamadır[758]. Bu durumda, insan müdahalesi olmaksızın verilen karar, ilgili kişinin haklarını doğrudan etkileyebilecek niteliktedir.

Algoritmalar aracılığıyla büyük kitlelere ait geniş veri setlerinin işlendiği durumlarda, bilgilendirme, şeffaflık ve hesap verebilirlik gibi temel ilkelerin uygulanmasında önemli güçlükler ortaya çıkmakta; bu ilkeler bazen uygulamada yetersiz kalabilmektedir[759]. Otomatik sistemler karşısında, bireyin özerkliğinin güçlendirilmesi ve mahremiyetinin korunması özel bazı güvenceler getirilmesini zorunlu kılmaktadır. Bununla birlikte, mevzuatımızda bu bağlamda yeterli güvencenin sağlanabildiğini söylemek güçtür. Zira KVKK'da yalnızca "İşlenen verilerin münhasıran otomatik

---

[757] Aksoy, "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme", 71-72.
[758] Marvin van Bekkum ve Frederik Zuiderveen Borgesius, "Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?", arXiv:2206.03262, preprint, arXiv, 28 Kasım 2022, 3.
[759] Kitlesel veri işlemede kolektif haklar ve güçlendirilmiş özel hayat koruması tartışmalarına ilişkin bknz. Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 95.

sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme" hakkı tanınmıştır.

Avrupa Birliği Hukuku'nda ise koruma alanı daha geniş tutulmuş ve GDPR'da konuya ilişkin ayrıntılı düzenlemeler getirilmiştir. Sözü geçen düzenlemelerde "itiraz hakkı" ile "profilleme dâhil otomatik işleme dayalı kararlara tabi olmama hakkı" iki ayrı hüküm olarak karşımıza çıkmaktadır. Bu düzenlemelerden ilki itiraz hakkına ilişkindir. GDPR'ın 21. maddesi, veri sahibine meşru menfaat veya kamu yararına dayalı veri işleme faaliyetlerine, özel durumu gerekçe göstererek her zaman itiraz etme hakkı tanımakta; bu durumda veri sorumlusunun işlemi durdurması ve ancak üstün meşru gerekçeleri ispatlaması hâlinde işleme devam etmesi mümkün olmaktadır[760]. Aynı şekilde profillemeye karşı kişisel gerekçelerle itiraz hakkı söz konusudur. Bireyin bu hakkı kullanımı şeffaf ve teknik olarak kolay erişilebilir şekilde kullanımı sağlanarak itiraz kolaylaştırılmıştır. Doğrudan pazarlamaya karşı ise özel bir koruma getirilmiştir. Böylece GDPR, yalnızca otomatik karar alma süreçlerine değil, genel veri işleme faaliyetlerine karşı da güçlü ve doğrudan bir müdahale imkânı sunmaktadır[761]. Buna karşın KVKK'da doğrudan ve genel nitelikli bir itiraz hakkı öngörülmemiş; yalnızca otomatik sistemlerle alınan kararlar bakımından KVKK 11. maddesinin 1. fıkrasının (g) bendi ile düzenleme yapılmıştır. Meşru menfaate dayalı işleme faaliyetlerine karşı özel duruma dayalı doğrudan bir itiraz hakkı tanınmazken, veri sorumlusuna başvuru, Kurul'a şikâyet, verilerin silinmesi ile yok edilmesi talebi ve tazminat mekanizmaları gibi dolaylı yollarla bu hakka işlerlik kazandırılabilmektedir.

KVKK 11. maddesinin 1. fıkrasının (g) bendi uyarınca, ilgili kişi, *"işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkması"* hâlinde bu sonuca itiraz etme hakkına sahiptir. Kanunun gerekçesinde de belirtildiği üzere, bu düzenleme özellikle çalışanların performanslarının algoritmik sistemler tarafından analiz edilmesi sonucunda olumsuz bir sonuca maruz kalmaları durumunda, bu sonuca karşı hukuki bir koruma yolu sağlamayı amaçlamaktadır[762]. İtiraz hakkının kullanılabilmesi üç temel unsurun

[760] De Stefano ve Wouters, *AI and Digital Tools in Workplace Management and Evaluation*, 39.
[761] Mahmut Furkan Balaban, "Elektronik Haberleşme Sektöründe İşlenen Kişisel Verilerin Korunması" (Doktora Tezi, Ankara Sosyal Bilimler Üniversitesi, 2023), 226.
[762] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 399.

varlığına bağlı bulunmaktadır: ilgili kişinin verilerinin münhasıran otomatik sistemler aracılığıyla işlenmiş olması, verilerin bu yolla analiz edilmiş olması ve bu analiz sonucunda ilgili kişinin aleyhine bir sonucun ortaya çıkması[763]. Tele çalışma özelinde bu hak, örneğin, bir çalışanın verimliliğinin, insan müdahalesi olmaksızın, sadece klavye aktivitesi, e-posta gönderme sıklığı gibi verileri analiz eden bir algoritma tarafından otomatik olarak düşük olarak puanlanması ve bu puanlama sonucunda kendisine bir uyarı gönderilmesi veya priminin kesilmesi durumunda devreye girmektedir. Çalışan, bu sonuca itiraz ederek kararın bir insan tarafından yeniden değerlendirilmesini talep edebilmektedir. Ancak işten çıkarma, örneğin üretim miktarı gibi doğrudan ölçülebilir ve insan müdahalesiyle denetlenmiş bir kritere dayanıyorsa, bu durumda itiraz hakkı sınırlı şekilde uygulanabilecektir[764]. Sözü konusu düzenleme ile getirilen itiraz hakkının aynı zamanda veri işleme faaliyetlerinin şeffaflığı ve hesap verebilirliği ilkeleriyle de bağlantılı olarak "açıklama isteme hakkı" ile birlikte değerlendirilmesi de mümkündür[765]. Buradaki "münhasıran otomatik sistem" ifadesi, karar alma sürecinde anlamlı bir insan müdahalesinin bulunmadığı durumları işaret etmektedir[766]. Bu bağlamda, algoritma tarafından verilen kararı değiştirme yetkisine ve değerlendirme becerisine sahip bir insanın sürece dâhil olmaması, kararın tamamen otomatik olduğu anlamına gelmektedir. Ayrıca, "kişinin aleyhine bir sonuç" kavramı, GDPR'da yer aldığı üzere, birey üzerinde hukuki etkiler doğuran veya benzer şekilde önemli ölçüde etkileyen kararları ifade etmektedir[767].

GDPR'da itiraz hakkının yanı sıra "otomatik işlemeye dayalı kararlara tabi olmama hakkı" da özel olarak düzenlenmiştir. İnsan müdahalesi olmaksızın alınan kararlara karşı koruma sağlamayı amaçlayan GDPR'ın 22. maddesi, bu yönüyle mevzuatımıza nazaran oldukça kapsamlı bir nitelik taşımaktadır. Nitekim Kişisel Verilerin Korunması Kanunu (KVKK) ile GDPR arasında bu konuda dikkate değer farklılıklar bulunmaktadır. GDPR, ilgili kişiye kendisiyle ilgili hukuki veya benzer şekilde önemli sonuçlar doğuran ve münhasıran otomatik işleme faaliyetlerine dayalı kararların muhatabı olmama hakkı tanırken, bu düzenleme ilgili kişinin yalnızca bir karara itiraz

[763] Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 399; Özer Deniz, "Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk", 11.
[764] Limoncuoğlu, "İşçiye Ait Kişisel Verilerin Korunması", 11.
[765] Aksoy, "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme", 82.
[766] Aksoy, "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme", 82.
[767] Aksoy, "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme", 91.

etmesini değil, aynı zamanda bu tür kararların en baştan uygulanamamasını güvence altına almaktadır. Buna karşın, KVKK münhasıran otomatik karar alınmasını açıkça yasaklamamakta, yalnızca aleyhe sonuç doğuran kararlara ilgili kişi tarafından itiraz edilebileceğini düzenlemektedir. Bu durum, özellikle yapay zekâ destekli sistemler açısından önemli bir eksiklik olarak değerlendirilmektedir. Avrupa Birliği'nden farklı olarak, Türkiye'deki kişisel verilerin korunmasına ilişkin mevzuatın profilleme ve otomatik karar alma sistemleri konusunda yetersiz kaldığı ifade edilmektedir[768].

GDPR'da bu hakka üç istisna öngörülmüştür: kararın, ilgili kişiyle veri sorumlusu arasında bir sözleşmenin kurulması veya ifası için gerekli olması; işlemenin, Birlik hukuku veya üye devlet hukuku çerçevesinde öngörülmesi ve ilgili kişinin haklarının korunması amacıyla gerekli tedbirlerin alınması koşuluyla gerçekleştirilmesi ve ilgili kişinin açık rızasının bulunması[769]. Ancak bu istisnaların uygulanması dahi, veri sorumlusuna sınırsız bir yetki vermemektedir. GDPR, bu durumlarda veri sahibinin haklarını korumak için bir dizi ek güvence öngörmüştür. Bu güvenceler, ilerleyen alt başlıklarda detaylı olarak incelenecek olan açıklama talep etme hakkı, karara itiraz etme imkânı ve anlamlı insan müdahalesi talep etme hakkı gibi unsurları içermektedir[770].

4.5.5.2. Algoritmik Karar Süreçlerine İlişkin Bilgi Edinme Hakkı ve Açıklama Yükümlülüğü

İşverenin, yapay zekâ tabanlı bir izleme ve gözetleme uygulaması kullanmaya başlamadan önce, çalışanı sistemin varlığı, işleyeceği veriler ve genel mantığı hakkında proaktif olarak bilgilendirme yükümlülüğü bulunmaktadır. Bu aydınlatmanın, çalışanın herhangi bir talepte bulunmasını beklemeden, şeffaflık ilkesi gereği en başta yapılması gerekmektedir. Bu genel bilgilendirmenin ardından, sistemin

---

[768] Dijital ortamda ayrımcılıkla mücadele edebilecek ve otomatik karar verme sistemlerinin neden olduğu algoritmik ayrımcılığı önleyebilecek ex ante (önleyici) düzenlemelere duyulan ihtiyaç için bknz. Bozkurt Gümrükçüoğlu ve Yakacak, "Yapay Zekânın İşe Alım Süreçlerinde Kullanımı ve Algoritmik Ayrımcılık", 1747 vd.; Ekmekçi vd., *Kişisel Verilerin Korunması Hukuku*, 399-400.

[769] Aloisi ve Gramano, "Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context", 113; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 263; Aksoy, "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme", 78; Öğretmen Kotil, *Kişisel Verilerin Korunması Çerçevesinde Yapay Zeka*, 150-51; Öztürk, "Kişisel Verilerin Korunmasında Yapay Zekânın Rolü", 65.

[770] Öğretmen Kotil, *Kişisel Verilerin Korunması Çerçevesinde Yapay Zeka*, 151.

çalışan aleyhine düşük performans puanı gibi somut bir karar vermesi durumunda, çalışanın bu karara itiraz etme ve spesifik gerekçelerini öğrenmek için "açıklama talep etme hakkı" devreye girmektedir. Dolayısıyla, bu iki aşamalı mekanizma, ilkiyle genel bir çerçeve sunarken, ikincisiyle bireysel kararlara karşı somut bir denetim ve savunma imkânı tanıyarak birbirini tamamlamaktadır.

Bir karara karşı çıkmak isteyen işçinin, algoritmaların sonuçlarının arkasındaki mantığı anlayabilmesi ve gerekli bilgilere erişebilmesi şarttır[771]. GDPR'ın 13. ve 15. maddeleri, bu hakkın temelini oluşturan "ilgili mantık hakkında anlamlı bilgi" edinme imkânını güvence altına alarak bu ihtiyacı karşılamayı hedeflemektedir. Bu, otomatik sistemin tasarımı hakkında genel, yani *ex ante* (önceden sunulan) bir açıklama talep etme hakkı olarak yorumlanabilmektedir[772]. Ancak GDPR'ın, veri sahiplerine belirli bir karara ilişkin bireyselleştirilmiş, yani ex post (sonradan) bir açıklama hakkı tanıyıp tanımadığı konusundaki tartışmalar devam etmektedir[773]. GDPR'ın 22. maddesinin otomatik kararlara "itiraz etme hakkını" garanti etmesinin, fiiliyatta ex post bir açıklama yükümlülüğü doğurduğu savunulmaktadır[774]. Ancak bu yükümlülüğün yerine getirilmesi, özellikle karmaşık makine öğrenimi modellerinin yarattığı kara kutu sorunu nedeniyle teknik zorluklar içermektedir. Zira yasal metinlerdeki "işlem mantığı hakkında anlamlı bilgi" tanımı, bu tür modellerin karar süreçlerini tam olarak yansıtmayabilmekte ve bu süreçleri açıklamak teknik olarak oldukça güçlük arz etmektedir. Bu soruna bir çözüm olarak, belirli bir sorguya odaklanan "konu merkezli açıklamalar" önerilmektedir.[775]. Söz konusu yaklaşım, algoritmanın genel tasarımını açıklamaktan ziyade, belirli bir kararın nasıl verildiğini aydınlatmakta ve bireylerin karar süreci hakkında daha net bir anlayış geliştirmelerini sağlamaktadır[776]. Bu

[771] Walter A. Mostowy, "Explaining Opaque AI Decisions, Legally", *Berkeley Technology Law Journal* 35, sy 4 (2020): 1292-93.
[772] Mostowy, "Explaining Opaque AI Decisions, Legally", 1292-93.
[773] Mostowy, "Explaining Opaque AI Decisions, Legally", 1292-93.
[774] Mostowy, "Explaining Opaque AI Decisions, Legally", 1293.
[775] Lilian Edwards ve Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking for International", *Duke Law & Technology Review* 16 (2018 2017): 81.
[776] Konu merkezli açıklamalar, özellikle makine öğrenmesi ve yapay zekâ sistemlerinin karar verme süreçlerinin şeffaflığını artırmaya yönelik geliştirilen bir açıklama yaklaşımıdır. Bu yöntem, modelin genel işleyiş mantığını açıklamak yerine, belirli bir sorgu ya da karar sonucuna odaklanarak açıklama üretir. Yani, modelin neden özellikle o spesifik kararı verdiğini anlamaya yardımcı olur. Bu sayede, kullanıcıya veya veri sahibine, kendi durumu bağlamında modelin nasıl çalıştığına dair daha anlamlı ve doğrudan bilgi sunulur. Bu yaklaşım, özellikle algoritmik kararların kişisel verilere etkisini

yaklaşımı hayata geçiren en etkili yöntemlerden birini ise bir sonraki bölümde incelenecek olan alternatif senaryo açıklamaları oluşturmaktadır.

4.5.5.3. Alternatif Senaryo Açıklamaları

İtiraz hakkının uygulamada etkili biçimde kullanılabilmesi, bireyin kendisi hakkında verilen kararın gerekçelerini anlayabilmesine bağlı bulunmaktadır. Ancak özellikle "kara kutu" olarak ifade edilen karmaşık yapay zekâ sistemlerinde, kararın arkasındaki mantığın birey tarafından kavranabilmesi neredeyse imkânsız hâle gelmektedir. Bu durum ise itiraz hakkını fiilen işlevsiz hâle getirme riski taşımaktadır. Sorunun üstesinden gelmek için veri koruma hukuku literatüründe geliştirilen yenilikçi yöntemlerden biri, "alternatif senaryo açıklamaları" (karşı olguya dayalı açıklamalar - counterfactual explanations) olarak adlandırılmaktadır[777].

Sözü geçen yöntem, karmaşık algoritmaların iç yapısını ya da kaynak kodlarını ifşa etmeden (yani "kara kutuyu açmadan"), ilgili kişiye anlaşılır, basit ve somut biçimde eyleme geçirilebilir bilgiler sunmaktadır[778]. Bu açıklama türünün temel formülü şu şekildedir: "Mevcut koşullarınız nedeniyle bu karara ulaşıldı. Eğer belirli koşullar farklı olsaydı, farklı bir sonuç ortaya çıkardı." Örneğin, kredi başvurusu reddedilen bir kişiye "Yıllık geliriniz 30.000 TL olduğundan başvurunuz reddedildi. Eğer geliriniz 45.000 TL olsaydı, başvurunuz kabul edilirdi" şeklinde yapılan açıklama, alternatif senaryo açıklamanın tipik bir örneğini oluşturmaktadır[779]. Bu tür açıklamalar, ilgili kişilere üç temel avantaj sağlamaktadır. Birincisi, kişi kararın hangi temel ve değiştirilebilir faktörlere dayandığını açıkça anlayabilmektedir. İkincisi, kararın gerekçesine dair somut bilgiye sahip olması, kişinin karara karşı etkili bir itirazda bulunmasına imkân tanımakta; örneğin, kişinin gelir bilgisinin yanlış ya da eksik kaydedildiğini fark etmesi durumunda, bu bilgiyi düzelttirerek başarılı bir itiraz süreci başlatabilmektedir. Üçüncüsü ise karar doğru olsa bile, kişi gelecekte istediği sonuca ulaşabilmek için hangi koşulları değiştirmesi gerektiğini net bir şekilde kavrayarak

değerlendirmek ve bireyin kendi verileri üzerindeki kontrolünü güçlendirmek açısından önem taşımaktadır. Ayrıntılar için bknz. Edwards ve Veale, 81.

[777] Wachter vd., "Counterfactual Explanations Without Opening the Black Box", 842-44.

[778] Wachter vd., "Counterfactual Explanations Without Opening the Black Box", 842-44.

[779] Wachter vd., "Counterfactual Explanations Without Opening the Black Box", 842-44.

kendisine stratejik bir yol haritası belirleyebilmektedir[780]. Bu yaklaşım, GDPR'ın veri sahiplerine "anlamlı bilgi" sunulmasına yönelik yükümlülüğünün amacına tam olarak hizmet etmekte ve işverenlerin ticari sırları ifşa etmek ya da sistemlerin kötüye kullanılmasını kolaylaştırmak gibi risklere maruz kalmadan şeffaflık sağlamasını mümkün kılmaktadır[781]. Dolayısıyla alternatif senaryo açıklamaları, tele çalışmada kullanılan algoritmik yönetim sistemlerinin denetimi ve çalışanların itiraz hakkının etkin biçimde kullanılabilmesi açısından mevcut hukuki çerçeveyi tamamlayıcı ve güçlendirici nitelikte kritik bir idari ve teknik tedbir olarak değerlendirilmesi gerekmektedir[782].

4.5.6. Zararın Tazminini İsteme Hakkı

Kişisel verilerin hukuka aykırı işlenmesi nedeniyle zarar gören ilgili kişinin tazminat talep etme hakkı, veri koruma rejiminin temel birini oluşturmaktadır. Bu hak, kişisel verilerin hukuka aykırı şekilde işlenmesi sonucunda bireyin uğradığı zararın giderilmesini amaçlamakta olup gerek KVKK gerekse GDPR'da ifade edilmiştir. KVKK'nın 11. maddesinin 1. fıkrasının (ğ) bendi, ilgili kişiye *"kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme"* yetkisini vermektedir. Ayrıca, Kurul'a yapılacak şikâyet usulünü düzenleyen 14. maddenin üçüncü fıkrasında, *"kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakları saklıdır"* ifadesiyle, vurgulanmaktadır[783]. Benzer şekilde, GDPR 82. maddesi çerçevesinde veri sahibine, kendisine atfedilebilen bir ihlal sonucu maddi veya manevi zarar meydana gelmişse, veri sorumlusu ve/veya veri işleyene karşı tazminat talep etme hakkı tanınmıştır[784]. Görüldüğü üzere GDPR'ın bu konudaki yaklaşımı hem veri sorumlusunu hem de veri işleyeni doğrudan sorumlu kılmasıyla öne çıkmaktadır. Bu durum, öğretide, zarar görene karşı müşterek ve müteselsil bir sorumluluk doğurduğu şeklinde belirtilmektedir[785]. Bu çerçevede hem

---

[780] Wachter vd., "Counterfactual Explanations Without Opening the Black Box", 843,878.
[781] Wachter vd., "Counterfactual Explanations Without Opening the Black Box", 871, 883.
[782] Wachter vd., "Counterfactual Explanations Without Opening the Black Box", 880.
[783] Ekmekçi vd., *Anayasa Mahkemesine bireysel başvurunun temel esasları ve iş ve sosyal güvenlik hukukuna ilişkin kararlar*, 402.
[784] Bryce Goodman ve Seth Flaxman, "European Union regulations on algorithmic decision-making and a 'right to explanation'", *AI magazine* 38, sy 3 (2017): 52.
[785] Yılmaz, "Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması", 224; Kaya, "Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) Kapsamında Ortak Veri Sorumluluğu", 78-84; Mustafa Çağrı Tuna, "Kişisel

KVKK hem de GDPR, ihlalin doğurduğu sonuçların bütün yönleriyle değerlendirilerek, maddi olduğu kadar manevi zararların da giderilmesine imkân tanımaktadır[786].

Tele çalışmada izleme ve gözetleme uygulamaları kapsamında bu hak, önemli sonuçlar doğurabilmektedir. Örneğin, bir çalışanın aktivite izleme yazılımından elde edilen hatalı veya doğru olmayan verilere dayanılarak haksız yere priminin kesilmesi veya terfi alamaması, doğrudan bir maddi zarar teşkil etmektedir. Buna karşılık sürekli olarak evinde izlendiğini bilmenin yarattığı stres, kaygı, aşağılanma hissi veya özel hayatının ihlal edildiği duygusu[787], veri koruma mevzuatı kapsamında açıkça tazmin edilebilen bir manevi zarar olarak kabul edilebilmektedir. İşveren, hukuka aykırı izleme faaliyetiyle bu tür bir zarara yol açtığı takdirde, çalışanın tazminat talebiyle karşı karşıya kalabilmektedir.

Hukuka aykırı ve orantısız nitelikteki izleme ve gözetleme faaliyetleri, çalışanın özel hayatının gizliliği başta olmak üzere temel kişilik haklarının ağır bir ihlali olmasının yanı sıra, işverenin çalışanı koruma ve gözetme yükümlülüğünün de açık bir ihlali niteliği taşımaktadır. Taraflar arasındaki güven ilişkisini temelden sarsarak iş ilişkisinin devamını çalışan açısından çekilmez kılan bu durum, 4857 sayılı İş Kanunu'nun 24. maddesinin II. fıkrası uyarınca ahlak ve iyiniyet kurallarına aykırılık teşkil etmektedir. Bu sebeple, iş sözleşmesini haklı nedenle derhal feshetme hakkını elde eden çalışan, bu feshe bağlı olarak kanundan doğan tazminat ve alacaklarını da talep etme imkânına sahip olmaktadır[788].

4.6. Teknik ve İdari Tedbirler

Tele çalışmada izleme ve gözetleme uygulamalarının hukuka uygun şekilde yürütülebilmesi, işverenin iş organizasyonu kapsamında kişisel veri işleme süreçlerini

---

Verilerin Korunması Hukuku ve Şirketlerin Yükümlülükleri" (Yayınlanmamış Doktora Tezi, Erciyes, Erciyes Üniversitesi, 2024), 152.

[786] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 414-18.

[787] De Stefano ve Taes, "Algorithmic Management and Collective Bargaining", 26-27.

[788] Tekergül, "İşyerinde Elektronik Gözetim Uygulamaları", 122-23; Savran, "İşçinin İşyerinde Elektronik Yöntemlerle İzlenmesi", 156-57; Seda Parlak, "İş İlişkisinde İşçinin İnternet ve E-Posta Kullanımının İzlenmesi ve Gözetlenmesi" (Yayınlanmamış Yüksek Lisans Tezi, Ankara Hacı Bayram Veli Üniversitesi, 2023), 153-55.

yukarıda belirtilen ilkelere dayandırarak açık bir politika hâline getirmesini ve bu politikayı çalışanlara şeffaf biçimde sunmasını gerektirmektedir. Bu politika çerçevesinde işverenin belirli idari ve teknik tedbirler alması zorunludur[789].

Kişisel verilerin işlenmesinde veri güvenliğinin sağlanması amacıyla alınması gereken tedbirler; genel olarak "teknik" ve "idari" olmak üzere iki başlık altında toplanmaktadır[790]. Teknik tedbirler, esas itibarıyla bilgi teknolojileri altyapısına ve bilişim sistemlerine yönelik önlemleri ifade etmektedir. Bu önlemler, kişisel verilerin dış müdahalelere, siber saldırılara ve yetkisiz erişimlere karşı korunmasını hedeflemektedir. İşverenin veri sorumlusu sıfatıyla bu kapsamda özen yükümlülüğü bulunmaktadır. Özellikle uzaktan çalışma ve dijital iletişim araçlarının yaygınlaştığı günümüz çalışma ilişkilerinde, teknik tedbirlerin etkili biçimde uygulanması, işletmenin veri güvenliğinin sağlanmasında da kritik bir rol oynamaktadır. Diğer yandan, idari tedbirler ise kurum içi politika belgeleri oluşturulması, çalışanlara yönelik düzenli eğitim faaliyetlerinin yürütülmesi ve veri işleme süreçlerinin denetimi gibi organizasyonel düzenlemeleri kapsamaktadır[791]. Bu yönüyle idari tedbirler, yalnızca teknik önlemleri tamamlayıcı nitelikte değil, aynı zamanda kişisel veri güvenliğine ilişkin farkındalığın kurumsal düzeyde yerleşmesini sağlayan bütüncül bir güvenlik yaklaşımının da temel bileşenini oluşturmaktadır. Bu kapsamda hem KVKK'nın 12. maddesinin 1. fıkrası hem de GDPR'ın 32. maddesinin 1. fıkrası, veri sorumlularına işlenen kişisel verilerin güvenliğini sağlamak üzere uygun teknik ve

---

[789] Covid-19 salgınında Kurum uzaktan çalışmaya özgü olarak yayımladığı 27.03.2020 tarihli Kamuoyu duyurusunda *"Kişisel verilerin korunması mevzuatı, evden çalışmanın önünde bir engel değildir. Salgın sırasında personel evden çalışabilir ve kendi cihazlarını veya iletişim ekipmanlarını kullanabilir. Kişisel verilerin korunması mevzuatı bunu engellemez, ancak kişisel verilerin güvenliğini sağlamaya yönelik gerekli idari ve teknik tedbirlerin alınması gerekmektedir. Uzaktan çalışmanın doğurabileceği risklerin asgariye indirilmesi adına, sistemler arasındaki veri trafiğinin güvenli iletişim protokolleriyle gerçekleştirilmesi ve herhangi bir zafiyet içermemesinin sağlanması ile anti-virüs sistemlerinin ve güvenlik duvarlarının güncelliğinin sağlanması başta olmak üzere, her türlü tedbirin alınması ve kişisel verilerin güvenliği açısından konuya ilişkin çalışanların dikkatle bilgilendirilmesi gerekmektedir. Ancak unutulmamalıdır ki, çalışanlar tarafından alınacak tedbirler Kanun kapsamında kişisel verilerin güvenliğinin sağlanması noktasında veri sorumlusunun yükümlülüğünü ortadan kaldırmamaktadır" şeklinde belirtmiştir.* Erişim 11.06.2025 https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecind e-KisiselVerilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler

[790] Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) (Kişisel Verileri Koruma Kurumu, 2018), 27 vd., https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf; Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) (2025), 9-10.

[791] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 230.

idari tedbirleri alma yükümlülüğü getirmektedir. Aşağıda öncelikle teknik tedbirler ardından idari tedbirler ayrı başlıklar altında incelenmeye çalışılacaktır.

4.6.1. Teknik Tedbirler

Tele çalışma modelinde kurumsal veri ve sistemlerin güvenliğinin sağlanması, işverenlerin öncelikli sorumlulukları arasında yer almaktadır. Zira bu modelde kullanılan iletişim araçları yapıları gereği siber güvenlik açıklarına daha fazla maruz kalmakta ve kişisel veri ile kurumsal bilginin üçüncü kişilerin eline geçmesi riskini artırmaktadır. Tele çalışanın kullandığı veri akışı sağlayan tüm teknolojik araçlarda veri depolama ve aktarım süreçlerinin güvenliğini sağlamak için gerekli teknik önlemler alınmalıdır. Bu kapsamda alınması gereken temel teknik tedbirler bu bölümde alt başlıklar hâlinde ele alınacaktır.

4.6.1.1. Güvenli Ağ Erişimi ve İletişim Altyapısı

Tele çalışmanın yaygınlaşmasıyla birlikte, çalışanlara ait kişisel verilerin ve kurumsal bilgilerin korunması için öncelikle çalışanların bağlanılan ağın ve işletmenin kullandığı iletişim altyapısının güvenliği sağlanması gerekmektedir[792]. Tele çalışma biçimlerinde kullanılan ağın güvenliğini sağlamanın en temel yollarından biri, çalışanların kurum sistemlerine güvenli şekilde bağlanmasını sağlayan "sanal özel ağ" bir diğer deyişle VPN (virtual private network) teknolojisi oluşturmaktadır[793]. VPN, çalışanın bilgisayarı ile işverenin ağı arasında adeta gizli bir tünel kurmaktadır. Bu tünelden geçen bilgiler özel bir şekilde şifrelenmektedir. Böylece, eğer çalışan evindeki interneti ya da halka açık bir Wi-Fi ağını kullanıyorsa, araya girip bilgi

[792] Karen Scarfone vd., "Guide to enterprise telework and remote access security", NIST Special Publication 800, sy 2009 (2009): ES-1; David Adame, "Managing and Securing Endpoints: A Solution for a Telework Environment" (Master's project, California State University, 2021), 8, https://scholarworks.lib.csusb.edu/etd/1316.
[793] Isabela Porcius, "The Rise of Telework and the Struggle Towards Cyber Security", *Fiat Iustitia* 1, sy 1 (2021): 151-55.

çalmaya çalışan kişiler bu verileri görememektedir[794]. VPN, bu yüzden özellikle tele çalışmada verilerin korunması için gerekli olmaktadır[795].

Ayrıca, tele çalışmada sık sık veri gönderme ve alma işlemleri gerçekleştiğinden, bu verilerin internet üzerinden (iletişim altyapısı) güvenli bir şekilde iletilmesi de hayati önem taşımaktadır. Burada devreye HTTPS[796] ve TLS[797] gibi şifreleme teknolojileri girmektedir. Bu teknolojiler, özellikle çalışanın performansına veya davranışlarına ilişkin toplanan izleme verileri gibi kişisel bilgilerin, internet üzerinden aktarılırken kötü niyetli kişiler tarafından ele geçirilmesini önlemektedir[798].

İşverenlerin doğrudan müdahale edemediği ev internet bağlantılarında başka bazı güvenlik riskleri de bulunmaktadır. Bu nedenle işverenler, çalışanlara güçlü Wi-Fi şifreleri oluşturma, modem veya yönlendirici yazılımlarını güncel tutma, misafir ağı kurma ve varsayılan parolaları değiştirme gibi konularda rehberlik sağlaması gerekmektedir[799]. Bu basit ama etkili adımlar, kötü niyetli kişilerin ev ağına sızmasını zorlaştırmaktadır.

4.6.1.2. Kullanılan Donanımların (Uç Nokta) Güvenliği

Modern çalışma hayatında kullanılan donanımların çeşitliliği, geleneksel olarak tanımlanan dizüstü bilgisayarlar ve akıllı telefonların ötesine geçmiştir. Bu donanımlar siber güvenlik literatüründe "uç nokta" (endpoint) olarak adlandırılmaktadır[800]. Uç nokta, bir ağa bağlanan ve veri alışverişi yapan masaüstü bilgisayar, dizüstü bilgisayar, akıllı telefon veya tablet gibi son kullanıcı cihazlarını tanımlamaktadır. Bu bağlamda,

---

[794] Scarfone vd., "Guide to enterprise telework and remote access security", 9-11; Adame, "Managing and Securing Endpoints", 32-35; Porcius, "The Rise of Telework and the Struggle Towards Cyber Security", 152-53.
[795] B.S. Mahlangu ve B. Schutte, "Analysing Information Technology Risks Affecting South African Government Employers Due to Remote Working", *Journal for New Generation Sciences* 22, sy 2 (2024): 48, http://journals.co.za/doi/10.47588/jngs.2024.22.02.a1.
[796] HTTPS (HyperText Transfer Protocol Secure), internet sitelerinin güvenli versiyonudur. Bir sitenin adresi "https://" ile başlıyorsa, o sitede girilen bilgilerin şifrelenerek iletildiği anlaşılır. Örneğin, bir kurumsal uygulamaya girilen şifre ya da bir belge yüklemesi, HTTPS ile korunur.
[797] TLS (Transport Layer Security) ise e-posta ve mesajlaşma gibi başka dijital iletişim araçlarında kullanılan bir şifreleme protokolüdür. Bu sayede gönderilen veriler sadece alıcısı tarafından okunabilir hâle gelir.
[798] Scarfone vd., "Guide to enterprise telework and remote access security", 2-8.
[799] Porcius, "The Rise of Telework and the Struggle Towards Cyber Security", 155.
[800] Adame, "Managing and Securing Endpoints", 1-2.

bir işyeri ağına güvenlik duvarının dışından bağlanan herhangi bir cihaz da uç nokta olarak kabul edilmektedir[801]. Bu tanım; masaüstü bilgisayarları, tabletleri, mobil cihazları, nesnelerin interneti (IoT) cihazlarını[802], sunucuları ve hatta ATM (Automated Teller Machine) makineleri ile tıbbi cihazlar gibi özel ekipmanları da kapsamaktadır. Tele çalışma modelinde bu cihazlar, çalışanların işyeri kaynaklarına erişim sağladığı ve verileri işlediği birincil ara yüzler hâline gelmektedir[803]. Bu durum, işletmenin geleneksel ve güvenli kabul edilen ağ sınırlarının, çalışanların ev ağları gibi kurumun doğrudan denetimi dışındaki ve siber tehditlere daha açık ortamlara taşımaktadır[804]. Tele çalışanların fiziksel olarak işyeri dışında, özellikle ev ağları veya açık Wi-Fi ağları gibi daha az güvenli ortamlarda çalışması, uç noktaların siber saldırılara maruz kalma riskini artırmaktadır[805].

Uç nokta güvenliğinde alınması gereken başlıca tedbirler arasında cihazların güvenli yapılandırılması, gereksiz yazılımların kaldırılması, kötü amaçlı yazılımlara karşı antivirüs programlarıyla koruma sağlanması[806], kişisel güvenlik duvarlarının kullanımı, yazılım güncellemelerinin düzenli uygulanması, cihaz seviyesinde veri şifreleme (örneğin, tam disk şifrelemesi), izleme yazılımlarının güvenliğinin sağlanması ve "kendi cihazını getir (BYOD- bring your own device)" politikalarının oluşturulması yer almaktadır[807]. Uç nokta güvenliğini destekleyen teknolojiler arasında veri kaybını önleme (DLP- data loss prevention) araçları, yeni nesil güvenlik duvarları (NGFW- next generation firewall), birleşik tehdit yönetimi (UTM- unified threat management) sistemleri ve mobil cihaz yönetimi (MDM- mobile device management) çözümleri önemli rol oynamaktadır[808].

---

[801] "Uç Nokta Nedir?", Microsoft, erişim 04 Haziran 2025, https://www.microsoft.com/tr-tr/security/business/security-101/what-is-an-endpoint; "Uç Nokta Güvenliği & Uç Nokta Koruması", Kaspersky, 27 Nisan 2022, https://www.kaspersky.com.tr/resource-center/definitions/what-is-endpoint-security.
[802] Bknz. 3.3.1.9. Bölüm
[803] Porcius, "The Rise of Telework and the Struggle Towards Cyber Security", 152.
[804] Adame, "Managing and Securing Endpoints", 3.
[805] Scarfone vd., "Guide to enterprise telework and remote access security", 3-5; Porcius, "The Rise of Telework and the Struggle Towards Cyber Security", 5.
[806] Falque-Pierrotin, *Opinion 2/2017 on Data Processing at Work*, 16-18.
[807] Ayrıntılı koruma yöntemleri için bknz. Adame, "Managing and Securing Endpoints", 25-63; Porcius, "The Rise of Telework and the Struggle Towards Cyber Security", 153-56.
[808] Falque-Pierrotin, *Opinion 2/2017 on Data Processing at Work*, 12-13.

Uç nokta güvenliği yalnızca teknik çözümlerden ibaret olmayıp, çalışanların farkındalığının artırılmasını ve güvenlik politikalarına uyumu da içeren bütüncül bir yaklaşımı gerektirmektedir. Böyle bütüncül bir strateji, tele çalışma modelinde hem kurumsal hem de kişisel verilerin etkin biçimde korunmasını sağlayarak hukuki yükümlülüklere uyumu desteklemektedir[809].

4.6.1.3. Veri Şifreleme (Kriptolama) Yöntemleri

Veri şifreleme (kriptolama), kişisel verilerin korunmasında temel teknik tedbirlerden biri olup, verilerin yetkisiz erişime karşı anlaşılmaz bir forma dönüştürülmesini sağlayan bir güvenlik yöntemini oluşturmaktadır[810]. Bu yöntem, verilerin ele geçirilmesi durumunda dahi içeriğinin çözülememesini amaçlamakta ve özellikle tele çalışma bağlamında, çalışanlara kişisel verilerin korunmasında kritik rol oynamaktadır[811]. Nitekim GDPR başlangıç bölümünün 83. maddesinde, veri güvenliğinin sağlanması için risklerin değerlendirilmesi ve özellikle şifreleme gibi uygun teknik ve organizasyonel tedbirlerin uygulanması gerektiği açıkça ifade edilmektedir.

Veri şifreleme iki temel biçimde uygulanmaktadır: aktarım hâlindeki verilerin şifrelenmesi (encryption in transit) ve durağan hâldeki verilerin şifrelenmesi (encryption at rest). Aktarım hâlindeki verilerin şifrelenmesi tele çalışanların cihazları ile kurum sistemleri arasında sürekli bir veri akışı söz konusu olduğundan, bu tür şifreleme özel bir önem taşımaktadır. Bu süreçte, HTTPS, TLS veya VPN gibi şifreleme protokolleri kullanılarak, iletim sırasında verilerin üçüncü kişilerce ele geçirilmesi önlenmektedir[812]. Özellikle izleme araçları aracılığıyla elde edilen kişisel verilerin güvenli aktarımı açısından zorunluluktur[813]. Durağan hâldeki verilerin şifrelenmesi ise verilerin; cihazlar, sunucular veya yedekleme sistemleri gibi depolama alanlarında korunması için tam disk şifrelemesi, veri tabanı şifrelemesi veya dosya

[809] Adame, "Managing and Securing Endpoints", 76-78; Porcius, "The Rise of Telework and the Struggle Towards Cyber Security", 153.
[810] Scarfone vd., "Guide to enterprise telework and remote access security", 4-5.
[811] Scarfone vd., "Guide to enterprise telework and remote access security", 4-5.
[812] Porcius, "The Rise of Telework and the Struggle Towards Cyber Security", 155.
[813] Scarfone vd., "Guide to enterprise telework and remote access security", 4-4.

bazlı şifreleme yöntemleri kullanılmaktadır[814]. Böylece cihaz kaybı, hırsızlık veya yetkisiz erişim durumlarında dahi verilerin gizliliğini korunmaktadır[815]. Güvenli ağ, güvenli cihaz ve şifrelenmiş veri üçgeni, tele çalışmada veri güvenliğinin temelini oluşturmaktadır. Ancak bu temel katman, veriye kimin, ne zaman ve ne yetkiyle erişebileceğini düzenleyen daha spesifik kontrol mekanizmalarıyla desteklenmesi gerekmektedir.

4.6.1.4. Erişim Kontrol Mekanizmaları ve Kimlik Doğrulama

Tele çalışma modelinde kişisel verilerin ve özellikle çalışanlara ait izleme verilerinin yetkisiz erişim, değişiklik ve ifşaya karşı korunmasında etkin erişim kontrolü ve güçlü kimlik doğrulama yöntemleri kritik öneme taşımaktadır[816]. Bu bağlamda, kimlik doğrulama, kullanıcıların iddia ettikleri kişi olduklarının doğrulanması; erişim kontrolü (yetkilendirme) ise doğrulanan kullanıcının hangi verilere ve kaynaklara erişebileceğinin belirlenmesi işlemini ifade etmektedir.

Kimlik doğrulamada güçlü parola politikaları önem arz etmektedir. Uzaktan erişim durumunda parola güvenliğini desteklemek için çok faktörlü kimlik doğrulama (MFA-multi-factor authentication) yöntemlerinin kullanılması önerilmektedir[817]. Tele çalışmada uzaktan erişim çalışma biçiminin doğasından kaynaklanmaktadır. Bu çalışma biçiminde MFA, parola gibi kullanıcının bildiği bir unsurun yanı sıra sahip olduğu bir cihaz veya farklı onay işlemleri gibi özellik gibi ek unsurlar gerektirerek güvenliği artırmaktadır[818]. Tele çalışanlara yönelik şifre koruma kapsamında tüm kullanıcı hesaplarında, büyük harf, küçük harf, rakam ve özel karakter içeren güçlü

---

[814] Demirbaş, *Kişisel Verileri Koruma Hukukunda Veri Sorumlusu ve Yükümlülükleri*, 99.
[815] Scarfone vd., "Guide to enterprise telework and remote access security", ES-1, 4-5.
[816] Soner Altıntaş ve Fatma Barkuş, "Dijital Ortamlarda Kişisel Veri Güvenliği Kavramı Üzerine Bir Derleme Çalışması", *Electronic Journal of Vocational Colleges*, sy 13 (2023): 50-51.
[817] Kişisel Verileri Koruma Kurumu, *Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)* (2018), 22.
[818] Mahlangu ve Schutte, "Analysing Information Technology Risks Affecting South African Government Employers Due to Remote Working", 51; "A Strong Password and the Importance of MFA to Protect Your Data - Cakemail Blog", erişim 05 Haziran 2025, https://www.cakemail.com/blog/post/a-strong-password-and-the-importance-of-mfa-to-protect-your-data.

parolaların kullanılması ve düzenli aralıklarla değiştirilmesi zorunluluğunun getirilmesi gerekmektedir[819].

Yetkilendirme sürecinde, "en az yetki ilkesi" (principle of least privilege) ve "bilmesi gereken ilkesi" (need-to-know principle) temel alınması gerekmektedir. En az yetki ilkesi, kullanıcının sistemdeki görevini ifası için asgari yeterlilikte yetki verilmesini ifade etmektedir. Bilmesi gereken ilkesi, çalışanların kendi görev ve sorumluluk alanları ile sınırlı düzeyde bilgiye erişebilmesi anlamına gelmektedir. Ayrıca çalışanların yalnızca görevleriyle ilişkili verilerle sınırlı erişimlerinin sağlanması için rol tabanlı erişim kontrolü (RBAC-Roll based access control) yöntemleri uygulanmalıdır[820]. Çalışanların yalnızca kendi görev tanımlarına uygun verilere erişebilmesini sağlamak üzere detaylı bir yetkilendirme matrisinin oluşturulması gerekmektedir[821]. Erişim düzeyleri teknik araçlarla sınırlandırılmalı, örneğin insan kaynakları biriminin personel özlük dosyalarına erişimi sağlanırken, bu verilere diğer departmanların erişimi engellenmelidir. Benzer şekilde, bir tele çalışanın performansını denetleyen bir ekip yöneticisinin, o çalışanın aktivite raporlarına ve tamamladığı görevlere ilişkin verilere erişim yetkisi olabilir; ancak aynı yöneticinin, çalışanın şifrelenmiş sağlık raporlarının veya diğer özel nitelikli verilerinin tutulduğu bir sisteme erişim yetkisi olmamalıdır. Ayrıca, sistem ve veri erişimlerinin düzenli olarak kayıt altına alınması, güvenlik ihlallerinin hızlı şekilde tespiti ve yönetilmesi açısından önem arz etmektedir[822].

4.6.1.5. Verilerin Depolanması ve Veri Kaybının Önlemesi

Tele çalışma düzeninde kişisel veriler, temel olarak yerel sistemler veya bulut tabanlı platformlarda depolanmakta; bu durum, veri güvenliği açısından farklı sorumlulukları ve riskleri beraberinde getirmektedir. Veri sorumlusu konumundaki işverenin doğrudan kontrolünde olan yerel sistemlerin güvenliğini sağlama yükümlülüğü net bir

---

[819] Rukiye Civan Kemiksiz, "Kişisel veri güvenliği üzerine bir alan araştırması: dijital yerliler ve dijital göçmenlerin güvenlik algıları", *Maltepe Üniversitesi İletişim Fakültesi Dergisi* 9, sy 1 (2022): 84-87; Altıntaş ve Barkuş, "Dijital Ortamlarda Kişisel Veri Güvenliği Kavramı Üzerine Bir Derleme Çalışması", 62.
[820] Mahlangu ve Schutte, "Analysing Information Technology Risks Affecting South African Government Employers Due to Remote Working", 51-52.
[821] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 228.
[822] Scarfone vd., "Guide to enterprise telework and remote access security", 5-1.

şekilde kendisine aitken, verilerin bulutta depolanması durumu daha karmaşık bir hâl almaktadır. Bulut depolama, verilerin işverenin kontrol alanından çıkmasına yol açarak hukuka aykırı erişim riskini artırmanın yanı sıra, bu verilerin yurt dışındaki sunucularda saklanması ihtimalini de doğurmaktadır. Bu durum, Kişisel Verilerin Korunması Kanunu kapsamında özel düzenlemelere tabi bir yurt dışı veri aktarımı anlamına geldiğinden, hizmet sağlayıcının sunduğu hem teknik güvenlik önlemlerinin hem de yasal güvencelerin işveren tarafından titizlikle incelenmesi zorunludur[823]. Depolama yöntemi ne olursa olsun verilerin bütünsel korunması ise şifreleme, uzaktan erişimde çift aşamalı kimlik doğrulama ve hizmet sona erdiğinde şifreleme anahtarlarının imhası gibi temel teknik tedbirlerin eksiksiz bir şekilde uygulanmasına bağlı bulunmaktadır[824].

Tele çalışma modeli, verilere farklı cihaz ve ağlardan erişimi mümkün kılarak veri kaybı ve sızıntı risklerini önemli ölçüde artırmaktadır. Bu risklerin yönetimi için geliştirilen Veri Kaybı Önleme (DLP) sistemleri, kurumsal verilerin yetkisiz kişilerle paylaşılmasını veya işyeri dışına aktarılmasını önlemeye yönelik teknik bir kalkan görevi görmektedir[825]. Bu sistemler, verileri tanımlayıp sınıflandırdıktan sonra tüm hareketlerini sürekli izlemekte ve belirlenmiş güvenlik politikalarına aykırı bir durum tespit ettiğinde engelleme, şifreleme veya uyarı verme gibi koruyucu tedbirleri otomatik olarak devreye almaktadır[826]. Bu teknolojinin en kritik uygulama alanını ise tele çalışma sırasında toplanan ve çalışanın özel hayatına dair çıkarımlar içerebilen ekran görüntüleri gibi kişisel verilerin korunması oluşturmakta; DLP sisteminin, bu tür gizliliği yüksek verilerin e-posta ile gönderilmesi veya harici belleğe kopyalanması gibi eylemleri otomatik olarak engelleyerek veri güvenliğini en üst seviyede sağlaması gerekmektedir.

DLP sistemlerinin koruma kapsamı üç temel veri türü üzerinden şekillenmektedir: kullanımdaki veriler (cihazlarda aktif olarak erişilen veya işlenen veriler), aktarım

---

[823] Naeem Allah Rakha, "Ensuring Cyber-security in Remote Workforce: Legal Implications and International Best Practices", *International Journal of Law and Policy* 1, sy 3 (2023): 13.
[824] Kişisel Verileri Koruma Kurumu, *Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)* (2018), 22.
[825] Stanley Ugochukwu Emenike, "Data loss prevention in a remote work environment" (Master Degree Project, University of Skövde, 2021), 1, https://www.diva-portal.org/smash/record.jsf?pid=diva2:1578629.
[826] Emenike, "Data loss prevention in a remote work environment", 1-2.

hâlindeki veriler (ağlar üzerinden iletilen veriler) ve durağan hâldeki veriler (sunucu, bulut depolama alanları ve veri tabanlarında saklanan veriler). Bu farklı veri türlerinin tamamının korunması, kapsamlı bir veri güvenliği yaklaşımı için gereklidir[827]. Ayrıca veri kaybını önlemek adına düzenli aralıklarla yedekleme yapılması, bu yedeklerin güvenli ortamlarda muhafaza edilmesi ve mümkünse farklı fiziksel konumlarda veya güvenli bulut hizmetlerinde şifrelenmiş olarak saklanması önem arz etmektedir[828].

Tele çalışmada kişisel verilerin korunması açısından dikkat edilmesi gereken bir diğer önemli konu, sıkça kullanılan online video konferans platformlarıdır. Tele çalışmanın yaygınlaşmasıyla birlikte Zoom, Google Meet ve Microsoft Teams gibi uygulamaların kullanımı da artmıştır. Söz konusu platformlar çoğunlukla bulut hizmet sağlayıcıları aracılığıyla çalıştığından, verilerin yurt dışına aktarılması söz konusu olabilmektedir. Dolayısıyla bu tür hizmetler aracılığıyla gerçekleştirilen toplantı kayıtları, paylaşılan belgeler ve sohbet içeriklerinin depolanması ve aktarılması süreçlerinde, veri işleme faaliyetlerinin ilgili veri koruma ilke ve esaslarına uygun olarak yürütülmesi ve yurt dışı aktarımlar için yeterli güvencelerin sağlandığından emin olunması gerekmektedir[829].

4.6.1.6. Güvenli Yazılım ve Uygulama Yapılandırması

Tele çalışma modelinde kullanılan dijital bileşenlerin, özellikle de çalışan izleme yazılımlarının güvenlik açıklarından arındırılması ve gizlilik odaklı yapılandırılması, veri güvenliği açısından kritik önem taşımaktadır. Söz konusu süreç, yazılımların seçimi, kurulumu, yapılandırılması, güncellenmesi ve kullanımdan kaldırılması aşamalarında güvenlik ve veri koruma ilkelerinin uygulanmasını kapsamaktadır[830]. Bu çerçevede işverenlerin veri sorumlusu olarak kullandıkları yazılımlara ilişkin birtakım önlemleri almaları gerekmektedir. İşverenler, tele çalışma ve çalışan izleme süreçlerinde kullanacakları yazılımları seçerken, veri güvenliği açısından güvenilir ve

[827] Emenike, "Data loss prevention in a remote work environment", 5-6.
[828] Rakha, "Ensuring Cyber-security in Remote Workforce: Legal Implications and International Best Practices", 10.
[829] Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 12; Ünal Adınır, "Tele çalışmada verilerin korunması", 991-93.
[830] Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) (2018), 23.

düzenli olarak güncellenen programları tercih etmelidir[831]. Ayrıca, bu yazılımların kişisel verilerin korunması hukukuna uygun çalışması ve özellikle GDPR gibi uluslararası standartlara uyum sağlaması gerekmektedir. Çalışanların izlenmesine yönelik yazılımlarda, programın verileri nasıl topladığı, sakladığı ve kimlerin erişebildiği gibi hususlar dikkatle değerlendirilmelidir. Yapılacak değerlendirme, gizliliğin tasarım aşamasından itibaren gözetilmesi ve başlangıçtan itibaren gizliliği esas alan yapılandırma ilkesinin ilk adımıdır. İşveren, daha en baştan, varsayılan ayarları en yüksek gizlilik seviyesinde ve sadece meşru amaç için zorunlu olan verileri toplayan, daha az müdahaleci izleme yazılımlarını tercih etmelidir. Aksi takdirde yaşanacak bir veri ihlali, veri koruma mevzuatına aykırılık oluşturmaktadır[832].

İzleme ve gözetleme uygulamaları, işverenin meşru denetim yetkisi ile çalışanın mahremiyet hakkı arasındaki dengeyi sağlama amacıyla farklı kategorilere ayrılmaktadır[833]. "En iyi uygulamalar" olarak nitelendirilen izleme yöntemleri, işverenin işin yürütülmesini sağlama, işçinin yükümlülüklerini yerine getirip getirmediğini denetleme ve gerektiğinde soruşturma yapma gibi meşru amaçlarını yerine getirirken çalışanın mahremiyetine en az müdahalede bulunan uygulamalardır. "Riskli uygulamalar", işverene daha sınırlı bir koruma sunarken çalışanın mahremiyetine olan etkisi de kısıtlı kalmaktadır. Bu yöntemler, ağırlıklı olarak işçinin yükümlülüklerini denetleme ve soruşturma amacıyla kullanılmaktadır. Ancak, bu tür uygulamaların işin yürütülmesi gibi temel bir amaçla dahi kullanılabilmesi için orantılılık ilkesine uygun olup olmadığının ayrıca değerlendirilmesi şarttır. "Sınırda uygulamalar" ise işverene daha yüksek koruma sağlamasına rağmen mahremiyeti ciddi şekilde ihlal eden tekniklerdir. Bu nedenle, yalnızca istisnai durumlarda ve tüm izleme amaçları için uygulanabilir kabul edilmektedirler. Son olarak, zayıf uygulamalar, işverenin çıkarlarını yeterince korumadan çalışanın mahremiyetine ağır müdahalede bulunmaktadır. Bu sebeple kural olarak yasaklanmaları gerekmekte; yalnızca sıkı bir orantılılık denetiminden geçebilen çok istisnai soruşturma hâllerinde sınırlı kullanımlarına izin verilebilmektedir[834].

---

[831] Altıntaş ve Barkuş, "Dijital Ortamlarda Kişisel Veri Güvenliği Kavramı Üzerine Bir Derleme Çalışması", 51.
[832] Mahlangu ve Schutte, "Analysing Information Technology Risks Affecting South African Government Employers Due to Remote Working", 33.
[833] Ciocchetti, "The Eavesdropping Employer", 289.
[834] Ciocchetti, "The Eavesdropping Employer", 289.

İşverenin denetim yetkisiyle çalışanın mahremiyeti arasındaki bu hassas denge, özellikle dijital izleme araçlarının yoğun olarak kullanıldığı tele çalışma modelinde daha da önem kazanmaktadır. Tele çalışma modelinde çalışanların dijital ortamda gerçekleştirdiği işlemlerle ilgili çeşitli kayıtlar (log kayıtları) tutulmaktadır. Örneğin, çalışanların sisteme giriş-çıkış saatleri, yapılan işlemler veya veri erişimleri kaydedilmektedir. Bu kayıtlar, ileride ortaya çıkabilecek bir uyuşmazlık veya güvenlik ihlali durumunda, olayların ne şekilde gerçekleştiğini tespit edebilmek için önemli bir işlev görmektedir[835]. Ayrıca bu tür kayıtların doğruluğu ve güvenli biçimde saklanması, hem işverenin veri güvenliğini sağlama yükümlülüğünün bir gereği hem de hukuki sorumlulukların yerine getirilmesi açısından gereklidir[836].

İşverenin bu veri güvenliği yükümlülüğü, sadece kayıtların doğru tutulmasını değil, aynı zamanda bu kayıtların ve diğer kurumsal verilerin bulunduğu tüm dijital altyapının teknik olarak korunmasını da gerektirir. Bu kapsamda, tüm yazılımların (işletim sistemleri, uygulamalar, tarayıcılar, eklentiler ve izleme araçları dâhil) bilinen güvenlik açıklarına karşı korunması için en son güvenlik yamalarının ve güncellemelerinin düzenli ve zamanında uygulanması hayati bir önem taşımaktadır[837]. Özellikle işyeri için geliştirilen özel yazılımlar veya kritik öneme sahip üçüncü taraf uygulamalar için, kullanıma alınmadan önce ve periyodik olarak güvenlik testleri (örneğin, sızma testleri, kod analizleri) ve zafiyet taramaları yapılmalıdır[838]. Bulut tabanlı hizmetler ve çevrim içi uygulamaların kullanımı, çalışan verilerinin uluslararası aktarımına yol açabilmektedir. Bu aktarım yalnızca yeterli düzeyde veri koruma sağlandığında yapılmalıdır. Bununla birlikte çalışanların işverenin erişemeyeceği özel alanlar oluşturmalarına olanak tanınmalıdır[839].

---

[835] Ayrıntlı bilgi için bknz. Campbell, "Security and Privacy Analysis of Employee Monitoring Applications".
[836] Nadeer Jansen, "Enhancing Cybersecurity Threat Prevention Through Information Security Event Management (SIEM) and Policy Deployment Effectiveness", preprint, Unpublished, 2023, 2, https://doi.org/10.13140/RG.2.2.33723.02088; Elisha Blessing ve K Hubert, "Security Auditing and Monitoring: Incident Response and Management", Hall Open Science, hal-04972073, 2024, 4-5, https://hal.science/hal-04972073v1; Sandeep Bhatt vd., "The Operational Role of Security Information and Event Management Systems", IEEE Security & Privacy 12, sy 5 (2014): 35-38, https://doi.org/10.1109/MSP.2014.103.
[837] Del Castillo, *Artificial Intelligence, Labour and Society*, 150-51.
[838] Altıntaş ve Barkuş, "Dijital Ortamlarda Kişisel Veri Güvenliği Kavramı Üzerine Bir Derleme Çalışması", 6.
[839] Falque-Pierrotin, *Opinion 2/2017 on Data Processing at Work*, 22-24.

Özellikle günümüzde artarak kullanılan yapay zekâ ve makine öğrenmesine dayalı yazılımların güvenilirliği için şeffaflık, hesap verebilirlik ve etik ilkelere uyum esas teşkil etmektedir. Kullanılan yazılımların işleyişinin anlaşılabilir olması, veri setlerinin doğru ve çeşitli olması insan haklarının korunmasına katkı sağlamaktadır[840]. Bu unsurlar sağlanmadığında, ortaya çıkacak zararlardan geliştirici ve uygulayıcıların sorumlu tutulması; ayrıca bireylerin veri üzerindeki denetim yetkisinin güçlendirilmesi ve ayrımcılık risklerine karşı gerekli hukuki yaptırımların mekanizmalarının sağlanması gerekmektedir[841].

GDPR'ın 25. maddesinde düzenlenen gizliliğin tasarım aşamasından itibaren gözetilmesi ve başlangıçtan itibaren gizliliği esas alan yapılandırma ilkesi, kullanılan tüm yazılım ve sistemlerin (işletim sistemleri, uygulamalar, izleme araçları dâhil) baştan itibaren ve tüm kullanım süresince en yüksek düzeyde güvenlik ve gizlilik sağlayacak şekilde yapılandırılmasını zorunlu kılmaktadır. Bu kapsamda, yalnızca işin yürütülmesi için gerekli fonksiyonlar aktif tutulmalı, gereksiz tüm özellikler, hizmetler ve veri toplama modülleri devre dışı bırakılmalıdır[842]. Böylelikle, hem saldırı yüzeyi daraltılmakta hem de gereksiz veya amacı aşan veri işleme riskleri asgari düzeye indirilmektedir. Bu yaklaşım teknik ve organizasyonel tedbirlerin iş süreçlerine bütüncül ve etkili biçimde entegre edilmesini gerektirmektedir. Alınacak önlemlerin

---

[840] Del Castillo, *Artificial Intelligence, Labour and Society*, 220.

[841] Bozkurt Gümrükçüoğlu ve Yakacak, "Yapay Zekânın İşe Alım Süreçlerinde Kullanımı ve Algoritmik Ayrımcılık", 1747-48.

[842] Benzer bir fikirle geliştirilen asla güvenme (zero trust) yaklaşımı, günümüzün dinamik ve sınırları belirsiz çalışma ortamında, geleneksel ağ güvenliği yöntemlerinin yetersiz kaldığı noktada öne çıkan modern bir siber güvenlik stratejisidir. Asla güvenme, en genel ifadeyle, hiçbir kullanıcıya, cihaza veya kaynağa otomatik olarak güvenilmeyen ve tüm erişimlerin sürekli olarak doğrulandığı bir güvenlik modelidir. Bir başka deyişle "asla güvenme, daima doğrula" ilkesiyle hareket edilir. Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü'nün (National Institute of Standards and Technology -NIST) tanımına göre asla güvenme, savunmayı statik ve ağ tabanlı sınırların ötesine taşıyarak, güvenliği kullanıcı, cihaz ve kaynak ekseninde sürekli bir doğrulama ve kontrol paradigmasına dönüştürmektedir. Pandemi sonrası dönemde, çalışanlar ve cihazlar ağ dışından da sistemlere eriştiği için, güvenliğin sadece kurum ağıyla sınırlı tutulması yetersiz kalmıştır. 2020'de yapılan araştırmalar, Kuzey Amerika'daki kuruluşların önemli bir bölümünün asla güvenme projeleri başlattığını göstermiştir. Bu yaklaşımın temelinde, uç noktaların ve erişimlerin etkin şekilde yönetilmesi, görünürlüğün artırılması ve tüm erişim taleplerinin doğrulanması yer alır. Microsoft'un da benimsediği bu modelde, en az ayrıcalık prensibi, ağ, kullanıcı ve uygulama bazında segmentasyon ile sürekli risk değerlendirmesi esastır. Microsoft Defender for Endpoint ve Intune gibi araçlar, bu modele geçişi destekleyerek, cihazların kimliğinin doğrulanması, erişimlerin kontrollü sağlanması ve olası bir ihlal durumunda cihazların hızla izole edilmesini mümkün kılmaktadır. Ayrıntılı bilgi için bknz. V. Stafford, "Zero trust architecture", *NIST special publication* 800, sy 207 (2020): 1-50; Adame, "Managing and Securing Endpoints", 78-80.

seçimi ise işleme faaliyetinin niteliği, kapsamı, amacı, teknolojinin güncelliği ve uygulama maliyetleri gibi kriterlere dayanmaktadır[843].

4.6.1.7. Otomatik Karar Alma Süreçlerinde Anlamlı İnsan Müdahalesi

Otomatik karar alma süreçlerinde anlamlı insan müdahalesi, bir yapay zekâ sisteminin ürettiği ve bireyler üzerinde hukuki veya benzer şekilde önemli etkiler doğuran kararların, yetkin bir insan tarafından gözden geçirilmesi, sorgulanması ve nihai olarak değiştirilebilmesi ilkesidir. Tele çalışmada yaygınlaşan yapay zekâ destekli izleme teknolojileri, çalışanların performansını değerlendirme, görev dağılımı yapma gibi süreçlerde sıklıkla otomatik karar alma ve profilleme mekanizmalarını kullanmaktadır[844]. Bu sistemlerin tamamen insan etkileşiminden bağımsız çalışması; adalet, şeffaflık ve ayrımcılık yasağı ilkeleri bakımından ciddi riskler barındırdığı için, anlamlı insan müdahalesi bu riskleri yönetmede en kritik idari tedbir ve hukuki güvence olarak kabul edilmektedir.

İnsan müdahalesinin gerekliliği, artık yalnızca etik bir beklenti olmaktan çıkıp bağlayıcı bir hukuki norma dönüşmüştür. Nitekim AB Yapay Zekâ Tüzüğü, 14. maddesi uyarınca insan müdahalesini, yüksek riskli olarak sınıflandırılan tüm yapay zekâ sistemleri için zorunlu kılmıştır. Bu düzenleme, sistemi kullanan işverenlere, denetimi gerçekleştirecek yetkin kişileri belirleme ve bu kişilere sisteme müdahale etme, onu durdurma veya sonuçlarını geçersiz kılma yetkisi verme yükümlülüğü getirmektedir[845]. Türk hukukunda ise, AB Yapay Zekâ Tüzüğü'ne benzer şekilde insan müdahalesini doğrudan zorunlu kılan bir düzenleme henüz bulunmamaktadır. Ancak KVKK'nın 11. maddesinin 1. fıkrasının (g) bendi, ilgili kişiye "işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme" hakkı tanımaktadır. Bu itiraz hakkının anlamlı ve işlevsel olabilmesi, otomatik kararın yetkin bir insan tarafından yeniden değerlendirilmesini zorunlu kılmaktadır. Bu durum, Türk hukuku açısından da insan müdahalesinin dolaylı bir gereklilik olduğunu göstermektedir.

---

[843] L. Jasmontaite vd., "Data Protection by Design and by Default":, *European Data Protection Law Review* 4, sy 2 (2018): 168-89, https://doi.org/10.21552/edpl/2018/2/7.
[844] Otomatik karar alma, profilleme ve bunlara karşı itiraz hakkı hakkında ayrıntılı bilgi için bknz. 4.4.9. Bölüm
[845] Voigt ve Hullen, *The EU AI Act*, 95-116.

Bu hukuki gelişmeler ışığında, bu bölümde incelenecek olan anlamlı insan müdahalesi modelleri, tele çalışmada kullanılan yüksek riskli izleme araçları için uyulması gereken hukuki bir standardın pratik uygulamaları olarak ele alınmalıdır.

4.6.1.7.1. Anlamlı İnsan Müdahalesinin Önemi

Daha önce de ifade edildiği üzere, yapay zekâ teknolojilerinin yaygınlaşması ile otomatik karar alma sistemleri de giderek daha fazla sayıda iş süreçlerinde kullanılmakta, bu durum insan müdahalesinin gerekliliğini daha da önemli hâle getirmektedir. Otomatik karar alma, genel olarak insan müdahalesi olmaksızın teknolojik araçlarla karar verme yeteneği olarak tanımlanabilir[846]. Ancak, özellikle bireylerin hak ve özgürlükleri üzerinde önemli etkileri olabilecek kararlarda, insan müdahalesinin varlığı kritik bir güvence mekanizması olarak görülmektedir. Teknolojiden insana yakışır iş anlayışı doğrultusunda yararlanmak ve teknolojiyi etkin bir şekilde yönetmek, çalışanlar ve yöneticilerin işin tasarımını birlikte müzakere etmesini gerektirmektedir. Aynı zamanda, yapay zekâ kullanımında, iş üzerinde etkili nihai kararların insanlar tarafından alınmasını sağlayan bir insan kontrolü yaklaşımının benimsenmesi önemlidir[847]. Uluslararası Çalışma Örgütü'nün Çalışmanın Geleceği Küresel Komisyonu'nun "Daha İyi Bir Gelecek İçin Çalışmak" başlıklı raporunda, teknolojinin insan onuruna uygun çalışma koşulları yaratmak amacıyla kullanılabilmesi için, insan kontrolüne dayalı bir yaklaşımın benimsenmesi gerektiği belirtilmektedir[848].

İnsan müdahalesinin temel gerekçeleri arasında yapay zekâ sistemlerinin doğasında var olan ve olası ön yargıları, ayrımcılığı, şeffaflık eksikliğini ve hesap verebilirlik sorunlarını ele almak yer almaktadır[849]. İnsan müdahalesi, insan değerlerini koruma,

---

[846] Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251rev.01), 6-8; Riikka Koulu, "Proceduralizing Control and Discretion: Human Oversight in Artificial Intelligence Policy", Maastricht Journal of European and Comparative Law 27, sy 6 (2020): 726.

[847] ILO, *Work for a brighter future–Global Commission on the Future of Work* (International Labour Office Geneva, 2019), 13, https://www.oitcinterfor.org/en/node/7468.

[848] Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 91.

[849] Ben Green, "The Flaws of Policies Requiring Human Oversight of Government Algorithms", *Computer Law & Security Review* 45 (Temmuz 2022): 2-7; Riikka Koulu, "Human Control Over Automation: Eu Policy and Ai Ethics", *EU Policy and AI Ethics* 12, sy 1 (2020): 10.

teknolojiye güveni artırma ve sistem doğruluğunu ve güvenliğini geliştirme gibi amaçlara hizmet etmektedir[850].

4.6.1.7.2. Anlamlı İnsan Müdahalesi Biçimleri (HITL, HOTL ve Diğer Modeller)

Öğretide, insan müdahalesinin farklı düzeylerini esas alan çeşitli biçimlere yer verilmektedir[851]. İnsanın sürece katılımı açısından üç temel tür öne çıkmaktadır. Bunlar, "döngü içinde insan" (human-in-the-loop -HITL), "döngü üzerinde insan" (human-on-the-loop), "döngü dışında insan" (human-out-of-the-loop) modelleri olarak anılmaktadır[852]

Döngü içinde insan modelinde, yapay zekâ veya algoritmik sistem bir karar önerir, ancak nihai kararı insan vermektedir. Karar alma sürecinin kontrolü insanda olup, yapay zekâ destekleyici bir rol oynamaktadır[853]. Tele çalışma bağlamında, bir algoritmanın bir çalışanın üretkenliğini düşük olarak işaretlemesi ve bu kararın insan bir yönetici tarafından onaylanması veya reddedilmesi döngü içinde insan modeline örneklik oluşturmaktadır. Bu yaklaşım, yapay zekânın insan üretkenliğini artırdığı, ancak insanın yerini almadığı bir nevi "geliştirme etkisi" olarak görülebilmektedir[854]. Avrupa Birliği Yapay Zekâ Yüksek Düzey Uzman Grubu (European Union High-Level Expert Group on Artificial Intelligence) da bu modeli, sistemin her karar döngüsünde insan müdahalesi yeteneği olarak tanımlamıştır[855].

Döngü üzerinde insan modelinde yapay zekâ sistemi kararı alır ve uygular, ancak bir insan aktör, karar yetkisini haiz bir otorite olarak her zaman müdahale etme ve kararı geçersiz kılma yetkisine sahiptir[856]. İnsanın karar alma sürecine katılımı minimum düzeydedir. Ancak yapay zekânın kararlarını denetleyebildiği ve uygunsuz gördüğü

---

[850] Andreas Holzinger vd., "Is Human Oversight to AI Systems Still Possible?", New Biotechnology 85 (Mart 2025): 59.
[851] Konuya temel kaynaklık oluşturan vekalet teorisine (agency theory) ilişkin ayrıntılı bilgi için bknz. Michael C Jensen, "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure", *Journal of Financial Economics* 3, sy 4 (2000): 58 vd.; Bart S Vanneste ve Phanish Puranam, "Artificial Intelligence, Trust, and Perceptions of Agency", *Academy of Management Review,* 2024, 1976 vd.
[852] Stanislav Hristov Ivanov, "Automated Decision-Making", *Foresight* 25, sy 1 (2023): 4-19, https://doi.org/10.1108/FS-09-2021-0183.
[853] Ivanov, "Automated Decision-Making", 7.
[854] Ivanov, "Automated Decision-Making", 9.
[855] Koulu, "Human Control Over Automation: Eu Policy and Ai Ethics", 32.
[856] Ivanov, "Automated Decision-Making", 7.

kararları geçersiz kılabildiği dolayısıyla nihai karar yetkisini elinde bulundurduğu için kararın sonuçlarından sorumludur[857]. Sözü geçen model, sistemin tasarım döngüsü sırasında insan müdahalesi öngörülmesini ve sistemin işleyişinin insan gözetimine açık şekilde yapılandırılmasını ifade etmektedir[858].

Döngü dışında insan modelinde ise yapay zekâ sistemi insan müdahalesi olmaksızın özerk kararlar almakta ve uygulamaktadır. Bu durum, ciddi sorunlar yaratır çünkü işverenin yapay zekâ sistemlerinin kararları ve uygulamaları üzerinde hiçbir kontrolü yoktur[859]. Bu modelde sorumluluk, genellikle süreci tasarlayan, yazılımı geliştiren ve teknik desteği sağlayan insan çalışanlar arasında paylaştırılır[860]. Bu modelin kullanımı özellikle GDPR gibi düzenlemeler kapsamında, bireyler üzerinde yasal veya benzeri önemli etkileri olan kararlar için genellikle kısıtlanmaktadır.

Anlatılan bu modeller ışığında, iş süreçlerinde yapay zekâdan en doğru şekilde faydalanmak için genellikle en etkili yol, makine ve insan yeteneklerini birleştiren dengeli bir yaklaşım benimsemektir. Özellikle Döngü İçinde İnsan (HITL) ve Döngü Üzerinde İnsan (HOTL) modellerinin bir karması olarak görülebilecek bu yaklaşımda, her iki taraf da en güçlü olduğu alana odaklanır. Örneğin, bir işe alım sürecinde yapay zekâ sistemi bir adayın deneyim süresi gibi nicel verileri objektif olarak analiz ederken, bir işe alım uzmanı adayın liderlik potansiyeli veya yaratıcılığı gibi nitel ve formlarda yer almayan yetkinliklerini değerlendirebilir. Bu iş birliği, hem otomasyonun potansiyel sistemik ön yargılarına hem de insanın bilinçdışı eğilimlerine karşı güçlü bir denetim mekanizması kurarak daha adil ve isabetli kararlar alınmasını sağlar[861].

4.6.1.7.3. Anlamlı İnsan Müdahalesinin Uygulanabilirliği

Anlamlı insan müdahalesi, otomatik karar verme süreçlerinde etkili bir güvence sağlamak için merkezi bir önem taşır ve yalnızca biçimsel veya sembolik bir onaylama mekanizmasından ibaret olmamalıdır. Bu müdahalenin gerçek anlamda etkili

[857] Ivanov, "Automated Decision-Making", 7.
[858] Koulu, "Human Control Over Automation: Eu Policy and Ai Ethics", 32.
[859] Ivanov, "Automated Decision-Making", 7.
[860] Ivanov, "Automated Decision-Making", 7-8.
[861] Fernández, "Big Data as a Tool to Enhance Recruitment Processes", 100.

olabilmesi için, çeşitli kriterlerin sağlanması gerekmektedir[862]. Avrupa Birliği'nin Madde 29 Veri Koruma Çalışma Grubu ve konuya ilişkin öğretideki yaklaşımlar tarafından belirlenen ilkelerle insan müdahalesinin niteliği ortaya konulmaktadır[863]. Bu kapsamda, müdahaleyi gerçekleştiren bireyin, otomatik olarak verilen kararları değiştirme veya geri çevirme konusunda hukuki ve fiili yetkiye, ayrıca bu yetkiyi kullanabilecek düzeyde mesleki ve bilişsel yeterliliğe sahip olması zorunludur. Ayrıca, AB Yapay Zekâ Tüzüğü'nün 26. maddesinin 2. fıkrası uyarınca yüksek riskli yapay zekâ sistemleri bakımından dağıtıcıların (deployers), sistemlerin insan gözetimi altında kullanılmasını temin etmek üzere, gerekli yetkinlik, eğitim, yetki ve desteğe sahip personel görevlendirmeleri zorunludur[864]. Son olarak, bu kişinin karar alma süreçlerine ilişkin tüm girdilere ve çıktılara, algoritmanın kullandığı veri setleri ve karar üretim mantığı da dâhil olmak üzere, tam ve şeffaf biçimde erişimi olmalıdır[865].

Anlamlı insan müdahalesinin gerçekleştirilmesinde, müdahaleyi yapan kişiye değerlendirme yapması için gerekli olan uygun zamanın tanınması da önemlidir. Müdahalenin hızlı ve baskı altında gerçekleştirilmesi durumunda, müdahalenin niteliği ve sonuç üzerindeki etkisi önemli ölçüde azalabilir. Bununla birlikte, müdahaleyi gerçekleştirecek kişinin gerekli mesleki formasyon ve teknik bilgiye sahip olması ve bu yetkinliklerin sürekli olarak desteklenmesi şarttır[866]. Bu destek, yalnızca teknik altyapı ile sınırlı kalmamalı; organizasyonel ve kurumsal destek mekanizmalarını da içermelidir[867]. Olası hatalarda müdahale eden kişinin sorumluluğunun açıkça tanımlanmış olması, hukuki hesap verebilirliğin yanı sıra, müdahalenin ciddiyetini ve etkinliğini de güçlendirmektedir. Ayrıca, karar alma süreçlerinde kullanılan sistemlerin, insan müdahalesini kolaylaştıracak ve insan operatörün ihtiyaçlarına uyum sağlayacak şekilde tasarlanması kritik öneme sahiptir. Bu bağlamda sistemlerin, insan operatörü teknik sınırlamalara uyum sağlamak zorunda bırakmak yerine, operatörün karar verme süreçlerini etkin biçimde destekleyecek esneklikte

[862] Ben Wagner, "Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems", Policy & Internet 11, sy 1 (2019): 104, https://doi.org/10.1002/poi3.198.
[863] Wagner, "Liable, but Not in Control?", 113-15; Koulu, "Proceduralizing Control and Discretion", 726; Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251rev.01)*, 21.
[864] Voigt ve Hullen, *The EU AI Act*, 116.
[865] Adams-Prassl vd., "Regulating Algorithmic Management", 150.
[866] De Stefano ve Wouters, *AI and Digital Tools in Workplace Management and Evaluation*, n. 54.
[867] Fernández, "Big Data as a Tool to Enhance Recruitment Processes", 100.

yapılandırılması gerekmektedir[868]. "Ölü adam kolu" olarak adlandırılan yaklaşıma dayalı sistemlerin tasarımından kaçınılmalı; bunun yerine algoritmanın herhangi bir anda bir insan operatör tarafından geçersiz kılınabilmesi için her zaman bir seçenek sunulmalıdır[869]. Bu durumda devreye "algoritmik geri çekilme" (algorithmic resignation) kavramı girmektedir. Algoritmik geri çekilme, yapay zekânın performans değerlendirmesi gibi kritik süreçlerde her zaman güvenilir olmayabileceğini ve belirli durumlarda bu sistemlerin stratejik olarak devre dışı bırakılmasının gerekliliğini vurgulamaktadır[870]. Bu yaklaşım, özellikle belirsiz verilerle karşılaşıldığında, yapay zekânın yanlış ya da yanıltıcı sonuçlar üretebileceği ve dolayısıyla kullanımının sınırlandırılması gerektiğini savunmaktadır[871]. Örneğin, düşük performans gösterdiği varsayılan çalışanların yanlış bir şekilde tespiti gibi riskler nedeniyle, işverenlerin yapay zekâ sistemlerine aşırı güvenmemesi önerilmektedir. Algoritmik geri çekilme, denetim mekanizmalarına entegre edildiğinde, işverenlerin ne zaman ve nasıl insan yargısını sürece dâhil etmeleri gerektiği konusunda rehberlik sağlamaktadır[872]. Bu strateji, yapay zekânın objektif değerlendirme ve verimlilik avantajlarını kullanırken, insani faktörleri ve yasal sorumlulukları dikkate alan bir koruma katmanı sunmaktadır. Böylece, organizasyonlar, performans değerlendirmelerinde yapay zekâ kullanımıyla ilgili sınırları belirleyerek hem ekonomik hem de etik açıdan dengeli kararlar alabilmektedir[873].

Son olarak, anlamlı müdahalenin bir diğer temel unsuru olan eylemlilik, müdahale eden kişinin kararları değiştirme yönündeki iradesini etkin biçimde kullanabilme kapasitesiyle ilgilidir. Bu, yalnızca teorik bir yetkinlik değil, aynı zamanda pratikte de düzenli olarak uygulanabilen bir yetki ve inisiyatif alanı olarak kurgulanmalıdır[874].

---

[868] Voigt ve Hullen, *The EU AI Act*, 87.

[869] "Ölü adam kolu" (dead man's lever) yaklaşımı, sistemin yalnızca insan operatörün kontrolü kaybetmesi veya devre dışı kalması halinde devreden çıkmasına imkân tanıyan bir güvenlik mekanizmasıdır. Ancak yapay zekâ destekli karar sistemlerinde bu yaklaşım yeterli bulunmamaktadır. Bu bağlamda, algoritmanın kararlarının her aşamada bir insan operatör tarafından geçersiz kılınabilmesini mümkün kılacak sürekli ve esnek bir denetim mekanizmasının tesis edilmesi, insan odaklı bir kontrolün sağlanması bakımından önem arz etmektedir. Ayrıntılar için bknz. Fernández, "Big Data as a Tool to Enhance Recruitment Processes", 100.

[870] Umang Bhatt ve Holli Sargeant, "When Should Algorithms Resign? A Proposal for AI Governance", arXiv:2402.18326, preprint, arXiv, 16 Temmuz 2024, 1, https://doi.org/10.48550/arXiv.2402.18326.

[871] Bhatt ve Sargeant, "When Should Algorithms Resign?", 1-2.

[872] Bhatt ve Sargeant, "When Should Algorithms Resign?", 2.

[873] Ayrıntılı bilgiler için bkz. Bhatt ve Sargeant, "When Should Algorithms Resign?"

[874] Adams-Prassl vd., "Regulating Algorithmic Management", 143 vd.; *The Impact of AI on the Workplace: Main Findings from the OECD AI Surveys of Employers and Workers*, OECD Social,

Tüm bu bileşenlerin bir arada ele alınmasıyla, otomatik karar alma süreçlerinde insan müdahalesinin anlamlı, etkin ve güvence sağlayıcı olması mümkün olmaktadır.

4.6.1.7.4. İnsan Müdahalesinin Sınırlılıkları ve Zorlukları (Otomasyon Ön Yargısı ve Kara Kutu Problemi)

İnsan müdahalesi kavramı, teorik olarak algoritmik sistemlerin denetlenmesi ve ortaya çıkabilecek risklerin önlenmesi açısından idealize edilmekle birlikte, uygulamada çeşitli kısıtlamalar ve önemli zorluklarla karşılaşmaktadır. Ampirik çalışmalar, insanların karmaşık algoritmik süreçleri etkili ve sürekli biçimde denetleyebilme kapasitesinin beklenildiği kadar yüksek olmadığını ortaya koymaktadır[875]. Bu sınırlılıklar, öncelikle insanların otomatik sistemlere yönelik aşırı güven eğilimini ifade eden otomasyon ön yargısı (automation bias) ile açıklanmaktadır. Otomasyon ön yargısı, kullanıcıların sistemden gelen önerileri yeterince sorgulamadan kabul etme eğilimidir[876]. Bu durum, iki tür hataya yol açabilmektedir: Sistem bir uyarı vermediği için gerekli bir eylemin atlanması veya sistemin önerdiği hatalı bir tavsiyeye uyularak yanlış bir eylemde bulunulması[877]. Bir yöneticinin, günde yüzlerce tele çalışanın aktivite raporunu üreten bir sisteme aşırı güvenmesi ve sistemin "normal" olarak işaretlediği, aslında sorunlu olan bir durumu gözden kaçırması (ihmal hatası), bu riskin somut bir yansımasıdır.

Bununla birlikte, otomasyona aşırı bağımlılığın bir sonucu olarak, insan operatörlerin becerilerinde zamanla gerileme ya da "beceri körelmesi" yaşanmakta ve sürekli sistem uyarılarına maruz kalma nedeniyle "uyarı yorgunluğu" (alert fatigue) ortaya çıkmaktadır. Bu durum, operatörlerin zaman içinde uyarılara karşı hassasiyetlerinin

Employment and Migration Working Papers no. 288, OECD Social, Employment and Migration Working Papers (2023), 288:5, https://doi.org/10.1787/ea0a0fe1-en.

[875] Green, "The Flaws of Policies Requiring Human Oversight of Government Algorithms", 7.

[876] Green, "The Flaws of Policies Requiring Human Oversight of Government Algorithms", 7; David Lyell ve Enrico Coiera, "Automation bias and verification complexity: a systematic review", *Journal of the American Medical Informatics Association* 24, sy 2 (2017): 423-31; Linda J. Skitka vd., "Does automation bias decision-making?", *International Journal of Human-Computer Studies* 51, sy 5 (1999): 991-1006, https://doi.org/10.1006/ijhc.1999.0252.

[877] Green, "The Flaws of Policies Requiring Human Oversight of Government Algorithms", 7.

azalmasına ve gerekli önleyici müdahaleleri yapma kapasitelerinin düşmesine neden olmaktadır[878].

Diğer bir önemli sınırlılık ise algoritmik sistemlerin açıklanabilirlik sorunlarıyla ilgili bulunmaktadır. Özellikle karmaşık yapay zekâ sistemlerinin karar mekanizmalarını tam olarak anlamak ve belirli bir sonuca nasıl ulaştığını açıklamak, insan denetçiler açısından önemli bir güçlük arz etmektedir[879]. Bu durum, öğretide yaygın olarak "kara kutu" (black-box) etkisi şeklinde tanımlanmaktadır[880]. Sistemin karar süreçlerine ilişkin şeffaflık eksikliği, insan müdahalesinin anlamlılığını zayıflatmakta ve denetim süreçlerinin kalitesini düşürmektedir[881].

Anılması gereken bir diğer husus ise "ahlaki tampon bölgeler" (moral crumple zones) sorunudur. Bu kavram, insan operatörlerin aslında kontrol düzeyi çok sınırlı olan otomatik sistemlerin hata ve eksikliklerinden sorumlu tutulmaları riskini ifade etmektedir[882]. Bazı durumlarda, sırf yasal zorunlulukları yerine getirmiş gibi görünmek için sistemlere göstermelik bir insan müdahalesi eklenebilir. Böylece amaç, sistemin gerçekten bir insan tarafından denetlendiği izlenimini yaratmak olsa da bu müdahale aslında yalnızca kâğıt üzerinde bir formaliteyi tamamlamaktan ibaret kalmaktadır[883].

İnsan müdahalesinin etkinliğini sorgulatan bir diğer önemli sınırlılık ise algoritmik sistemlerin açıklanabilirlik sorunları karşısında insan müdahalesini gerçekleştirecek kişinin niteliğine ilişkin belirsizliklerdir. Örneğin, makine öğrenimi veya yapay zekâ bağlamında, bu müdahaleyi yapacak "insanın" kim olması gerektiği ve bu kişinin üçüncü taraf algoritmaları, önceden öğrenilmiş modeller veya diğer bireylerin kişisel verilerini içeren karmaşık veri setlerine dayalı bir süreci ya da "kara kutu" olarak

---

[878] Green, "The Flaws of Policies Requiring Human Oversight of Government Algorithms", 7; Holzinger vd., "Is Human Oversight to AI Systems Still Possible?", 60.
[879] Green, "The Flaws of Policies Requiring Human Oversight of Government Algorithms", 8.
[880] Kara kutu sorunu ve bununla bağlantılı olarak işverenin açıklama yükümlülüğü hakkında ayrıntılı bilgi için bknz. 4.4.9.2. Bölüm
[881] Koulu, "Proceduralizing Control and Discretion", 727.
[882] Koulu, "Proceduralizing Control and Discretion", 720; Madeleine Clare Elish, "Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction", *Engaging Science, Technology, and Society* 5 (Mart 2019): 40.
[883] Wagner, "Liable, but Not in Control?", 113; Green, "The Flaws of Policies Requiring Human Oversight of Government Algorithms", 7.

nitelenen şeffaf olmayan makine öğrenimi modellerini ne ölçüde inceleyebileceği belirsizliğini korumaktadır. Ayrıca, kararı gözden geçirecek kişinin, ilk kararı veren kişi olup olamayacağı ve bu kişinin veri sahibi hakkında önceki bilinçli ya da bilinçdışı ön yargılar ve taraflılıklardan etkilenip etkilenmeyeceği de net değildir. Bu durum, insan müdahalesinin kendisinin de yeni bir hata ve yanlılık kaynağı olabileceği riskini ortaya koyarak, müdahalenin beklenen güvenceyi sağlama kapasitesini önemli ölçüde sınırlamaktadır[884].

Son olarak, modern yapay zekâ sistemlerinin artan karmaşıklığı, büyük ölçeği ve özerklik seviyeleri de insan müdahalesini güçleştiren temel faktörlerdendir. Bu durum, insan müdahalesinin gerçek anlamda etkili ve sürekli olmasını ciddi biçimde engellemekte ve müdahalenin beklenen güvenceleri sağlayabilmesini önemli ölçüde sınırlamaktadır[885]. Tüm bu nedenlerle, anlamlı insan müdahalesinin sağlanması amacıyla, bahsedilen sorunların sistematik olarak ele alınması ve gerekli iyileştirmelerin yapılması kritik önem taşımaktadır.

4.6.1.7.5. Avrupa Birliği Düzenlemelerinde Anlamlı İnsan Müdahalesi

Avrupa Birliği, yapay zekâya yönelik "insan merkezli" ve "güvenilir" bir yaklaşım benimsemiştir ve insan müdahalesi bu yaklaşımın temel bir unsuru olarak kabul edilmektedir[886]. AB Yapay Zekâ Tüzüğü, özellikle yüksek riskli YZ sistemleri için insan müdahalesini zorunlu kılmaktadır. AI Act 14. madde, insan müdahalesinin, yapay zekâ sisteminin kullanımı sırasında ortaya çıkabilecek sağlık, güvenlik veya temel haklara yönelik riskleri önlemeyi veya en aza indirmeyi amaçladığını belirtir[887]. Bu madde ayrıca, denetçilerin sistemin kapasite ve sınırlamalarını anlamasını, otomasyon ön yargısının farkında olmasını ve sistemi durdurma veya müdahale etme yeteneğine sahip olmasını sağlayacak önlemleri detaylandırmaktadır[888]. Benzer

[884] Aloisi ve Gramano, "Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context", 107-8.
[885] Holzinger vd., "Is Human Oversight to AI Systems Still Possible?", 59.
[886] Koulu, "Proceduralizing Control and Discretion", 721-27.
[887] Hanne Hirvonen ve Frida Alizadeh Westerling, "Beyond Human Oversight—Quality Management as a Tool to Control Automated Decision-Making Systems", içinde *De Gruyter Handbook of Automated Futures: Imaginaries, Interactions and Impact*, 2. bs (Walter de Gruyter, 2024), 6.
[888] Hirvonen ve Westerling, "Beyond Human Oversight—Quality Management as a Tool to Control Automated Decision-Making Systems", 6.

şekilde, AB Komisyonu'nun Beyaz Kitabı (2020) ve Avrupa Parlamentosu'nun 2019 tarihli kararı da insan müdahalesi, karar alma ilkeleri ve şeffaflık konularına vurgu yapmaktadır[889].

Bu kapsamda karar alma süreçlerinde güvenliği ve denetimi sağlamak için insan-makine ara yüzünün oluşturulması önemlidir[890]. Söz konusu yapı sayesinde yapay zekâ sistemleri sürekli izlenmekte, düzenli geri bildirimlerle güncellenmekte ve olası hatalar erken tespit edilerek müdahale edilebilmektedir. Özellikle, doğrudan verilerle çalışan, şeffaf ve hesap verebilir algoritmalar, sistemin güvenilirliğini artırmaktadır[891].

4.6.1.7.6. İnsan Müdahalesinin Ötesi: Kalite Yönetimi ve Süreç Gözden Geçirilebilirliği

İnsan müdahalesinin sınırlılıkları göz önüne alındığında, tek başına yeterli bir güvence olmadığı ve tamamlayıcı veya alternatif yaklaşımlara ihtiyaç duyulduğu açıktır[892]. AI Act, 17. maddesinde, yapay zekâ sistemlerinin geliştirilmesi, test edilmesi ve doğrulanması için kapsamlı prosedürler sunan kalite yönetim sistemlerinin kurulmasını zorunlu kılmaktadır. Bu yaklaşım, insan denetimini daha sistematik ve izlenebilir bir çerçeveye oturtarak denetimin etkinliğini artırmayı amaçlamaktadır.

Kalite yönetim sistemleri daha çok sistemin tasarım aşamasına odaklanırken, bir de sistemin işleyişi sırasında şeffaflığı temel alan farklı bir bakış açısı bulunmaktadır. Alternatif bir yaklaşım ise, tekil kararlara anlık açıklamalar sunmak yerine, tüm otomatik karar alma sürecinin bütüncül olarak gözden geçirilebilirliğini (reviewability) sağlamayı hedeflemektedir. Başka bir deyişle bu yaklaşım, sistemin attığı her adımın ve aldığı her kararın kayıt tutma ve günlükleme (logging) gibi mekanizmalarla kalıcı bir dijital iz bırakmasını sağlamaktadır. Böylece, sadece

---

[889] Ida Skubis ve Krzysztof Wodarski, "HUMANOID ROBOTS IN MANAGERIAL POSITIONS – DECISION-MAKING PROCESS AND HUMAN OVERSIGHT", *Scientific Papers of Silesian University of Technology. Organization and Management Series* 2023, sy 189 (2023): 589-91, https://doi.org/10.29119/1641-3466.2023.189.36.
[890] Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 89.
[891] Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", n. 199.
[892] Hirvonen ve Westerling, "Beyond Human Oversight—Quality Management as a Tool to Control Automated Decision-Making Systems", 8.

algoritmanın teknik işleyişi değil, insan faktörünü de içeren tüm sosyo-teknik süreç, geriye dönük olarak denetlenebilir ve sorgulanabilir hâle gelmektedir[893].

Sonuç olarak, otomatik karar alma süreçlerinde insan müdahalesi, kişisel verilerin korunması ve temel hakların güvence altına alınması açısından hayati bir idari tedbirdir. Ancak bu müdahalenin anlamlı olması ve pratikteki sınırlılıklarının farkında olunması gerekmektedir. Yalnızca sembolik bir insan varlığı yerine, yetkin, yetkili ve gerekli bilgiye sahip bireyler tarafından gerçekleştirilen etkin bir denetim hedeflenmelidir. İnsan müdahalesinin etkinliği, otomasyon ön yargısı ve karmaşık sistemleri anlama zorluğu gibi engellerle sınırlıdır. Bu nedenle, insan denetimini destekleyici ve tamamlayıcı mekanizmalar olarak kalite yönetim sistemleri ve süreçlerin bütüncül gözden geçirilebilirliği gibi yaklaşımların da benimsenmesi, tele çalışma ortamlarında kişisel verilerin korunması ve adil süreçlerin sağlanması için kritik öneme sahiptir. Yapay zekâ düzenlemeleri geliştikçe, insan müdahalesinin rolü ve uygulama biçimleri de sürekli olarak değerlendirilmeli ve iyileştirilmelidir.

4.6.1.8. Takma Adlandırma ve Anonimleştirme

Kişisel verilerin işlenmesinde mahremiyet risklerini azaltmaya yönelik başlıca teknik tedbirlerden ikisi takma adlandırma (pseudonymisation) ve anonimleştirmedir. Her iki yöntem de kişisel verilerin doğrudan bir gerçek kişiyle ilişkilendirilme olasılığını düşürerek veri koruma düzeyini artırmayı hedeflerken[894] aralarında hukuki sonuçları ve uygulama biçimleri açısından bazı temel farklar bulunmaktadır. Kişisel verilerin, kimliği belirli veya belirlenebilir bir kişiyle ilişkilendirilmesini zorlaştıracak şekilde işlenmesi, veri güvenliğini artıran ve özellikle veri ihlallerinin olası olumsuz etkilerini azaltma potansiyeli taşıyan bir yaklaşımdır[895]. Bu yöntemlerin tele çalışma modelinde toplanan izleme verilerine uygulanması hem yasal uyumluluğa katkı sağlar hem de

[893] Jennifer Cobbe ve Jatinder Singh, "Reviewable Automated Decision-Making", *Computer Law & Security Review* 39 (Kasım 2020): 1, https://doi.org/10.1016/j.clsr.2020.105475.
[894] Samson Esayas, "The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing'approach", *European Journal of Law and Technology* 6, sy 2 (2015): 4, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746831.
[895] Mike Hintze ve Khaled El Emam, "Comparing the benefits of pseudonymisation and anonymisation under the GDPR", *Journal of Data Protection & Privacy* 2, sy 2 (2018): 157.

çalışanların mahremiyet beklentilerine daha fazla saygı gösterilmesine olanak tanımaktadır.

Anonimleştirmeden farklı olarak, takma adlandırma KVKK'da açıkça tanımlanmamıştır. Lakin bu kavram, Avrupa Birliği'nin temel veri koruma düzenlemesi olan GDPR'da bir güvence mekanizması olarak detaylıca ele alınmıştır. GDPR'ın 4. maddesinin 5. fıkrasında *"kişisel verilerin, ek bilgiler kullanılmaksızın belirli bir veri sahibiyle artık ilişkilendirilemeyecek şekilde işlenmesidir; şu kadar ki, bu tür ek bilgiler ayrı tutulur ve kişisel verilerin tanımlanmış veya tanımlanabilir bir gerçek kişiye atfedilmemesini sağlamak için teknik ve organizasyonel önlemlere tabi tutulur"* şeklinde tanımlanmıştır[896]. Takma adlandırılmış veriler, ek bilgi (örneğin, bir eşleştirme anahtarı) ile birleştirildiğinde ilgili kişi yeniden tanımlanabileceği için hukuken kişisel veri niteliğini korumaya devam eder ve GDPR ile KVKK kapsamındaki veri koruma ilkelerine tabidir[897]. GDPR, takma adlandırmayı önemli bir güvenlik tedbiri ve gizliliğin tasarım aşamasından itibaren gözetilmesi ve başlangıçtan itibaren gizliliği esas alan yapılandırma ilkesinin bir unsuru olarak teşvik etmektedir[898]. Takma adlaştırmanın veri minimizasyonu ilkesinin uygulanmasında da bir araç olabileceği belirtilmektedir[899]. Tele çalışmada izleme bağlamında, çalışanların performans verileri veya aktivite logları takma adlandırılarak genel eğilimlerin analizi, sistem iyileştirmeleri veya belirli bir sorun hakkında genel çıkarımlar yapılması gibi amaçlarla kullanılabilirken, bireysel müdahale veya değerlendirme gerektiren durumlarda (meşru bir amaç ve hukuki dayanak varlığında) ek bilgi kullanılarak veriler tekrar ilgili kişiye atfedilebilmektedir[900]. Takma adlandırma, doğası gereği

---

[896] Hintze ve El Emam, "Comparing the benefits of pseudonymisation and anonymisation under the GDPR", 146; Zhicheng He, "From Privacy-Enhancing to Health Data Utilisation: The Traces of Anonymisation and Pseudonymisation in EU Data Protection Law", Digital Society 2, sy 2 (2023): 6; Richard Rak, "Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS)", European Journal of Risk Regulation 15, sy 4 (2024): 932-33.

[897] Hintze ve El Emam, "Comparing the benefits of pseudonymisation and anonymisation under the GDPR", 147; Esayas, "The role of anonymisation and pseudonymisation under the EU data privacy rules", 8.

[898] Emanuele Raso vd., "Anonymization and Pseudonymization of FHIR Resources for Secondary Use of Healthcare Data", *IEEE Access* 12 (2024): 44930, https://doi.org/10.1109/ACCESS.2024.3381034; Hintze ve El Emam, "Comparing the benefits of pseudonymisation and anonymisation under the GDPR", 154.

[899] Rak, "Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS)", 932.

[900] Aloisi ve Gramano, "Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context", 103.

hukuki ve teknik ekiplerin yakın çalışmasını gerektiren bir yöntemdir. Bu iş birliği sayesinde, verilerin yeniden kimliklendirilmesine yönelik kurallar ve prosedürler hem yasal gerekliliklere uygun hem de teknik olarak daha etkin bir şekilde hayata geçirilebilecektir[901].

Anonimleştirme ise KVKK'nın 3. maddesinin 1. fıkrasının (b) bendinde *"kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi"* olarak tanımlanmıştır. Benzer şekilde GDPR, başlangıç bölümünün 26. maddesinde, veri koruma ilkelerinin "kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkili olmayan" veya "veri sahibinin artık tanımlanamayacağı şekilde anonim hâle getirilmiş kişisel verilere" uygulanmaması gerektiğini belirtmektedir[902]. Dolayısıyla, veriler geri döndürülemez bir şekilde anonim hâle getirildiğinde artık kişisel veri olarak kabul edilmeyecektir. Bu durumda da KVKK ile GDPR'ın getirdiği yükümlülükler büyük ölçüde ortadan kalkmaktadır[903]. Böylece anonimleştirilmiş verilerin istatistiksel analiz, araştırma, kamuoyuyla paylaşılacak genel raporlar veya uzun vadeli eğilim analizleri gibi daha geniş amaçlar için kullanılması mümkün hâle gelmektedir. Tele çalışmaya ilişkin izleme verileri, işlenme amaçları ortadan kalktıktan sonra anonimleştirilerek gelecekteki analizler için saklanabilir. Zira tam anonimleştirme, silme işleminin işlevsel eşdeğeri olarak kabul edilebilir ve bu tür veriler süresiz olarak saklanabilmektedir[904]. Ancak, gerçek anlamda ve geri döndürülemez bir anonimleştirme sağlamak teknik olarak zorlayıcı olabilmekte[905] ve yetersiz anonimleştirme sonucunda verilerin yeniden kimliklendirilmesi riski doğmaktadır[906]. Gerçek bir anonimleştirme sağlamanın teknik zorlukları, beraberinde önemli hukuki riskler getirmektedir. Yetersiz veya hatalı anonimleştirilmiş veriler, başka veri

---

[901] Raso vd., "Anonymization and Pseudonymization of FHIR Resources for Secondary Use of Healthcare Data", 44929.
[902] He, "From Privacy-Enhancing to Health Data Utilisation", 6; Raso vd., "Anonymization and Pseudonymization of FHIR Resources for Secondary Use of Healthcare Data", 44930.
[903] Hintze ve El Emam, "Comparing the benefits of pseudonymisation and anonymisation under the GDPR", 147.
[904] Hintze ve El Emam, "Comparing the benefits of pseudonymisation and anonymisation under the GDPR", 155.
[905] Esayas, "The role of anonymisation and pseudonymisation under the EU data privacy rules", 6.
[906] Raso vd., "Anonymization and Pseudonymization of FHIR Resources for Secondary Use of Healthcare Data", 44930; He, "From Privacy-Enhancing to Health Data Utilisation", 3; Rak, "Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS)", 933.

setleriyle birleştirilerek yeniden kimliklendirilebilir hâle gelebilmektedir (re-identification). Bu durumda veriler tekrar kişisel veri sayılacağı için, veri sorumlusu hukuka aykırı veri işleme durumuyla karşı karşıya kalmaktadır. Bu riskleri azaltmak amacıyla verileri daha genel hâle getiren veya bazı detayları gizleyen çeşitli anonimleştirme teknikleri mevcuttur.[907]. Bu nedenle, yeniden kimliklendirme riskinin dikkatle değerlendirilmesi, her anonimleştirme sürecinin en kritik adımlarından biridir[908]

Hukuki uyumluluğu sağlamak adına, takma adlandırma ve anonimleştirme arasındaki temel farkın kavranması zorunluluk arz etmekte; zira takma adlandırma veri güvenliğini artıran ancak verinin kişisel veri niteliğini ortadan kaldırmayan bir önlemken, anonimleştirme doğru uygulandığında veriyi kişisel veri koruması kapsamından tamamen çıkarmaktadır. Bu kavramsal ayrım, özellikle işverenlerin tele çalışma modelinden elde ettikleri izleme verilerini yönetirken, veri minimizasyonu ve amaçla sınırlılık ilkeleri doğrultusunda kritik bir rol oynamaktadır. Bu çerçevede, işleme faaliyetinin gerekliliklerine göre, bireysel kimlik tespiti gerektirmeyen genel performans analizleri için takma adlandırmanın tercih edilmesi, verinin işlendiği asıl amaç sona erdiğinde ve uzun vadeli istatistiksel analiz gibi meşru bir sebeple saklanması gerektiğinde ise anonimleştirme yöntemine başvurulması gerekmektedir. Dolayısıyla, bu ilkeler ışığında hareket etmek, işverenin hem yasal veri koruma yükümlülüklerini eksiksiz yerine getirmesini hem de çalışan mahremiyetini etkin bir şekilde güvence altına almasını sağlayan temel bir stratejiyi oluşturmaktadır[909].

2000'li yılların başında kişisel verilerin korunmasında güvenilir ve etkili bir yöntem olarak kabul edilen anonimleştirme, zamanla bu itibarını sorgulatan bulgularla karşı karşıya kalmıştır. Nitekim sonraki dönemde yapılan araştırmalar, teoride geri döndürülemez olduğu varsayılan anonimleştirilmiş veri setlerinin dahi yeniden

[907] Ayrıntılı bilgi için bknz. He, "From Privacy-Enhancing to Health Data Utilisation", 2; Hintze ve El Emam, "Comparing the benefits of pseudonymisation and anonymisation under the GDPR", 148.
[908] Hintze ve El Emam, "Comparing the benefits of pseudonymisation and anonymisation under the GDPR", 148.
[909] Rak, "Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS)", 928.

kimliklendirilme (re-identification) riski taşıdığını ortaya koymuştur[910]. Bu durum, her anonimleştirme tekniğinin kategorik olarak yetersiz olduğu anlamına gelmese de bu yöntemin tek başına mutlak bir mahremiyet güvencesi sağlayamayacağını kanıtlamıştır. Sonuç olarak, yeniden kimliklendirme riskinin ciddiyeti, anonimleştirme kavramının hukuki ve etik çerçevede yeniden değerlendirilmesini ve bu tekniğe dayalı veri koruma stratejilerinin güncellenmesini zorunlu kılmıştır[911].

Yeniden kimliklendirme yöntemlerinin kolaylaşması, anonimleştirmenin mahremiyet korumasındaki etkinliğine yönelik geleneksel varsayımları köklü biçimde değiştirmiştir. Bu gelişmeler, bireylerin kişisel bilgilerinin korunması için daha kapsamlı ve sürdürülebilir düzenlemelere ihtiyaç olduğunu göstermekte, mevcut hukuki ve etik yaklaşımları yeniden değerlendirme zorunluluğunu ortaya koymaktadır[912]. Tıpkı suç mahallindeki parmak izinin tek bir bireyi benzersiz tanımlaması gibi, veri kombinasyonları da kişilerin "veri parmak izlerini" oluşturmakta ve anonimleştirme yöntemlerinin yetersizliğini ortaya çıkarmaktadır[913]. Günümüzde teknolojik gelişmelerle birlikte, anonimleştirme yöntemlerinin ciddi riskler barındırdığı ve yeniden kimliklendirme olasılığının yüksek olduğu dikkate alınmalıdır. Anonimleştirme her ne kadar tanımı gereği verilerin tekrar kimliklendirilemeyecek şekilde işlenmesini ifade etse de uygulamada bu güvencenin tam anlamıyla sağlanması çoğu zaman mümkün olamamaktadır. Bu nedenle, iş ilişkisi kapsamında anonimleştirme yönteminin bir güvence aracı olarak kullanılmasının uygun olmayacağı kanaatindeyiz.

---

[910] Yeniden kimliklendirme ile ilgili ayrıntılı bilgi için bkz. Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", *UCLA Law Review* 57, sy 6 (2010 2009): 1776-77.

[911] Yeniden kimliklendirme riskinin yalnızca teorik bir olasılık olmadığı, ampirik çalışmalarla defalarca kanıtlanmıştır. Bu alandaki öncü çalışmalar, basit tanımlayıcıların kaldırılmasının veriyi güvenli kılmaya yetmediğini göstermektedir. Örneğin, kişilerin posta kodu, doğum tarihi ve cinsiyet gibi dolaylı tanımlayıcılarının kamuya açık seçmen kütükleri gibi başka veri setleriyle birleştirilmesi yoluyla, "anonimleştirilmiş" sağlık kayıtlarına dahi ulaşılabildiği ortaya konmuştur. Benzer şekilde, kullanıcıların film değerlendirmeleri veya internet arama geçmişleri gibi davranışsal verilerinin, kendilerine özgü bir "veri parmak izi" oluşturduğu ve bu izler takip edilerek kimliklerinin kolayca ifşa edilebildiği tespit edilmiştir. Bu ve benzeri vakalar, anonimleştirme kavramına yönelik ilk iyimser yaklaşımları kökünden sarsmış ve veri koruma hukukunda daha sofistike teknik ve hukuki güvencelere olan ihtiyacı net bir şekilde gözler önüne sermiştir. Bu konudaki örnekler için bknz. Ohm, "Broken Promises of Privacy", 1716-20.

[912] Ohm, "Broken Promises of Privacy", 1776-77.

[913] Ohm, "Broken Promises of Privacy", 1723.

4.6.1.9. Verilerin Silinmesi ve Yok Edilmesi

Kişisel verilerin işlenmesini gerekli kılan amaçların sona ermesi, ilgili kişinin geçerli bir silme talebinde bulunması veya verilerin silinmesini gerektiren bir yasal yükümlülüğün ortaya çıkması durumunda, veri sorumlusu, söz konusu verileri gecikmeksizin silmek, yok etmek ya da anonimleştirmekle yükümlüdür. Bu yükümlülük, amaçla sınırlılık ve veri minimizasyonu ilkeleri uyarınca, verilerin artık işleme amacıyla orantılı biçimde saklanmasının mümkün ya da hukuken meşru olmaması nedeniyle yerine getirilmelidir. Zira bu durumda verilerin muhafazası, gereklilik ve ölçülülük ilkeleriyle bağdaşmayan bir veri işleme faaliyetine dönüşmekte ve veri koruma mevzuatına aykırılık teşkil etmektedir[914].

4.6.2. İdari Tedbirler

Tele çalışma süreçlerinde veri güvenliğini sağlamak ve hukuka uygunluğu temin etmek, yalnızca teknik önlemlerle mümkün değildir; bu önlemlerin kapsamlı idari tedbirlerle desteklenmesi zorunludur. Bu kapsamda alınabilecek temel idari tedbirler arasında; veri koruma bilincini artırmaya yönelik eğitimler düzenlenmesi, detaylı politikalar ve prosedürler oluşturulması, Veri Koruma Etki Değerlendirmesi gibi risk analizlerinin yapılması, otomatik karar süreçlerinde anlamlı insan müdahalesinin temin edilmesi, "Kendi Cihazını Getir" uygulamalarının yönetilmesi, üçüncü taraf veri işleyenlerle ilişkilerin düzenlenmesi, giyilebilir teknolojiler ile sosyal medya kullanımına ilişkin kuralların belirlenmesi ve sertifikasyon mekanizmalarından yararlanılması bulunmaktadır. Takip eden alt başlıklarda bu tedbirler ayrıntılı olarak incelenecektir.

4.6.2.1. Veri Koruma Bilinci Geliştirme ve Eğitim Faaliyetleri

Kişisel veri güvenliğinin sağlanmasında en önemli unsurlardan biri, teknik önlemlerin yanı sıra insan faktörünün de yönetilmesidir. Bu nedenle, veri sorumlusu olan işverenin en temel idari tedbirlerinden biri, tele çalışma süreçlerine dâhil olan tüm

[914] Konuya ilişkin teknik ve hukuki açıklamalara daha önce 4.4.8. Bölümde kapsamlı şekilde yer verildiğinden, bu bölümde ayrıca ayrıntılandırılmasına gerek görülmemiştir.

çalışanlar için kapsamlı ve düzenli veri koruma eğitimleri düzenlemektir. Tele çalışma modelinde çalışanlar, kurumun fiziksel güvenlik alanının dışında ve daha az kontrollü ağ ortamlarında faaliyet gösterdikleri için siber saldırılara ve veri ihlallerine karşı daha savunmasız hâle gelebilmektedirler. Bu riskler, çalışanların veri güvenliği konusundaki farkındalığını artırarak ve onlara gerekli bilgi ve becerileri kazandırarak en aza indirilebilmektedir. Bu eğitim faaliyetleri, yalnızca teorik bilgilerle sınırlı kalmamalı, aynı zamanda pratik uygulamaları da içermelidir. Eğitimlerin içeriğinde öncelikle kişisel veri, özel nitelikli kişisel veri gibi temel kavramlar, veri işlemenin hukuki dayanakları ve KVKK'dan doğan temel ilkeler yer almalıdır. Devamında, işverenin oluşturduğu veri güvenliği, cihaz kullanımı ve tele çalışma politikaları, güçlü parola oluşturma ve yönetimi, güvenli ağ kullanımı, oltalama (phishing) saldırılarını tanıma ve veri ihlali durumunda izlenmesi gereken prosedürler gibi somut konular işlenmelidir. Teknolojinin gelişmesiyle birlikte iş süreçlerinde kullanılan araçlar da karmaşıklaşmaktadır. Bu nedenle eğitimler, yapay zekâ tabanlı izleme ve algoritmik yönetim sistemleri gibi yeni nesil teknolojilerin yarattığı özel riskleri de kapsayacak şekilde güncellenmelidir. Özellikle bu sistemleri doğrudan kullanan veya çıktılarından yararlanan insan kaynakları personeli ve yöneticilere yönelik özel eğitimler düzenlenmelidir. Bu eğitimlerde, algoritmaların ayrımcı ön yargılar içerebilecek verilerle beslenmesi riski vurgulanmalı ve otomatik sistemlerin ürettiği sonuçları eleştirel bir süzgeçten geçirme, yorumlama ve denetleme konularında gerekli özen yükümlülüğünün nasıl yerine getirileceği öğretilmelidir[915].

4.6.2.2. Politikaların ve Prosedürlerin Oluşturulması

Tele çalışanların izlenmesinde sürecin hukuka uygun ve şeffaf bir şekilde yönetilebilmesi, işverenlerin bu konuda açık, kapsamlı ve erişilebilir kurumsal politikalar ile prosedürler oluşturmasını gerektirmektedir[916]. Bu politika ve prosedürler, hem işverenin yasal yükümlülüklerini yerine getirmesine yardımcı olur

[915] Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 87.

[916] KVKK, "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", 2018, 11, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf; S Prakash Somasundaram, "Enhancing Organizational Data Protection: Advanced Security Measures for Database Systems", *International Journal of Research in Computer Applications and Information Technology* 6, sy 1 (2023): 58; Dominik Huth ve Florian Matthes, "'Appropriate Technical and Organizational Measures': Identifying Privacy Engineering Approaches to Meet GDPR Requirements" (Twenty-fifth Americas Conference on Information Systems, Cancun, 2019), 1.

hem de çalışanların hakları ve beklentileri konusunda net bir çerçeve sunmaktadır[917]. İşverenlerin, kişisel verilerin korunmasına yönelik hukuka uygun bir yapı tesis etmek amacıyla öncelikle bir kişisel veri işleme politikası geliştirmesi ve bu politikayı düzenli olarak gözden geçirerek güncellemesi önem taşımaktadır[918]. Zira kişisel verilerin fiili korunması, yalnızca yasal düzenlemelere değil, aynı zamanda bu düzenlemelerin pratikte nasıl uygulandığına ve yorumlandığına da bağlıdır[919].

Tele çalışma ve çalışan izleme süreçleri için hazırlanacak politika ve prosedürler, KVKK ve GDPR'da yer alan uygun teknik ve idari tedbirlerin alınması önlemler gibi genel ilkelere dayanmalıdır. Bu genel ilkeler; şeffaf, işlevsel, sektöre özgü ve bağlama duyarlı somut kurallara dönüştürülerek hayata geçirilmelidir[920]. Bu politika ve prosedürlerin, veri koruma ilkelerini tasarım aşamasından itibaren süreçlere entegre edilmesi gerekmektedir[921].

Geliştirilecek politika ve prosedürlerin içermesi gereken bazı temel esaslar bulunmaktadır. Bu çerçevede izlemenin hangi meşru amaçlarla (örneğin, iş verimliliğinin ölçülmesi, veri güvenliğinin sağlanması, yasal yükümlülüklerin yerine getirilmesi) yapıldığı ve bu amaçların hangi hukuki işleme şartlarına dayandığı açıkça belirtilmelidir[922]. Ayrıca, hangi çalışanların, hangi aktivitelerinin (örneğin, e-posta, internet kullanımı, bilgisayar aktivitesi, kullanılan yazılımlar), hangi teknolojik araçlarla (yazılım, donanım), ne zaman (örneğin, sadece çalışma saatleri içinde mi) ve ne şekilde izleneceği detaylı bir biçimde tanımlanmalıdır[923]. Bunun yanında izleme ve

---

[917] Santiago Martín-Romo Romero ve Carmen De-Pablos-Heredero, "Data Protection by Design: Organizational Integration", Harvard Deusto Business Research 7, sy 2 (2018): 60; Christina Tikkinen-Piri vd., "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", Computer Law & Security Review 34, sy 1 (2018): 135, https://doi.org/10.1016/j.clsr.2017.05.015.

[918] Somasundaram, "Enhancing Organizational Data Protection: Advanced Security Measures for Database Systems", 60.

[919] Bart Custers vd., EU Personal Data Protection in Policy and Practice, Information Technology and Law Series (T.M.C. Asser Press, 2019), 29:2, https://doi.org/10.1007/978-94-6265-282-8; Bart Custers vd., "A Comparison of Data Protection Legislation and Policies Across the EU", Computer Law & Security Review 34, sy 2 (2018): 235.

[920] Huth ve Matthes, "'Appropriate Technical and Organizational Measures': Identifying Privacy Engineering Approaches to Meet GDPR Requirements", 2.

[921] Custers vd., *EU Personal Data Protection in Policy and Practice*, 29:2; Custers vd., "A Comparison of Data Protection Legislation and Policies Across the EU", 235; Martín-Romo Romero ve De-Pablos-Heredero, "Data Protection by Design", 60.

[922] Tikkinen-Piri vd., "EU General Data Protection Regulation", 138.

[923] Martín-Romo Romero ve De-Pablos-Heredero, "Data Protection by Design", 64.

gözetleme sonucunda hangi tür kişisel verilerin toplandığı, bu verilerin hangi amaçlar için kullanılacağı (örneğin, performans değerlendirmesi, disiplin süreçleri), veri koruma mevzuatıyla uyumlu "erişim kontrolü/yetkilendirme" mekanizmaları çerçevesinde kimlerin bu verilere erişebileceği ve verilerin ne kadar süreyle saklanacağı, "veri minimizasyonu" ve "saklama sınırlaması" ilkeleri kapsamında, işleme amaçları için gerekli olan asgari düzeyle sınırlandırılarak netleştirilmelidir[924]. Ayrıca çalışanların, "bilgilendirilme/şeffaflık" ilkesi gereğince izleme faaliyetleri hakkında nasıl aydınlatılacakları ve erişim, düzeltme, silme/unutulma, işlemenin kısıtlanması, veri taşınabilirliği ve itiraz gibi nasıl kullanabilecekleri açıklanmalıdır. GDPR, veri sahiplerinin bu haklarını kullanabilmeleri için, elektronik yollar da dâhil olmak üzere, gerekli prosedürlerin ve mekanizmaların sağlanmasını zorunlu kılmaktadır[925].

Donanım güvenliği, ağ güvenliği, şifreleme, parola yönetimi gibi tele çalışmaya özgü riskleri ele alan detaylı güvenlik kuralları belirlenmelidir. Kurumsal bilişim kaynaklarının (cihazlar, yazılımlar, ağ erişimi) tele çalışma sırasında nasıl kullanılması gerektiğini tanımlamalıdır. Tele çalışma kapsamında meydana gelebilecek bir veri ihlali durumunda (örneğin, çalışanın cihazının kaybolması, yetkisiz erişim) atılacak adımları, bildirim süreçlerini yönetmelidir. Ayrıca, bu politikalara uyulmamasının hem işveren hem de çalışan açısından sonuçlarının (örneğin, disiplin cezaları) net bir şekilde belirtilmesi gerekmektedir. Tele çalışma modeli, veri ihlallerinin tespiti, soruşturulması ve müdahalesi açısından bazı özel zorluklar getirebilmektedir. Bu nedenle, veri ihlali müdahale prosedürleri, tele çalışmaya özgü senaryoları da dikkate alarak tasarlanmalı ve çalışanlara, bir güvenlik olayını veya şüphesini nasıl ve kime bildirecekleri konusunda net talimatlar verilmelidir. İşverenin bu politikayı yalnızca yazılı olarak oluşturması yeterli olmayıp, aynı zamanda bu kuralları çalışanlara açık şekilde bildirmesi ve gerektiğinde farkındalık eğitimi[926] gibi yollarla bu politikanın

---

[924] Huth ve Matthes, "'Appropriate Technical and Organizational Measures': Identifying Privacy Engineering Approaches to Meet GDPR Requirements", 4; Somasundaram, "Enhancing Organizational Data Protection: Advanced Security Measures for Database Systems", 60.

[925] Tikkinen-Piri vd., "EU General Data Protection Regulation", 139.

[926] Bu bağlamda AB Yapay Zekâ Tüzüğü, doğrudan bağlayıcı bir eğitim yükümlülüğü getirmemektedir. Bununla birlikte Tüzüğün Başlangıç Bölümü 20, "Yapay Zekâ Okuryazarlığı" (AI Literacy) kavramını düzenleyerek; sağlayıcıların, dağıtıcıların ve sistemden etkilenen kişilerin yapay zekâ sistemlerinin işleyişini ve etkilerini anlamalarını sağlayacak bir kültürün geliştirilmesini teşvik etmektedir. Bknz. Voigt ve Hullen, *The EU AI Act*, 42.

içselleştirilmesini sağlaması da önem arz etmektedir[927]. Politikalar yaşayan belgeler olmalı, yasal değişiklikler, teknolojik gelişmeler (ve kurumsal ihtiyaçlar doğrultusunda düzenli olarak gözden geçirilmeli ve güncellenmelidir[928].

Politika geliştirmenin temel amacı, şeffaflığı sağlayarak çalışanların haklarını güvence altına almaktır. Etkili ve düzenli olarak güncellenen bir politika, çalışanların neyin, neden ve nasıl izlendiği konusunda açıkça bilgilendirilmelerini gerektirmektedir. Bu kapsamda çalışanların, iş ilişkisi kapsamındaki her türlü izleme ve gözetleme faaliyeti hakkında önceden kapsamlı biçimde bilgilendirilmeleri (aydınlatma yükümlülüğü) esastır. Politikalar aynı zamanda sendika üyeliği gibi özel nitelikli kişisel veriler ile ayrımcılığa yol açabilecek verilerin toplanmasına katı sınırlamalar getirmeli; çalışanların işlenen kişisel verilerine erişimini ve bu bilgileri, talep hâlinde temsilcileri veya denetleyici otoritelerle paylaşabilmelerini sağlamalıdır[929]. Sonuç olarak, iyi tanımlanmış ve etkin şekilde uygulanan politikalar, tele çalışma modelindeki izleme faaliyetlerinin adil, hesap verebilir ve hukuka uygun bir çerçevede yürütülmesini sağlamaktadır. Bu sayede veri işleme süreçlerinin öngörülebilirliği ve denetlenebilirliği artmaktadır. Bu durum ise işverenlerin mevzuata uyumunu güçlendirmekte, çalışan güvenini artırarak rekabet avantajı yaratmakta ve veri ihlali risklerini en aza indirmektedir[930].

4.6.2.3. İş Verileri ile Kişisel Verilerin Ayrıştırılması ve Yönetimi

Tele çalışma modelinde, iş ve özel hayat arasındaki sınırların belirsizleşmesi, özellikle çalışanların kullandığı cihazlar ve dijital platformlar üzerinde işe ait verilerin yanı sıra kişisel verilerin bulunması riskini artırır. Çalışan izleme faaliyetleri yürütülürken, işverenin meşru işletmesel amaçlarıyla ilgili olmayan veya iş görme ediminin kapsamı dışında kalan kişisel verilere müdahale etmemesi; veri minimizasyonu, amaçla

---

[927] Ayrıntılı bilgi için bknz. Kişisel Verileri Koruma Kurumu, *Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)* (2018), 8; Mahlangu ve Schutte, "Analysing Information Technology Risks Affecting South African Government Employers Due to Remote Working", 53; Altıntaş ve Barkuş, "Dijital Ortamlarda Kişisel Veri Güvenliği Kavramı Üzerine Bir Derleme Çalışması", 47; Chukwudi Tabitha Aghaunor vd., "Data Security Strategies to Avoid Data Breaches in Modern Information Systems", *World Journal of Advanced Research and Reviews* 20, sy 3 (2023): 2122.
[928] Custers vd., *EU Personal Data Protection in Policy and Practice*, 29:8.
[929] ILO, *Work for a brighter future–Global Commission on the Future of Work*, 44.
[930] Tikkinen-Piri vd., "EU General Data Protection Regulation", 135.

sınırlılık ve özel hayatın gizliliğinin korunması ilkeleri açısından hayati önem taşımaktadır. Bu nedenle, iş görme edimine ilişkin verilerin çalışanın kişisel verilerinden etkin bir şekilde ayrıştırılması zorunluluk arz etmektedir. Bu doğrultuda, verileri tamamen ayrı dijital ortamlarda tutan güvenli sanal alan (secure sandbox) ve sanal masaüstü altyapısı (VDI) gibi teknik izolasyon yöntemlerinden, verileri "iş" veya "kişisel" olarak sınıflandıran veri etiketleme süreçlerinden ve hem depolama hem de aktarım sırasında güçlü şifreleme politikalarından yararlanılması gerekmektedir.

Kurumsal veriler ile kişisel verilerin birbirinden ayrılması, en temel koruma yöntemlerinden biridir. Özellikle çalışanın kendi kişisel cihazını iş için kullandığı durumlarda bu teknik yalıtım hayati önem taşır ve güvenli sanal alan (secure sandbox)[931] veya sanal masaüstü altyapısı (Virtual Desktop Infrastructure – VDI)[932] gibi teknolojilerle sağlanabilmektedir[933]. Bu sayede işveren, yalnızca işletmeye ilişkin verilerin bulunduğu alanı yönetebilir ve olası bir uzaktan silme işleminde yalnızca bu alan hedeflenmektedir. Ayrıca, hem cihazda depolanan (data-at-rest) hem de aktarım hâlindeki (data-in-transit) kurumsal verilerin güçlü bir şekilde şifrelenmesi zorunlu tutulmalıdır[934].

Veri ayrımını sağlayan teknolojik yöntemlerden ilki olan güvenli sanal alan (secure sandbox), özellikle bulut ortamlarında kullanılan yazılım bileşenlerinin, örneğin belirli alt programlar veya yerel kod parçaları gibi, ana sistemden izole edilerek

---

[931] Ayrıntılı bilgi için bknz. Marco Abbadini, "Sandboxing and Data Protection in Cloud Computing Environments" (Doktora Tezi, Bergamo, University of Bergamo, 2025), https://tesidottorato.depositolegale.it/bitstream/20.500.14242/209385/1/Abbadini_Marco_1048650_PhD_Thesis_rev.pdf.

[932] Sanal masaüstü altyapısı, kullanıcıların fiziksel bir bilgisayarda değil, uzaktaki bir sunucu üzerinde çalışan masaüstü oturumlarına erişmesini sağlayan teknolojiyi ifade eder. Ayrıntılı bilgi için bknz. Asaf Algawi vd., "Efficient Protection for VDI Workstations" (2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Paris, France: IEEE, 2019), 169-72, https://ieeexplore.ieee.org/document/8854034/; Srinivasa Rao Thumala, "Running Sustainable Virtual Desktop Infrastructure (VDI) Solutions in the Cloud", *International Journal on Recent and Innovation Trends in Computing and Communication* 9, sy 12 (2021): 91-102.

[933] Jessica Keyes, Bring Your Own Devices (BYOD) Survival Guide (CRC Press Taylor & Francis Group, 2016), 159; Veri tabanı bölümlendirme (fiziksel ayrıştırma), sunucu ve ağ seviyesinde ayrıştırma, mantıksal ayrıştırma (sanal bölümlendirme), rol tabanlı ayrıştırma (erişim kontrolü) gibi diğer yöntemler için bknz. "What Is Data Segregation?", PrivacyEngine Data Protection Software and Solutions, t.y., erişim 07 Haziran 2025, https://www.privacyengine.io/resources/glossary/data-segregation/.

[934] Madhavi Dhingra, "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)", *Procedia Computer Science* 78 (2016): 181; Georg Disterer ve Carsten Kleiner, "BYOD Bring Your Own Device", *Procedia Technology* 9 (2013): 46.

çalıştırılmasını sağlayan bir güvenlik önlemidir[935]. Bu yöntemin temel amacı, sistemde oluşabilecek bir güvenlik açığının tüm sisteme yayılmasını engellemektir. Söz konusu yöntemde esas alınan en az ayrıcalık ilkesi uyarınca, bir yazılım bileşeni yalnızca görevini yerine getirebilmesi için zorunlu olan sistem kaynaklarına erişebilmekte; bunun dışında bir erişim yetkisi tanınmamaktadır. Bu erişim kuralları, geliştiriciler tarafından açık ve anlaşılır şekilde tanımlanmaktadır. Örneğin, dosya okuma-yazma izinleri, ağ bağlantılarına erişim veya başka programlarla iletişim kurma yetkileri bu kurallarla sınırlandırılmaktadır[936]. Tele çalışma modelinde bu yöntem, çalışanların şirket kaynaklarına erişmek için kullandığı uygulamaların güvenliğini artırmak için kullanılabilmektedir. Çalışanın bilgisayarına kurulan bir işyeri uygulaması, bu yöntemle oluşturulmuş bir sanal alan içinde çalıştırılabilmektedir. Bu sanal alan, uygulamanın çalışanın kişisel dosyalarına veya yerel ağdaki diğer cihazlara erişmesini engelleyen katı bir politika uygulamaktadır. Aynı zamanda, uygulamanın yalnızca belirli işyeri sunucularıyla iletişim kurmasına izin vererek, olası bir güvenlik ihlali durumunda verilerin yetkisiz yerlere sızdırılmasını veya kötü amaçlı yazılımların yayılmasını önlemektedir. Bu sayede hem işletme verileri hem de çalışanın kişisel verileri, tele çalışma modelinin getirebileceği potansiyel risklere karşı korunmuş olmaktadır.

Güvenli sanal alan yöntemine ek olarak, veri ayrımını sağlamada farklı bir yaklaşım sunan bir diğer güçlü teknolojiyi sanal masaüstü altyapısı (VDI) oluşturmaktadır. Sanal masaüstü altyapısı, çalışanların masaüstü bilgisayar deneyimini doğrudan kendi cihazları üzerinden değil, güçlü ve merkezi bir sunucu üzerinden uzaktan yaşamalarını sağlayan bir teknolojiyi ifade etmektedir[937]. Bu sistemde çalışanlar, genellikle kendi başlarına işlem gücü çok düşük olan ve yalnızca ana sunucuya bağlanma görevi gören ince istemci (thin client) gibi basit cihazlar kullanarak şirketin veri merkezindeki sanal masaüstlerine bağlanmaktadır. . Yani çalışanın bilgisayarı sadece bir "ekran" görevi görmekte; asıl işlem ve veri işleme şirketin kontrolündeki merkezî sunucuda gerçekleşmektedir. VDI yapısında tüm masaüstleri, aynı temel ayarlara sahip bir "ana

[935] Falque-Pierrotin, *Opinion 2/2017 on Data Processing at Work*, 17.
[936] Ayrıntılar için bknz. Abbadini, "Sandboxing and Data Protection in Cloud Computing Environments", 17-87.
[937] "What Is Virtual Desktop Infrastructure (VDI)? | Microsoft Azure", erişim 13 Haziran 2025, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-virtual-desktop-infrastructure-vdi.

sistem kopyasından" çoğaltılarak oluşturulmaktadır. Bu sayede hem bakım ve güncellemeler merkezi şekilde yönetilebilmekte hem de binlerce fiziksel bilgisayarı tek tek kontrol etmeye gerek kalmamaktadır. Bu durum hem maliyetleri azaltmakta hem de tüm cihazlarda aynı güvenlik ayarlarının uygulanmasını sağlamaktadır[938]. VDI, özellikle tele çalışma için son derece etkili bir çözüm sunmakta, zira çalışanların internet bağlantısı olan her yerden kurumsal masaüstlerine güvenli bir şekilde erişmelerini sağlamaktadır.

Altyapı düzeyinde teknik ayrım sağlayan yöntemlerin yanı sıra, doğrudan verinin kendisine odaklanan idari yaklaşımlar da büyük önem taşımaktadır. Bu yaklaşımların en etkililerinden biri olan verilerin etiketlenmesi (data labelling/tagging), dijital verilerin veya dosyaların içeriklerine veya niteliklerine göre (örneğin, "iş", "kişisel", "gizli", "hassas") sınıflandırılmasını ve işaretlenmesini içeren teknik ve idari bir süreci oluşturmaktadır. Veriler, işveren veya işçi tarafından "kişisel" veya "iş" olarak etiketlenebilmektedir. Etiketleme, çalışanlar tarafından manuel olarak yapılabileceği gibi, belirli anahtar kelimeler, dosya türleri veya kaynaklar (örneğin, kurumsal e-posta alan adı) temelinde otomatik sistemler tarafından da gerçekleştirilebilmektedir[939]. Etiketlenmiş veriler, izleme araçlarının yalnızca "iş" olarak etiketlenmiş ve meşru amaçla ilgili verilere odaklanacak şekilde yapılandırılmasına, "kişisel" olarak etiketlenmiş verilerin ise izleme kapsamı dışında tutulmasına veya en azından daha sıkı erişim ve işleme kurallarına tabi tutulmasına olanak tanımaktadır.

4.6.2.4. Risk Değerlendirmesi ve Veri Koruma Etki Değerlendirmesi

Tele çalışmada izleme faaliyetlerinin çalışanların kişisel verileri ve temel hakları üzerinde oluşturduğu risklerin düzenli olarak değerlendirilmesi işverenin temel sorumluluklarındandır. Bu değerlendirme, izleme teknolojilerinin kullanımının başladığı andan itibaren düzenli olarak güncellenmeli ve özellikle teknolojik, hukuki veya operasyonel değişiklikler göz önüne alınmalıdır. Bu kapsamda, çalışmamızın önceki bölümlerinde de değinildiği üzere[940], GDPR'da düzenlenen veri koruma etki

[938] Ayrıntılı bilgi için bknz Algawi vd., "Efficient Protection for VDI Workstations", 169-72; Thumala, "Running Sustainable Virtual Desktop Infrastructure (VDI) Solutions in the Cloud", 91-102.
[939] Bknz.: Case of Libert V. France.
[940] Veri koruma etki değerlendirmesinin GDPR kapsamındaki yasal dayanağı için bknz. 3.4.1.3. Bölüm

değerlendirmesi önemli bir rol oynamaktadır. Veri koruma etki değerlendirmesi, veri işleme faaliyetlerinin sistematik ve proaktif şekilde analizini sağlamakta ve olası risklerin önceden tespiti ile önlenmesine yönelik hem teknik hem de organizasyonel önlemler içermektedir. Bu yaklaşım, özellikle sağlık, biyometrik ve genetik gibi özel nitelikli kişisel veri türleri için kritik bir önem taşımaktadır. İşverenlerin kişisel veri işleme faaliyetlerinde, GDPR 6. maddesinin 1. fıkrasının (f) bendi uyarınca, orantılılık ilkesine uygun hareket etmeleri ve çalışanların makûl gizlilik beklentilerini göz önünde bulundurmaları gerekmektedir. Bu çerçevede, herhangi bir izleme teknolojisini uygulamadan önce, olası risklerin ve etkilerin sistemli bir şekilde değerlendirilmesini sağlayan veri koruma etki değerlendirmesi yapılmalıdır[941].

Tele çalışma sırasındaki izleme faaliyetleri kişisel veriler açısından yüksek risk taşıyorsa daha kapsamlı bir değerlendirme gereklidir. Örneğin, bir işverenin, tüm tele çalışanlarının verimliliğini ölçmek ve duygu durumlarını analiz etmek amacıyla yapay zekâ destekli, sürekli ekran ve webcam kaydı yapan bir sistemi devreye alması, özel hayatın gizliliğine yönelik yüksek risk oluşturacağı için, bu faaliyete başlamadan önce bir GDPR 35. maddesi uyarınca bir veri koruma etki değerlendirmesi yapılması zorunludur[942]. Veri koruma etki değerlendirmesi, kişisel veri işleme faaliyetlerinin amaçlarını ve kapsamını açıkça tanımlamalı, işlemenin gerekliliğini ve orantılılığını göstermeli kişisel verilerin korunmasına yönelik riskleri ve bu riskleri azaltacak önlemleri içermelidir[943].

Her ne kadar mevzuatımızda, GDPR'da olduğu gibi "veri koruma etki değerlendirmesi" başlığı altında açık bir yükümlülük düzenlenmemiş olsa da; 6698 sayılı Kanun'un 4. maddesinde yer alan genel ilkeler ile 12. maddesinde düzenlenen veri güvenliğine ilişkin yükümlülükler birlikte değerlendirildiğinde, veri sorumlusu konumundaki işverenlerin, özellikle tele çalışma süreçlerinde ortaya çıkabilecek veri

---

[941] Falque-Pierrotin, *Opinion 2/2017 on Data Processing at Work*, 13-15.
[942] Dimitra Georgiou ve Costas Lambrinoudakis, "DPIA for Cloud-Based Health Organizations in the Context of GDPR", European Conference on Cyber Warfare and Security 22, sy 1 (2023): 187, https://doi.org/10.34190/eccws.22.1.1144; Joshua Blume, "A Contextual Extraterritoriality Analysis of the DPIA and DPO Provisions in the GDPR", Georgetown Journal of International Law 49, sy 4 (2018): 1435.
[943] Blume, "A Contextual Extraterritoriality Analysis of the DPIA and DPO Provisions in the GDPR", 1435; Fatemeh Zarrabi vd., "Changes in Conducting Data Protection Risk Assessment and After GDPR Implementation", preprint, Leicester, UK, 24 Nisan 2023, 10, https://doi.org/10.48550/arXiv.2304.11876.

güvenliği risklerini önceden tespit etmesi, gerekli teknik ve idari tedbirleri alması gerekmektedir. Nitekim Kişisel Verileri Koruma Kurulu tarafından yayımlanan rehberlerde de kişisel verilerin özel nitelikli kişisel veri olup olmadığı, mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği, güvenlik ihlali hâlinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği belirlenerek gerekli tedbirlerin alınması belirtilmiştir[944]. Bu çerçevede, KVKK, her ne kadar veri koruma etki değerlendirmesini açıkça tanımlamasa da benzer içerikte bir değerlendirme sürecini dolaylı olarak zorunlu kılmaktadır[945].

4.6.2.5. Kendi Cihazını Getir Politikaları

Teknolojinin tüketim malı hâline gelmesi (IT consumerization) ve mobil bilişimin yaygınlaşması, geleneksel çalışma modellerinde önemli bir dönüşüme yol açmıştır[946]. Çalışanların kişisel akıllı telefon, tablet ve dizüstü bilgisayar gibi cihazları iş süreçlerine dâhil etme eğilimi, "kendi cihazını getir" (BYOD) olarak adlandırılan yeni bir kurumsal politikayı ortaya çıkarmıştır[947]. Bu politika, çalışanların kişisel cihazlarını kullanarak kurumsal ağlara ve verilere erişmesine olanak tanımaktadır[948]. Temel motivasyon, çalışanların hem kişisel hem de iş amaçlı görevler için tek bir cihaz kullanma ("dual use") arzusudur; zira hiç kimse iki farklı cihazı yanında taşımak ve yönetmek istememektedir[949]. Buna ek olarak, işverenler de bu politika sayesinde çalışanlara cihaz temin etme maliyetinden kaçınabilmektedir[950]. Uygulamada bu denli yaygınlaşan BYOD politikalarının hukuki zemini ise, işverenin araç gereç sağlama borcuna ilişkin yasal düzenlemelerde bulunmaktadır.

---

[944] Ayrıntılı bilgi için bknz. Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) (2018), 8.
[945] Arzu Galandarlı, "Veri Etki Değerlendirilmesi (GDPR Article 29 Ve KVKK)", Hukuk ve Bilişim Dergisi -, 01 Nisan 2025, https://www.hukukvebilisimdergisi.com/veri-etki-degerlendirilmesi-gdpr-article-29-ve-kvkk/.
[946] Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 17; Disterer ve Kleiner, "BYOD Bring Your Own Device", 44; Morufu Olalere vd., "A Review of Bring Your Own Device on Security Issues", *Sage Open* 5, sy 2 (2015): 1, https://doi.org/10.1177/2158244015580372.
[947] Disterer ve Kleiner, "BYOD Bring Your Own Device", 43; Olalere vd., "A Review of Bring Your Own Device on Security Issues", 1.
[948] Dhingra, "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)", 179.
[949] Disterer ve Kleiner, "BYOD Bring Your Own Device", 43.
[950] Bello Garba, "Bring Your Own Device Organizational Information Security and Privacy", *ARPN Journal of Engineering and Applied Sciences,* 10, sy 3 (2015): 1279; Zehra Özsürünç ve Arafat Salih Aydıner, "Kendi Cihazını Getir (KCG) Kavramının Uygulanmasına Genel Bir Bakış", 2022, 372-80.

Bu bağlamda "Kendi Cihazını Getir" politikaları, Türk Borçlar Kanunu'nun 413. maddesinde düzenlenen işverenin, iş için gerekli araç ve malzemeyi sağlama yükümlülüğü çerçevesinde bir istisna teşkil etmektedir. Gerçekten de TBK 413. maddesi 1. fıkrası uyarınca asıl kural, aksine bir anlaşma veya yerel adet bulunmadıkça, işin görülmesi için gerekli olan araç ve malzemenin işveren tarafından temin edilmesidir[951]. Ancak, TBK 413. maddesi 1. fıkrasının, işçi ile işverenin anlaşması durumunda işçinin kendi araç veya malzemesini işin görülmesi için kullanmasına olanak tanıması, BYOD politikalarının hukuki dayanağını oluşturmaktadır. Bu tür bir anlaşma mevcut olduğunda işveren, yine aksi kararlaştırılmadıkça veya yerel bir adet bulunmadıkça, işçinin kendi cihazını kullanması karşılığında "uygun bir karşılık" ödeme yükümlülüğü altındadır. Özellikle uzaktan çalışma ve evde çalışma gibi yeni normal çalışma modellerinin yaygınlaşmasıyla birlikte BYOD uygulamaları da artış göstermiştir. Bu modellerde, işveren tarafından sağlanan ekipman ve bunların korunmasına yönelik yükümlülüklerin iş sözleşmesinde belirtilmesi esastır[952]. İşçi kendi cihazını kullandığında dahi, internet bağlantısı, yazılım lisansları gibi işin görülmesinin gerektirdiği her türlü harcamanın TBK madde 414 uyarınca işveren tarafından karşılanması gerekmektedir; zira bu masrafların işçiye yükletilmesine yönelik anlaşmalar geçersiz sayılmaktadır[953]. Ancak yasal bir zemine oturtulmuş olsa dahi bu uygulama, doğasında barındırdığı menfaat ve risk çatışması nedeniyle işveren açısından dikkatle yönetilmesi gereken bir ikilem yaratmaktadır.

Kendi cihazını getir politikaları, bir yandan çalışan memnuniyetini, motivasyonu, esnekliği ve verimliliği artırma gibi önemli faydalar sunarken[954], diğer yandan kurumlar için ciddi güvenlik, gizlilik ve hukuki riskler barındırmaktadır. Bu riskler o

---

[951] Muhammed Türkalp Seçkin, "İşverenin Araç ve Malzeme Sağlama ile Giderlere Katlanma Borcu" (Doktora Tezi, Marmara Üniversitesi, 2024), 134; Sevcan Günsu Gerçek, "Türk İş Hukukunda Uzaktan Çalışma" (Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, 2024), 99.

[952] Rabia Büşra Erafşar, "Bireysel İş Hukukunda Yeni Normal Çalışma Modeli: Evden Çalışma" (Yayınlanmamış Yüksek Lisans Tezi, Ankara Yıldırım Beyazıt Üniversitesi, 2023), 59; Seçkin, "İşverenin Araç ve Malzeme Sağlama ile Giderlere Katlanma Borcu", 135; Gerçek, "Türk İş Hukukunda Uzaktan Çalışma", 99.

[953] Seçkin, "İşverenin Araç ve Malzeme Sağlama ile Giderlere Katlanma Borcu", 136; Gerçek, "Türk İş Hukukunda Uzaktan Çalışma", 100.

[954] Dhingra, "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)", 179; Melina Seedoyal Doargajudhur ve Peter Dell, "The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation", *Journal of Computer Information Systems* 60, sy 6 (2020): 518; Disterer ve Kleiner, "BYOD Bring Your Own Device", 45.

kadar ciddidir ki, bazı araştırmacılar kendi cihazını getir politikasını ifade etmekte kullanılan BYOD kısaltmasını "kendi tehlikeni getir" (bring your own danger) olarak yorumlamıştır[955]. Bu ikilem, işletmeleri tele çalışma ve uzaktan erişim süreçlerinde kişisel verilerin korunması hukuku çerçevesinde dikkatli idari tedbirler almaya zorlamaktadır. Etkin bir kendi cihazını getir politikası, bu dengeyi kuran temel idari tedbirdir.

Kendi cihazını getir politikalarının getirdiği en temel zorluk, kişisel alan ile iş alanının iç içe geçmesinden kaynaklanmaktadır[956]. Çalışanın kişisel cihazı, aile fotoğrafları, filmler, kişisel e-postalar, banka hesap bilgileri, kullanıcı adları ve şifreler gibi son derece önemli veriler içermektedir[957]. Aynı cihaz kurumsal verilere erişmek için kullanıldığında, kurumun güvenlik ve denetim ihtiyaçları ile çalışanın gizlilik hakkı arasında bir gerilim ortaya çıkmaktadır[958]. Bu gerilim, aşağıda detaylı olarak incelenecek olan şu dört temel hususta somutlaşmaktadır: izleme ve gözetleme hakkı, veri sızıntısı ve kayıp riski, uzaktan silme (remote wipe) ve veri yönetimi ile hukuki sorumluluk ve e-keşif.

İşverenlerin ağ güvenliğini ve veri bütünlüğünü sağlama amacıyla talep ettiği izleme ve gözetleme hakkı, kişisel cihazlar söz konusu olduğunda çalışanın özel hayatının gizliliği ve mahremiyet beklentileriyle çelişmektedir[959]. Ancak bu durum, kişisel cihazlar söz konusu olduğunda çalışanın özel hayatının izlenmesi anlamına gelebilir ve bu mahremiyet beklentileriyle çelişmektedir[960].

Mahremiyet endişelerine ek olarak, kişisel cihazların taşınabilir yapısı somut güvenlik risklerini de beraberinde getirmektedir. Çalışanların bu cihazları kaybetme veya çaldırma olasılığının masaüstü bilgisayarlara göre daha yüksek olması, önemli bir veri sızıntısı ve kayıp riski doğurmaktadır[961]. Cihazın kaybedilmesi durumunda hem kişisel

---

[955] Doargajudhur ve Dell, "The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation", 519.
[956] Keyes, *Bring Your Own Devices (BYOD) Survival Guide*, 2.
[957] Dhingra, "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)", 181.
[958] Falque-Pierrotin, *Opinion 2/2017 on Data Processing at Work*, 16-18.
[959] Dhingra, "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)", 182.
[960] Olalere vd., "A Review of Bring Your Own Device on Security Issues", 2.
[961] Keyes, *Bring Your Own Devices (BYOD) Survival Guide*, 2.

hem de kurumsal veriler yetkisiz kişilerin eline geçebilmektedir[962]. Bu durum, veri sızıntısı riskinin yanı sıra, şirketin yasal yükümlülüklere uyumu açısından da büyük bir risk oluşturmaktadır[963]. Çalışanın cihazının kaybolması veya çalınması durumunda kurumsal verilerin uzaktan silinmesi (sadece kurumsal verilerin hedeflenmesi kaydıyla) gibi önlemler ve iş ilişkisi sona erdiğinde veya cihaz artık iş amacıyla kullanılmayacaksa kurumsal verilerin cihazdan güvenli bir şekilde kaldırılmasına yönelik prosedürler tanımlanmalıdır.

Veri sızıntısı riskine karşı sunulan çözümlerin kendisi de yeni hukuki sorunlar doğurabilmektedir. Örneğin işverenler, bir güvenlik ihlali veya cihaz kaybı durumunda veri yönetimi kapsamında cihazdaki kurumsal verileri uzaktan silebilme (remote wipe) hakkını talep etmektedir[964]. Ancak bu işlem, çalışanın kişisel verilerinin de (fotoğraflar, kişiler, vb.) silinmesi veya cihazın kullanılamaz hâle gelmesi ("bricking") riskini taşımaktadır[965]. Bu, çalışanın mülkiyet hakkına ve kişisel verilerinin bütünlüğüne yönelik ciddi bir müdahaledir.

Veri yönetimiyle ilgili bu operasyonel sorunların ötesinde, BYOD politikaları işvereni ciddi hukuki sorumluluklarla da karşı karşıya bırakmaktadır. Bir dava sürecinde çalışanın kişisel cihazındaki kurumsal veriler (e-postalar, belgeler) delil niteliği taşıyabilir. Bu durum, "e-keşif" (e-discovery) olarak bilinen yasal süreçlerde, şirketin çalışanın kişisel cihazına erişmesini zorunlu hâle getirebilmektedir. Böyle bir zorunluluk ise hem ciddi gizlilik sorunlarına yol açar hem de şirketin omuzlarına ağır bir hukuki yükümlülük bindirir[966].

Bu riskleri yönetmek ve hukuki uyumluluğu sağlamak için işverenlerin kapsamlı ve net bir kendi cihazını getir politikası oluşturması kritik bir idari tedbirdir. Bu politika, işverenin kontrol ve güvenlik ihtiyaçları ile çalışanın hakları arasında bir denge kurmalıdır[967]. Etkili bir kendi cihazını getir politikası aşağıda belirtilen unsurları içermelidir.

---

[962] Olalere vd., "A Review of Bring Your Own Device on Security Issues", 3.
[963] Disterer ve Kleiner, "BYOD Bring Your Own Device", 46.
[964] Keyes, *Bring Your Own Devices (BYOD) Survival Guide*, 4.
[965] Dhingra, "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)", 182.
[966] Keyes, *Bring Your Own Devices (BYOD) Survival Guide*, 237.
[967] Dhingra, "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)", 184.

Etkili bir politikanın temelini, açık ve anlaşılır bir rıza mekanizması oluşturmaktadır. Bu doğrultuda, çalışanların kişisel cihazlarını iş amacıyla kullanmaya başlamadan önce, tüm şartları anladıklarını ve kabul ettiklerini yazılı olarak beyan ettikleri bir sözleşme veya onay formu imzalamaları gerekmektedir[968]. Bu belgede, işverenin cihazı izleme, denetleme ve gerektiğinde verileri uzaktan silme gibi yetkileri açıkça belirtilmeli ve çalışanın bu şartları kabul ettiğine dair rızası kayıt altına alınmalıdır[969].

Politikanın bir diğer önemli unsuru, kabul edilebilir kullanım kurallarını net bir şekilde ortaya koymaktır. Bu çerçevede politika, çalışanın kişisel cihazını iş için kullanırken hangi uygulamaları yükleyebileceğini, hangi web sitelerine erişebileceğini ve hangi verileri cihazda saklayabileceğini tereddüde yer bırakmayacak şekilde tanımlamalıdır[970]. Bu kurallara örnek olarak; güvenilmeyen kaynaklardan uygulama indirmek, hassas şirket verilerini kişisel bulut hesaplarında depolamak, root/jailbreak gibi işlemlerle cihaz güvenliğini zayıflatmak veya halka açık güvensiz Wi-Fi ağları üzerinden sisteme bağlanmak gibi eylemlerin kısıtlanması gösterilebilmektedir.

Politika ayrıca, çalışanların uyması gereken temel güvenlik yükümlülüklerini de net bir şekilde tanımlamalıdır. Bu yükümlülükler arasında; karmaşık bir parola veya PIN kullanımı, cihazın belirli bir süre işlem yapılmadığında otomatik olarak kilitlenmesi, işletim sistemi ile uygulamaların güncel tutulması ve anti-virüs yazılımı kullanımı gibi asgari standartlar yer almaktadır[971].

Politikanın son temel unsuru, ayrılma prosedürleridir (exit procedures). Bu prosedürler, çalışanın işten ayrılması hâlinde kişisel cihazındaki tüm kurumsal verilere erişimin nasıl sonlandırılacağını ve bu verilerin nasıl güvenli bir şekilde silineceğini net bir şekilde belirlemelidir[972].

Sonuç olarak, kendi cihazını getir politikaları, tele çalışmanın getirdiği esnekliğin bir uzantısı olarak modern iş hayatında giderek daha fazla yer bulmaktadır. Ancak bu

---

[968] Keyes, *Bring Your Own Devices (BYOD) Survival Guide*, 233.
[969] Keyes, Bring Your Own Devices (BYOD) Survival Guide, 271.
[970] Keyes, Bring Your Own Devices (BYOD) Survival Guide, 215.
[971] Keyes, *Bring Your Own Devices (BYOD) Survival Guide*, 255; Disterer ve Kleiner, "BYOD Bring Your Own Device", 52.
[972] Dhingra, "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)", 182.

model, kişisel verilerin korunması hukuku açısından işverenleri ciddi yükümlülükler ve risklerle karşı karşıya bırakmaktadır[973]. Bu risklerin yönetimi, sadece teknik çözümlerle değil, aynı zamanda çalışanın gizlilik haklarına saygı duyan, şeffaf, rızaya dayalı ve net kurallar içeren kapsamlı idari tedbirlerle mümkündür. İyi yapılandırılmış bir kendi cihazını getir politikası, işverenin meşru güvenlik çıkarları ile çalışanın temel hak ve özgürlükleri arasında uygun bir denge kurmanın en önemli aracıdır.

4.6.2.6. Üçüncü Taraf Veri İşleyenlerle (İzleme Aracı Sağlayıcıları) İlişkilerin Yönetimi

Tele çalışanların izlenmesi amacıyla kullanılan yazılım ve hizmetler, sıklıkla işveren (veri sorumlusu) tarafından doğrudan geliştirilmek yerine, bu alanda uzmanlaşmış üçüncü taraf hizmet sağlayıcıları tarafından sunulmaktadır. Bu durum, işvereni veri sorumlusu, izleme aracını sunan teknoloji şirketini ise veri işleyen konumuna getirmektedir. Veri koruma hukukunun en temel ilkelerinden biri, veri işleme faaliyetinin dış kaynaklardan temin edilmesinin, işverenin veri sorumlusu sıfatıyla taşıdığı yükümlülükleri ortadan kaldırmamasıdır. Aksine bu durum, veri işleyenlerle kurulan ilişkilerin titizlikle yönetilmesini gerektiren önemli idari tedbirlerin alınmasını zorunlu kılmaktadır[974]. İşveren, veri işleyenin eylemlerinden de müştereken sorumlu olduğundan, bu sürecin doğru bir hukuki ve operasyonel zemine oturtulması hayati önem taşımaktadır[975].

İşverenlerin, üçüncü taraflardan izleme hizmetleri alırken yerine getirmesi gereken yükümlülüklerin başında, kapsamlı bir durum tespiti (due diligence) gelmektedir. GDPR 28. maddesinin 1. Fıkrasında açıkça belirtilen yükümlülük uyarınca, işverenin seçtiği veri işleyenin, kişisel verilerin korunmasına yönelik uygun teknik ve idari tedbirleri sağlayabilecek yeterlilikte olması gerekmektedir. Bu kapsamda işveren, öncelikle veri işleyenin teknik altyapısını, veri güvenliği tecrübesini ve varsa sahip olduğu ulusal ya da uluslararası sertifikaları (örneğin ISO 27001) değerlendirmelidir. Ayrıca, veri işleyenin verileri hangi ülkelerde ve veri merkezlerinde sakladığını,

---

[973] Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 17.
[974] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 229.
[975] Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 62-66.

özellikle Avrupa Birliği dışına veri aktarımının olup olmadığını incelemeli ve daha önce yaşanmış olası veri ihlalleri ve bu ihlaller karşısındaki şeffaflık durumunu analiz etmelidir.

İşveren ile seçilen izleme hizmet sağlayıcısı arasındaki ilişki, hukuki belirlilik ve güvence sağlamak adına mutlaka KVKK ve GDPR'ın 28. maddesinin 3. fıkrası hükümleri ile uyumlu, yazılı bir veri işleme sözleşmesi (data processing agreement - DPA) ile düzenlenmelidir. Bu sözleşme, veri işlemenin hukuki çerçevesini belirleyerek, tarafların yükümlülük ve sorumluluklarını netleştirecek şekilde hazırlanmalıdır. Sözleşmede özellikle veri işlemenin kapsamı, süresi, niteliği ve amacı ayrıntılı olarak açıklanmalı; işlenecek kişisel veri türleri (aktivite logları, ekran görüntüleri, konum bilgileri gibi) ve veri sahipleri kategorileri (örneğin tele çalışanlar) açıkça tanımlanmalıdır.

Veri işleyenin, yalnızca veri sorumlusunun yazılı olarak vereceği talimatlar doğrultusunda hareket edeceği de taahhüt altına alınmalıdır. Ayrıca, veri işleyenin personelinin kişisel verilere erişimi gizlilik yükümlülüğü ile sınırlanmalı ve bu yükümlülük sözleşmede belirtilmelidir. Veri işleyenin somut olarak hangi teknik ve idari güvenlik tedbirlerini alacağı sözleşme ile açıkça düzenlenmeli ve eğer alt işleyen kullanılacaksa, bu konuda veri sorumlusundan önceden yazılı izin alınması ve aynı yükümlülüklerin alt işleyene de aktarılması sağlanmalıdır.

Veri sahiplerinin haklarını (erişim, silme, düzeltme gibi) kullanabilmeleri için veri işleyenin, veri sorumlusuna destek olması gerektiği sözleşmede ifade edilmeli; herhangi bir veri ihlali durumunda ise veri işleyenin bunu derhâl ve gecikmeksizin veri sorumlusuna bildireceği açıkça belirtilmelidir. İş ilişkisinin sona ermesi hâlinde, işlenen tüm kişisel verilerin veri sorumlusunun talebi doğrultusunda ya silinmesi ya da geri verilmesi hususunda net hükümler konulmalıdır. Ayrıca, veri sorumlusunun veya yetkilendireceği denetçinin sözleşmedeki yükümlülüklere uyumu denetleme ve bu denetimlere aktif katılım sağlama hakkı sözleşmede yer almalıdır.

Sonuç olarak, üçüncü taraf izleme araçları kullanmak, işverenler için operasyonel avantajlar sağlasa da kişisel veri koruma hukuku açısından önemli sorumlulukları ve riskleri beraberinde getirmektedir. İşverenlerin, yukarıda belirtilen kapsamlı durum

tespiti süreçlerini yürütmeleri ve hukuki olarak bağlayıcı "veri işleme sözleşmeleri" düzenlemeleri, bu risklerin etkin yönetilmesi ve mevzuata uyum sağlanması açısından temel öneme sahip idari tedbirlerdir.

4.6.2.7. Giyilebilir Teknolojilerin Kullanımına İlişkin Politikalar

İşyerinde giyilebilir teknoloji kullanımının artması, işverenlerin bu teknolojilerin kullanımını düzenleyen net, şeffaf ve hukuka uygun bir politika oluşturmasını zorunlu bir idari tedbir hâline getirmektedir. Bu politikalar oluşturulurken taşıdığı riskler de mutlaka göz önünde bulundurulmalıdır. Giyilebilir teknolojiler verimliliğe önemli katkılar sunsa da bu cihazların iş ilişkisi kapsamında kullanımı ciddi hukuki ve etik sorunları da beraberinde getirmektedir. Bu cihazlar vücuda doğrudan temas ettiği ve kullanıcıya ait fizyolojik verileri topladığı için, çalışan mahremiyeti açısından önemli riskler barındırmaktadır. Özellikle, geleneksel veri koruma ilkeleri ile uyumluluk konusunda çeşitli güçlükler ortaya çıkmaktadır. Örneğin, yapay zekâ destekli giyilebilir teknolojiler işçilerin farkında olmadıkları sağlık sorunları ya da hamilelik gibi özel durumlarına ilişkin bilgileri açığa çıkarabilir ve işverenler tarafından bu bilgilerin iş akdinin sona erdirilmesi süreçlerinde değerlendirilmesi ihtimali doğabilmektedir[976]. Bu bağlamda giyilebilir cihazların iş ilişkisi kapsamında kullanımı yeniden değerlendirilmelidir. Özellikle ekranı olmayan ve görünmez veri toplayan cihazların, çalışanların bilgilendirilmesi ve rızalarının alınması açısından sorun yaratabileceği dikkate alınmalıdır[977].

Giyilebilir teknolojilerin zorunlu hâle getirildiği iş ilişkilerinde, çalışanların bu cihazları kullanmayı reddetme imkânı büyük ölçüde ortadan kalkmaktadır. Bu durum, işverenin çalışanların anlık konumlarını, fiziksel aktivitelerini ve fizyolojik verilerini izleyebilme kapasitesi ile birleştiğinde, çalışanların sendikal faaliyetler gibi yasal olarak korunan kolektif haklarını kullanma konusunda caydırıcı bir etki yaratma potansiyeline sahiptir[978].

---

[976] Güzel vd., "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", 62; Alp ve Doğan, "Giyilebilir Teknolojiler ve İş İlişkisine Etkileri", 2614 vd.
[977] Ajunwa, "Algorithms at Work", 42-43; Alp ve Doğan, "Giyilebilir Teknolojiler ve İş İlişkisine Etkileri", 2614 vd.
[978] Ajunwa, "Algorithms at Work", 43.

Giyilebilir cihazlardan elde edilen veriler yalnızca iş süreçlerinin yönetimiyle sınırlı kalmamakta, aynı zamanda çalışan sağlığına ilişkin öngörülerde bulunmak için de kullanılmaktadır. Örneğin, bazı işverenler sağlıklı yaşam programlarından elde edilen biyometrik verileri analiz ederek, hangi çalışanların iş kazası geçirme riski taşıdığını tahmin edebilmektedir. Ancak bu tür uygulamalar, çalışanın kilosu, sigara içme alışkanlığı gibi özel hayatına ilişkin bilgileri içeren veri kümeleri üzerinden değerlendirme yapılmasına neden olmakta ve bu durum, ayrımcılık yasağı ilkesi ile çatışma riski doğurmaktadır[979].

4.6.2.8. Sosyal Medya Kullanımına İlişkin Sınırlamalar

İşverenlerin, çalışanların sosyal medya kullanımından kaynaklanabilecek riskleri yönetmek ve hukuki belirsizlikleri ortadan kaldırmak için kapsamlı bir sosyal medya kullanım politikası oluşturması, önemli bir idari tedbirdir. Bu politika, işçi ile işveren arasındaki hukuki denge gözetilerek hazırlanmalıdır.

Genel olarak sosyal medyanın kullanımı, iş ilişkisi kapsamında özel amaçlı internet kullanımı kapsamında değerlendirilebilse de çalışanların sosyal medya platformlarında yaptıkları paylaşımlar bu kapsamdan farklı özellikler göstermektedir. İşçilerin sosyal medya paylaşımları, ifade özgürlüğü, özel hayatın gizliliği ve kişisel verilerin korunması gibi temel hak ve özgürlükler bakımından önemli sonuçlar doğurmaktadır[980]. İş ilişkisi çerçevesinde söz konusu paylaşımların, işverenin meşru menfaatleri, çalışma düzeni ve işçinin sadakat borcu ile dengelenmesi gerekmektedir. İşverenler, işletmenin itibarı, iş sırlarının korunması ve olası hukuki zararların önlenmesi gibi nedenlere dayanarak işçilerin sosyal medya paylaşımlarını denetleyebilecektir[981].

---

[979] Ajunwa, "Algorithms at Work", 51; Alp ve Doğan, "Giyilebilir Teknolojiler ve İş İlişkisine Etkileri", 2624.
[980] Yücel, "İşçilerin Sosyal Medya Paylaşımlarının İşveren Tarafından Denetimi ve İş İlişkisine Etkisi", 25.
[981] Yücel, "İşçilerin Sosyal Medya Paylaşımlarının İşveren Tarafından Denetimi ve İş İlişkisine Etkisi", 80.

İşverenin denetimi açısından günümüz koşullarında sosyal medyanın işyerlerinde tamamen yasaklanması mümkün görünmemektedir[982]. Dolayısıyla işverenlerin, internet erişiminin artık temel bir insan hakkı olarak kabul edildiğine ilişkin tartışmaları da göz önünde bulundurarak, makûl bir internet ve sosyal medya kullanım politikası belirlemesi önem taşımaktadır. İşverenlerin, hukuka aykırı veya işveren açısından risk teşkil eden sosyal medya kullanımını önlemek amacıyla gerekli tedbirleri almasının yanı sıra, çalışanlara belirlenmiş sınırlar içerisinde ve makûl sürelerle internet ve sosyal medya kullanım imkânı tanıması gerekmektedir. Böylece işverenler, çalışanlarının sosyal medya kullanımını hukuka uygun, ölçülü ve şeffaf bir şekilde denetleyebilecektir[983].

İşçilerin sosyal medya kullanımını kontrol etmek veya sınırlamak amacıyla iş sözleşmeleri, toplu iş sözleşmeleri ve iç yönetmelikler gibi hukuki düzenlemelerden yararlanılmakta[984] ayrıca yönetim hakkı kapsamında, işçinin çalışma süresi içerisindeki sosyal medya kullanımına ilişkin sınırlandırmalar getirilebilmektedir[985]. Getirilen sınırlandırmaların hukuki açıdan değerlendirilmesinde, işçinin temel hak ve özgürlükleri ile işverenin yönetim hakkı arasında hassas bir dengenin kurulması önem taşımaktadır.

İşçilerin sosyal medya profilleri işveren tarafından genel bir izleme kapsamına alınmamalıdır. İşverenlerin, çalışanlardan veya iş başvurusunda bulunan adaylardan sosyal ağlarda başkalarıyla paylaştıkları bilgilere erişim talep etmekten kaçınması gerekmektedir[986]. Ayrıca işveren tarafından sağlanan veya yönetilen sosyal medya hesaplarını kullanma zorunluluğu çalışanlara dayatılmamalıdır. Görevleri itibarıyla sosyal medya kullanımı gerekli olan çalışanlar açısından (örneğin işyerinin resmi sözcüsü gibi), işle ilgili olmayan ve kamuya kapalı (özel) bir sosyal medya profilini

---

[982] Özdemir, "İnternet ve İş Sözleşmesi: Yeni Teknolojilerin İş İlişkisine Etkileri Üzerine", 19; Bozkurt Gümrükçüoğlu, "İşçinin Sosyal Medya Kullanımının İş Hukukundaki Etkileri", 375.
[983] Bozkurt Gümrükçüoğlu, "İşçinin Sosyal Medya Kullanımının İş Hukukundaki Etkileri", 375.
[984] Aslı Çalışkan Yıldırım ve Ömer Uğur, "İşveren Bakımından Fesih Sebebi Olarak İşçinin Sosyal Medya Kullanımları", *İstanbul Hukuk Mecmuası* 80, sy 4 (2022): 1174.
[985] Uncular, "Giriş Kontrol Sistemleri, Yer Belirleme Sistemleri ve Sosyal Medya Vasıtasıyla İzleme", 1684.
[986] Ayrıntılı bilgi için bknz. Gizem Sarıbay Öztürk, "İşverenin İşçileri ve Adayları Sosyal Medya Vasıtasıyla Araştırması", içinde *İş Hukukunda Yeni Yaklaşımlar IV.*, ed. Kübra Doğan Yenisey ve Seda Ergüneş Emrağ (On İki Levha Yayıncılık, 2021), 1-108.

kullanabilme seçeneği açıkça tanınmalı ve bu husus, iş sözleşmesinde net şekilde düzenlenmelidir[987].

İş sözleşmesi yoluyla sosyal medya kullanımına yönelik getirilen sınırlamalar, Türk Borçlar Kanunu'nun 27. maddesinde öngörülen *"kanunun emredici hükümlerine, ahlaka, kamu düzenine ve kişilik haklarına aykırılık"* ölçütüne uygun olmak zorundadır. Aynı şekilde işçinin, yönetim hakkı kapsamında getirilen bu sınırlamalara dürüstlük kuralının öngördüğü ölçüde uyması beklenmektedir[988].

İşçinin sosyal medya paylaşımlarının hukuka aykırı yöntemlerle elde edilmesi veya iş sözleşmesinin feshini gerektirecek ağırlıkta bulunmaması hâlinde, bu paylaşımlar iş sözleşmesinin feshinde geçerli bir neden oluşturmayacaktır[989]. Nitekim yargı kararları incelendiğinde, işveren veya işletmeyi hedef alan, itibar zedeleyici, hakaret içerikli veya iş sırlarını ifşa eden sosyal medya paylaşımlarının, iş sözleşmesinin haklı ya da geçerli nedenle feshine yol açabileceği görülmektedir[990]. Bu doğrultuda, çalışanların sosyal medya kullanımlarında özenli davranmaları ve sadakat borcunun gerekliliklerine uygun hareket etmeleri büyük önem taşımaktadır.

4.6.2.9. Sertifikasyon Sistemleri

Genel Veri Koruma Tüzüğü, veri koruma süreçlerinde şeffaflığın artırılması ve GDPR'a uygunluğun sağlanması açısından sertifikasyon mekanizmalarını, veri koruma mühürlerini ve işaretlerini temel araçlar olarak değerlendirmektedir[991]. Sertifikasyon sistemleri, bağımsız ve uzman kuruluşlar aracılığıyla kurumların ürün, hizmet ve kişisel veri işleme faaliyetlerinin belirlenen standartlara uyumunu denetleyip belgelendirme işlevini yerine getirmektedir[992] Bu sistemler, veri

---

[987] Falque-Pierrotin, Opinion 2/2017 on Data Processing at Work, 12.
[988] Çalışkan Yıldırım ve Uğur, "İşveren bakımından fesih sebebi olarak işçinin sosyal medya kullanımları", 1174-75.
[989] Ayrıntılı bilgi için bknz. Fatih Aydın, "İşçinin Sosyal Medya Paylaşımlarının İş Sözleşmesinin Feshine Etkisi" (Doktora Tezi, T.C. Erciyes Üniversitesi, 2022); Yiğit, "Yargı Kararları Işığında İşçinin Sosyal Medya Paylaşımı Nedeniyle İş Sözleşmesinin İşverence Feshinin Koşulları", 975 vd.
[990] Ayrıntılar için bknz. Hediye Ergin, "Sosyal Medya Paylaşımlarıyla İşverenin İtibarını Zedeleyen İşçinin İş Sözleşmesinin Feshi", *Sicil İş Hukuku Dergisi* 1, sy 49 (2023): 45-59.
[991] Rowena Rodrigues vd., "The Future of Privacy Certification in Europe: An Exploration of Options Under Article 42 of the GDPR", *International Review of Law, Computers & Technology* 30, sy 3 (2016): 253, https://doi.org/10.1080/13600869.2016.1189737.
[992] Rodrigues vd., "The Future of Privacy Certification in Europe", 254.

sorumlularına hukuki uyum açısından güvence sunarken, veri sahiplerinin şeffaflık, hesap verebilirlik ve güven beklentilerini karşılamayı hedeflemektedir[993]. Böylelikle, veri sahipleri kullandıkları ürün ve hizmetlerin veri koruma seviyelerini kolaylıkla değerlendirebilirler. Bu kapsamda, sertifikasyon mekanizması yalnızca nihai sonuç odaklı değil; kişisel verilerin korunmasına ilişkin tüm işleme faaliyetlerinin ve bu faaliyetlerin uygulama süreçlerinin bütüncül bir yaklaşımla denetlenip belgelendirilmesine olanak sağlayan bir yapı sunmaktadır[994].

Avrupa Birliği Yapay Zekâ Tüzüğü de benzer bir yaklaşımla yüksek risk taşıyan yapay zekâ sistemlerinin piyasaya sürülmeden önce hukuka uygunluğunu kontrol eden bir değerlendirme prosedürü getirmiştir. GDPR'daki sertifikasyona benzeyen bu değerlendirme, yapay zekâ sistemlerinin risk yönetimi, veri kalitesi, şeffaflık, insan denetimi, olay kayıtları, dayanıklılık ve güvenlik gibi özelliklerinin bağımsız olarak incelenmesini sağlamaktadır. Bazı durumlarda işverenler bu kontrolleri kendileri yapabilir, ancak yüksek riskli sistemlerin çoğunda bağımsız dış kuruluşlar tarafından denetim zorunludur. Denetimler sonucunda, sistemlerin uygunluğu belgelenmekte ve güvenli olduğunu gösteren CE işareti ile piyasaya sunulmaktadır[995]. Bu kapsamda işverenler, kullandıkları yapay zekâ sistemlerinin GDPR ve AI Act düzenlemelerine uygunluğunu sağlamak için gerekli kontrolleri yaptırmalı ve bağımsız değerlendirme süreçlerine katılmalıdırlar.

4.7. Üçüncü Kişilerin Kişisel Verilerinin Korunması

Tele çalışma modelinde, işverenlerin çalışanlarını izleme ve gözetleme faaliyetleri sırasında, yalnızca çalışanlara ait kişisel verilerin değil, aynı zamanda çalışanla aynı ortamı paylaşan aile bireyleri, ev ziyaretçileri veya çalışanın iletişim kurduğu müşteriler, tedarikçiler gibi üçüncü kişilere ait kişisel verilerin de tesadüfen veya dolaylı olarak işlenmesi gündeme gelebilmektedir. Örneğin, bir video konferans kaydında çalışanın arka planında aile üyelerinin görünmesi, ekran paylaşımlarında üçüncü kişilere ait e-posta veya belgelerin görüntülenmesi ya da sesli izleme sırasında ortamdaki diğer kişilerin konuşmalarının kaydedilmesi bu duruma örnek teşkil

[993] Rodrigues vd., "The Future of Privacy Certification in Europe", 249.
[994] Rodrigues vd., "The Future of Privacy Certification in Europe", 253.
[995] Voigt ve Hullen, *The EU AI Act*, 151-61.

edebilmektedir. İşverenler, veri sorumlusu sıfatıyla, bu şekilde işledikleri üçüncü kişilere ait kişisel verilerin korunmasından da KVKK ve GDPR hükümleri uyarınca sorumluluk taşımaktadır. Bu nedenle, üçüncü kişilerin kişisel verilerinin işlenmesinin hukuka uygunluk şartlarının değerlendirilmesi ve bu verilerin yetkisiz işlenmesine karşı gerekli teknik ve idari tedbirlerin alınması büyük önem taşımaktadır.

4.7.1. Üçüncü Kişinin Verilerinin İşlenmesinin Hukuka Uygunluğu

Üçüncü kişilere ait kişisel verilerin, çalışan izleme faaliyetleri kapsamında işlenmesinin hukuka uygun kabul edilebilmesi için öncelikle geçerli bir hukuka uygunluk sebebinin bulunmalıdır. Tele çalışma modelinde üçüncü kişilere ait verilerin tesadüfen toplanması durumunda, bu işlemenin hukuki dayanağını bulmak genellikle zordur. İzleme sırasında tesadüfen verisi işlenebilecek tüm üçüncü kişilerden (örneğin, çalışanın ev halkı) önceden açık rıza alınması pratik olarak mümkün olmamakta ve iş ilişkisinin doğasıyla bağdaşmamaktadır. İşveren, işletme güvenliği, iş sürekliliği veya çalışan performansının denetlenmesi gibi meşru menfaatlerini gerekçe gösterebilmektedir. Ancak, bu meşru menfaatin, verisi işlenen üçüncü kişinin temel hak ve özgürlükleri (özellikle özel hayatın gizliliği hakkı) karşısında dikkatli bir denge testinden geçirilmesi zorunludur. Üçüncü kişinin verilerinin işlenmesinin bu meşru amaca ulaşmak için kesinlikle "gerekli" ve "orantılı" olması şart koşulmaktadır[996]. Örneğin, bir güvenlik kamerası kaydında arka planda beliren bir aile üyesinin görüntüsünün sürekli saklanması, meşru menfaatle orantılı bir uygulama teşkil etmemektedir. Kanunlarda açıkça öngörülme, sözleşmenin ifası veya hukuki yükümlülüğün yerine getirilmesi gibi diğer hukuki sebepler, genellikle çalışan izleme sırasında tesadüfen toplanan üçüncü kişi verileri için doğrudan bir dayanak oluşturmamaktadır. Bu nedenlerle, üçüncü kişi verilerinin işlenmesinde temel ilke, bu tür verilerin toplanmasından mümkün olduğunca kaçınılmasıdır.

KVKK'nın 4. maddesinin 2. fıkrasının (ç) bendi ve GDPR'ın 5. maddesinin 1. fıkrasının (c) bendi uyarınca veri minimizasyonu ilkesi, yalnızca çalışanlara ait değil, aynı zamanda tesadüfen toplanabilecek üçüncü kişilere ait veriler için de geçerlidir.

---

[996] Gürsel, *İşçinin Kişisel Verilerinin Korunması Hakkı*, 215-16; Küzeci, *Kişisel Verilerin Korunması Hukuku*, 213-19; Yiğit, *İş İlişkisinde Kişisel Verilerin Korunması*, 21; Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 152.

İşveren, izleme faaliyetlerini tasarlarken ve uygularken üçüncü kişilerin mahremiyetini ihlal etme riskini en aza indirecek şekilde hareket etmelidir[997]. Aydınlatma yükümlülüğü bağlamında ise, işverenler en azından çalışanlarını, izleme sırasında üçüncü kişilere ait verilerin tesadüfen toplanabileceği riski ve bu riski azaltmak için (örneğin, kamera açısını ayarlama, özel görüşmeler için ayrı bir alan kullanma) alabilecekleri önlemler konusunda bilgilendirmelidir.

4.7.2. Üçüncü Kişilerin Verilerinin İşlenmesinde Teknik ve İdari Tedbirler

İşverenler, tele çalışma modelinde üçüncü kişilere ait kişisel verilerin hukuka aykırı olarak işlenmesini önlemek veya bu riski en aza indirmek için hem idari hem de teknik düzeyde çeşitli tedbirler almalıdır. Bu, çalışanın ev ortamındaki üçüncü kişilerin veya özel eşyaların görünmesini engellemektedir. Gelişmiş gürültü engelleme teknolojileri, ortamdaki diğer konuşmaları veya sesleri filtreleyerek sadece çalışanın sesine odaklanılmasına yardımcı olabilmektedir. Eğer video veya ses kayıtları yapılıyorsa ve bu kayıtlarda üçüncü kişiler yer alıyorsa, bu kayıtların saklanmasından veya daha fazla işlenmesinden önce üçüncü kişilere ait görüntü veya seslerin otomatik veya manuel olarak bulanıklaştırılması, mozaiklenmesi veya silinmesi için teknik imkanlar kullanılmalıdır[998]. Ev veya kamuya açık alanlar gibi görüntü ya da ses kaydı alınması durumunda, üçüncü kişilere ait yüz, ses veya diğer belirlenebilir özelliklerin mozaiklenmesi ya da silinmesi yoluyla anonimleştirilmesi gerekmektedir[999]. İzleme yazılımları, sadece iş görme edimiyle doğrudan ilgili ve kesinlikle gerekli olan veri türlerini toplayacak şekilde yapılandırılmalıdır. Örneğin, ekran kaydı yapılıyorsa, bu kayıt yalnızca belirli uygulamalar veya pencerelerle sınırlandırılabilmekte; mikrofon kaydı gerekiyorsa, bu da yalnızca belirli iş görüşmeleri sırasında aktif hâle

---

[997] Bozkurt Gümrükçüoğlu ve Savaş Kutsal, "Uzaktan Çalışma", 11; Akın, "Türk Çalışma Yaşamında Pandemi Sürecinde Uzaktan/Evden Çalışma ve Olası Sonuçları", 279; Bozkurt Gümrükçüoğlu, "COVID-19 Pandemi Döneminde Home-Office", 200-201; Dulay Yangın, "Bilgi ve İletişim Teknolojilerinde Yaşanan Gelişimin İş Hukuku Üzerindeki Etkileri: Tele Çalışmaya İlişkin Tespit ve Öneriler", 253; Ünal Adınır, "Tele çalışmada verilerin korunması", 971.

[998] Hongbo Zhang vd., *Artificial Intelligence for Privacy Conservation in Remote Learning*, MT Open Press, Middle Tennessee State University, https://openpress.mtsu.edu, 31 Ocak 2023, https://mtsu.pressbooks.pub/privacyandsafetyinonlinelearning/chapter/artificial-intelligence-for-privacy-conservation-in-remote-learning/.

[999] Kathleen Morrison, "Is It Legal to Record Video Meetings?", Lexology, 19 Ağustos 2020, https://www.lexology.com/library/detail.aspx?g=1d582939-2279-42cb-9892-ae088c2f9396.

getirilebilmektedir[1000]. Tesadüfen toplanan ve saklanması gerekmeyen üçüncü kişi verilerinin geri getirilemeyecek şekilde silinmesini sağlayan güvenli silme araçları ve prosedürleri uygulanmalıdır. Bu teknik tedbirlerin etkinliği, aynı zamanda idari bir tedbir olan çalışanların eğitilmesine ve bu araçları (örneğin, sanal arka plan özelliğini) doğru ve tutarlı bir şekilde kullanmaları konusunda bilinçlendirilmesine bağlıdır[1001]. İşverenin tele çalışma politikasında bu konuya özel bir bölüm ayırması, bu riskin yönetiminde kritik rol oynamaktadır.

Sonuç olarak, tele çalışma modelinde üçüncü kişilerin kişisel verilerinin korunması, işverenlerin etkin bir şekilde risk değerlendirmesi yapmasını, veri minimizasyonu ve ölçülülük ilkelerini titizlikle uygulamasını ve hem çalışanları bu konuda bilinçlendirmesini hem de uygun teknik ve idari tedbirleri hayata geçirmesini gerektiren önemli bir sorumluluktur. Bu tedbirler hem yasal uyumluluğun sağlanması hem de tüm bireylerin mahremiyet haklarına saygı gösterilmesi açısından kritik öneme sahiptir.

[1000] European Data Protection Board (EDPB), *Guidelines 3/2019 on Processing of Personal Data Through Video Devices*, 10-11.

[1001] Ayrıntılı bilgi için bknz. Kişisel Verileri Koruma Kurumu, *Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)* (2018), 8; Mahlangu ve Schutte, "Analysing Information Technology Risks Affecting South African Government Employers Due to Remote Working", 53; Altıntaş ve Barkuş, "Dijital Ortamlarda Kişisel Veri Güvenliği Kavramı Üzerine Bir Derleme Çalışması", 47; Chukwudi Tabitha Aghaunor vd., "Data Security Strategies to Avoid Data Breaches in Modern Information Systems", 2122.

BÖLÜM V

SONUÇ VE DEĞERLENDİRME

Dijitalleşmeyle birlikte çalışma yaşamının merkezine yerleşen tele çalışma, getirdiği esneklik ve verimlilikle birlikte, işverenin yönetim hakkı ile çalışanın kişisel verilerinin korunması hakkı arasındaki dengeyi en tartışmalı hukuki sorunlardan biri hâline getirmiştir. Bu bağlamda, tele çalışma pratiklerinde kullanılan izleme ve gözetleme teknolojileri, işverenin denetim kapasitesini niceliksel ve niteliksel olarak dönüştürerek farklı bir seviyeye taşımıştır. Klasik kamera ve konum takibi gibi yöntemlerin ötesinde, nesnelerin interneti, giyilebilir teknolojiler, nöroteknoloji ve özellikle yapay zekâ destekli sistemler, işverenlere yalnızca çalışanın performansını değil; davranışlarını, alışkanlıklarını ve hatta zihinsel süreçlerini dahi analiz etme imkânı tanımaktadır. Dahası, bu teknolojiler, "profilleme" yoluyla hassas olmayan verilerden yola çıkarak bireyin siyasi görüşü, felsefi inancı veya sağlık durumu hakkında son derece hassas yeni bilgiler türetme kapasitesine de sahiptir. Bu teknolojiler bir yandan verimliliği artırma, iş süreçlerini kontrol etme, iş sağlığı ve güvenliğini sağlama gibi meşru amaçlara hizmet etme hedefi taşırken, diğer yandan çalışan üzerinde sürekli bir baskı yaratan, görünmez bir "dijital panoptikon" etkisi doğurmaktadır. Bu durum izleme ve gözetlemenin çalışanın en mahrem alanı olan konutuna kadar uzanmasına zemin hazırlayarak, özel hayatın gizliliğini ihlal riskini daha da derinleştirmektedir.

Çalışmamızda izleme ve gözetleme teknolojilerinin iş ilişkisi kapsamındaki kullanımının hukuki sınırları, özellikle Kişisel Verilerin Korunması Kanunu ve AB Genel Veri Koruma Tüzüğü temelinde analiz edilmiştir. Ayrıca seçilen bazı örnek ülkelerdeki mevzuat ile uygulama sorunları karşılaştırmalı hukuk yöntemi ile incelenmiştir. Bu çerçevede, veri koruma mevzuatının amaçla sınırlılık, ölçülülük ve veri minimizasyonu gibi temel ilkeleri ile hukuka uygunluk şartlarının bu yeni nesil izleme araçları karşısında önemli bir hukuki kalkan görevi görmekle birlikte ülkemizde hâlen yeterli olmadığı sonucuna ulaşılmıştır. Bu yetersizliğin temelinde,

KVKK ve ilham aldığı düzenlemelerin, verilerin basitçe "toplandığı, analiz edildiği ve uygulandığı" daha eski bir anlayış üzerine inşa edilmiş olması yatmaktadır. Oysaki modern yapay zekâ, görünüşte anonimleştirilmiş verilerin dahi yeniden kimliklendirilmesi veya gruplar üzerinde ayrımcılık yaratacak profiller oluşturulması gibi, bu çerçevenin öngörmekte zorlandığı yeni riskler doğurmaktadır. İşveren ve çalışan arasındaki güç dengesizliği nedeniyle, çalışanın kişisel verilerinin işlenmesine yönelik verdiği "açık rıza", çoğu zaman gerçek anlamda özgür iradeyi yansıtmamaktadır. Benzer biçimde, kişisel verilerin işlenmesinde hukuka uygunluk gerekçelerinden biri olan işverenin "meşru menfaati" de açık ve net şekilde tanımlanmadığı takdirde çalışanın hak ihlallerine yol açabilmektedir. Ayrıca ifade etmek gerekir ki, ülkemizde tele çalışmaya ilişkin mevzuat bu çalışma biçiminin kendine özgü sorunlarını giderebilecek nitelikte değildir. Tele çalışma süreçlerinde işçinin kişisel verilerinin korunması ise düzenlenmemiştir. Daha önce de ifade edildiği üzere tele çalışmada izleme ve gözetleme teknolojileri yapay zekâ ile farklı bir boyut kazanmıştır. Ancak yapay zekânın bu alandaki kullanımına ilişkin olarak henüz yasal bir düzenleme getirilmemiştir. Sonuç olarak, mevcut yasal çerçevenin, teknolojinin dönüştürücü hızına ayak uydurmakta zorlandığı ve tele çalışmanın getirdiği özgün mahremiyet sorunlarına spesifik cevaplar üretmekte yetersiz kaldığı tespit edilmiştir. Bu tespitler doğrultusunda tele çalışma modelinde insan onuruna yaraşır ve hukuki güvence altına alınmış bir çalışma düzeni tesis etmenin en ideal yolu kanaatimizce lex specialis (özel kanun) niteliğinde bir düzenleme getirilmesidir. Mukayeseli hukukta da bu yönde bir eğilim gözlenmektedir. Zira çalışmamızda değindiğimiz üzere Yunanistan'ın web kamerası ile performans izlemeyi doğrudan yasaklaması ve Bulgaristan'ın algoritmik yönetim sistemlerine insan denetimi zorunluluğu getirmesi, bu alanda özel düzenlemelerin gerekliliğini ortaya koymaktadır.

Kanaatimizce getirilecek yeni düzenleme hem işverenlerin meşru menfaatlerini koruyacak hem de çalışanların mahremiyet alanına yönelik keyfi ve ölçüsüz müdahaleleri engelleyecek öngörülebilir bir zemin sunmalıdır. Bu bakımdan ifade edilmesi gerekir ki, gelişen teknolojiler bakımından hukukun asli görevi detaylı teknik düzenlemeler yapmak ya da yasaklama getirmek değil, kullanımından doğan zararları önlemek ve ortaya çıkan hak ihlallerini gidermek olduğudur. Zira gelinen noktada teknolojinin kullanımının tümden sınırlanması ya da yasaklanması mümkün olmadığı gibi makûl de değildir. Gerektiğinde menfaatler arasındaki denge gözetilerek keskin

sınırlamalar getirilmesi gerektiğinde ise sınırlı izin verilmesi isabetli olacaktır. Bu kapsamda getirilmesi önerilen düzenlemenin, Avrupa Birliği Yapay Zekâ Tüzüğü'nde benimsenen risk temelli yaklaşımı model alması, etkin bir koruma sağlaması ve önleyici etkisi değerlendirildiğinde yararlı olabilecektir. Kanaatimizce izleme ve gözetleme teknolojileri de doğurdukları mahremiyet riskine göre sınıflandırılmalıdır. Buna göre, çalışanın özel hayat alanında sürekli ve kesintisiz video veya ses kaydı yapılması, çalışanın rızası dışında biyometrik veriler veya nöroteknolojik veriler aracılığıyla duygu veya niyet analizi yapılması gibi insan onuruna ve temel hakların özüne dokunan uygulamaların "kabul edilemez risk" kategorisinde değerlendirilerek açıkça ve kesin olarak yasaklandığı bir "kara liste" oluşturulmalıdır. Buna karşılık, klavye hareketlerinin kaydedilmesi veya yapay zekâ ile sürekli performans puanlaması gibi yöntemler "yüksek riskli" olarak tanımlanmalı ve kullanımları; işin doğası gereği mutlak zorunluluk bulunması, daha az müdahaleci bir yöntemin olmaması ve veri koruma etki değerlendirmesinin zorunlu olarak yapılması gibi katı şartlara bağlanarak "gri liste" olarak düzenlenmelidir. Bu gibi listeler oluşturulurken kullanılan izleme ve gözetleme aracının amacının meşruluğu ile amaçla sınırlı kalıp kalmadığı ve işçi üzerindeki etkileri bir arada değerlendirilmelidir.

İş hukukunun ortaya çıkış nedeni sözleşme tarafları arasındaki güç dengesizliğidir. Bu dengenin sağlanabilmesi ise ancak katılımcı modellerle sağlanabilir. Özellikle tele çalışmada kullanılan yüksek riskli izleme ve gözetim teknolojileri, katılımcı karar alma süreçlerinin tesis edilmesini zorunlu kılmaktadır. Bu bağlamda, kolektif bir denetim ve rıza mekanizmasının kurulması, iş hukukunun koruyucu ve dengeleyici işleviyle de örtüşmektedir. Kolektif bir denetim ve rıza mekanizmasının tesisi bakımından, mukayeseli hukukta öne çıkan bazı modellerden yararlanılması mümkündür. Nitekim, Alman Hukukunda işçi temsilciliğinin (Betriebsrat), teknik izleme araçlarının kurulumu konusunda ortak karar yetkisine sahip olduğu görülmektedir. Benzer şekilde, Fransız Hukukunda bu tür sistemlerin uygulanmasından önce Sosyal ve Ekonomik Komite'ye bildirim ve görüş alma zorunluluğu öngörülmüştür. Türkiye'de de benzer bir yapının tesisi, kanaatimizce yüksek riskli teknolojilerin keyfi kullanımını önleyecektir. Ancak belirtelim ki, ülkemizde katılımcı model ihtiyacı konumuzla sınırlı değildir. Zira öğretideki eleştirilere rağmen çalışanların iş ilişkisi çerçevesinde alınan kararlara katılımını tesis eden bir model hâlihazırda söz konusu değildir.

Hazırlanacak yeni mevzuatın yalnızca yasak ve sınırlamaları değil, aynı zamanda çalışanların dijital çağdaki haklarını güçlendiren pozitif yükümlülükleri de içermesi gerekmektedir. Zira gerek tele çalışma gerekse diğer esnek çalışma biçimleri açısından henüz dijitalleşmenin doğurduğu yeni risk alanlarına yönelik bütüncül bir normatif çerçeve oluşturulmamıştır. Bu bağlamda, dikkat çeken bazı temel eksiklikler doğrudan çalışma konumuzla da ilişkilidir. Örneğin, yalnızca çalışma süresinin sınırlandırılması değil; dijital ortamda çalışan davranışlarını sürekli izleyen sistemlerin şeffaf ve denetlenebilir hâle getirilmesi de temel bir gerekliliktir. Bu gereklilik, tele çalışma modelinde daha da belirgindir. Fransa, İtalya ve İspanya gibi Avrupa ülkelerinde açıkça düzenlenen "ulaşılabilir olmama hakkı" (right to disconnect), Türk hukukunda da açık, bağlayıcı ve uygulanabilir şekilde yasal güvence altına alınmalıdır. Düzenleme eksikliğinin söz konusu olduğu bir diğer önemli alan "algoritmik yönetim sistemleri"dir. Bu bağlamda, algoritmik yönetim sistemlerinin şeffaflığının ve hesap verebilirliğinin sağlanması bakımından çalışanların bilgi edinme hakkının kapsamı genişletilmeli ve işverenlerin aydınlatma yükümlülüğü daha açık ve net bir biçimde düzenlenmelidir. Ayrıca Genel Veri Korumu Tüzüğü 22. maddesi ve Avrupa Birliği Yapay Zekâ Tüzüğü 14. maddesi ile uyumlu olarak, otomatik sistemlerin ürettiği kararlara karşı, bu kararı değiştirme yetkisine sahip bir yetkilinin "anlamlı insan müdahalesi" (meaningful human intervention) zorunlu kılınmalıdır. Bu hak, çalışana yalnızca karara itiraz etme imkânı vermekle kalmamalı, aynı zamanda kararın mantığını anlamasını sağlayacak "alternatif senaryo açıklamaları" gibi somut bilgiler talep etme yetkisini de kapsamalıdır. Otomatik karar alma süreçlerine ilişkin düzenlemelerde, bireylerin yalnızca bu kararların sonuçlarına itiraz etme hakkı ile yetinilmemeli; aynı zamanda, GDPR'a paralel şekilde doğrudan bu tür karar alma mekanizmalarına tabi tutulmama hakları da açık, bağlayıcı ve uygulanabilir biçimde hukuki güvence altına alınmalıdır.

Kapsamlı bir yasal reform süreci zaman alacağından, Kişisel Verileri Koruma Kurulu'nun mevcut yetkileri çerçevesinde proaktif bir rol üstlenmesi de büyük önem taşımaktadır. Kanaatimizce Kurul, Birleşik Krallık Bilgi Komiserliği Ofisi'nin yaptığı gibi, tele çalışmada izleme ve gözetleme uygulamalarına ilişkin detaylı bir rehber yayımlamalıdır. Bu rehber, uygulamada karşılaşılan belirsizlikleri gidererek ve işverenler ile çalışanlar için önemli bir yol gösterici olacaktır. Ayrıca Kurul, alacağı ilke kararlarıyla, tele çalışanın mahremiyet alanına müdahale içeren durumlarda

işverenin “meşru menfaat” hukuka uygunluk sebebini son derece dar yorumlamalı ve ölçülülük denetiminde ispat yükünü ağırlaştırmalıdır. Bu yaklaşım, yasal düzenleme yapılana kadar geçecek sürede, mevcut normların çalışan lehine yorumlanarak temel hakların daha etkin korunmasını sağlayacaktır.

Son olarak, işverenin tele çalışma modelindeki izleme ve gözetleme faaliyetlerine ilişkin temel sorumluluğu, tepkisel önlemler almak yerine, “gizliliğin tasarım aşamasından itibaren gözetilmesi ve başlangıçtan itibaren gizliliği esas alan yapılandırma” (privacy by design and by default) ilkesini benimseyerek proaktif ve bütüncül bir hukuki çerçeve tesis etmektir. Bu felsefenin en somut yansıması, tüm izleme faaliyetlerinin hukuki zeminini, sınırlarını ve usullerini belirleyen açık, anlaşılır ve şeffaf bir “tele çalışma ve izleme politikası” oluşturulmasıdır. Bu politika; izlemenin meşru amacını ve hukuki dayanağını, hangi verilerin hangi yöntemle ve ne kadar süreyle işleneceğini, toplanan verilere kimlerin “en az yetki prensibi” dâhilinde erişebileceğini ve çalışanların haklarını nasıl kullanacağını net bir şekilde tanımlamalıdır. Bu politikanın etkinliği ise güçlü teknik ve idari tedbirlerle desteklenmesine bağlıdır. Teknik düzeyde; kurumsal ağa erişimde sanal özel ağ ve çok faktörlü kimlik doğrulama gibi güvenli kimlik doğrulama yöntemlerinin zorunlu kılınması hem aktarım hem de durağan hâldeki verilerin şifrelenmesi ve özellikle “kendi cihazını getir” senaryolarında kurumsal verilerle kişisel verilerin ayrıştırılması kritik öneme sahiptir. Kanaatimizce işverenlere bu yönde bir politika oluşturma yükümlülüğünün de yasal düzenleme ile getirilmesi isabetli olacaktır. İdari tedbirler bakımından ise, her yeni ve müdahaleci izleme teknolojisi için proaktif bir veri koruma etki değerlendirmesi yapılması, çalışanlara düzenli olarak veri güvenliği ve mahremiyet eğitimleri verilmesi ve özellikle yapay zekâ tabanlı otomatik karar verme süreçlerinde, algoritmanın ürettiği sonuçların nihai olmadan önce mutlaka “anlamlı bir insan gözetiminden” geçirilmesi, adil, hesap verebilir ve hukuka uygun bir sistemin temel taşlarını oluşturur.

Netice itibarıyla, tele çalışmada izleme ve gözetleme teknolojileri, doğru ve ölçülü kullanıldığında iş süreçlerine katkı sağlayabilecek araçlardır. Ancak bu teknolojilerin denetimsiz ve sınırsız bir şekilde uygulanması, çalışma yaşamını insan onurunu zedeleyen, sürekli bir gözetim rejimine dönüştürme riski taşımaktadır. Teknolojinin insana hizmet etmesi ilkesinden hareketle, bu alanda temel hakları merkeze alan,

şeffaf, hesap verebilir ve öngörülebilir bir hukuki çerçevenin ivedilikle tesis edilmesi, yalnızca çalışanların değil, aynı zamanda adil ve sürdürülebilir bir dijital toplumun geleceği için bir zorunluluktur.

REFERANSLAR

"A Strong Password and the Importance of MFA to Protect Your Data - Cakemail Blog". Erişim 05 Haziran 2025. https://www.cakemail.com/blog/post/a-strong-password-and-the-importance-of-mfa-to-protect-your-data.

Abbadini, Marco. "Sandboxing and Data Protection in Cloud Computing Environments". Doktora Tezi, UNIVERSITY OF BERGAMO, 2025. https://tesidottorato.depositolegale.it/bitstream/20.500.14242/209385/1/Abbadini_Marco_1048650_PhD_Thesis_rev.pdf.

Abudureyimu, Yiliyaer, ve Yucel Ogurlur. "Yapay Zekâ Uygulamalarının Kişisel Verilerin Korumasına Dair Doğurabileceği Sorunlar ve Çözüm Önerileri". İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi 20, sy 41 (2021): 765-82.

Acar Ünal, Özlem. "Veri Sorumlusunun Aydınlatma Yükümlülüğü". Banka ve Finans Hukuku Dergisi 8, sy 32 (2019): 1325-78.

Ackerman, Evan, ve Eliza Strickland. "Neurotechnology and Emotional AI Are Creating a New Kind of Line Manager". IEEE Spectrum, 19 Kasım 2022. https://www.bps.org.uk/psychologist/neurotechnology-and-emotional-ai-are-creating-new-kind-line-manager.

ActivTrak. "ActivTrak: Work Wiser with Workforce Analytics & Productivity Insights". Erişim 27 Şubat 2025. https://www.activtrak.com/.

Adame, David. "Managing and Securing Endpoints: A Solution for a Telework Environment". Master's project, California State University, 2021. https://scholarworks.lib.csusb.edu/etd/1316.

Adams-Prassl, Jeremias, Halefom Abraha, Aislinn Kelly-Lyth, Michael 'Six' Silberman, ve Sangh Rakshita. "Regulating Algorithmic Management: A Blueprint". European Labour Law Journal 14, sy 2 (2023): 124-51.

Adams-Prasslt, Jeremias. "What If Your Boss Was An Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work". Comp. Lab. L. & Pol'y J. 41, sy 123 (2019): 123-46.

Ahmed, Aliyu Aminu, ve Rukayya Aminu Muhammed. "Accessibility, Use and Effectiveness of Neurotechnology Devices for Improved Productivity in Workplace". International Journal of Scientific and Research Publications (IJSRP) 11, sy 10 (2021): 15-22.

Ajax Systems. "NVR vs. DVR: Understanding the Key Differences | Blog Ajax". 30 Eylül 2024. https://ajax.systems/blog/nvr-vs-dvr-key-differences/.

Ajunwa, Ifeoma. “Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law”. Louis ULJ 63, sy 21 (2018).

Ajunwa, Ifeoma, Kate Crawford, ve Jason Schultz. “Limitless Worker Surveillance”. California Law Review 105, sy 3 (2017): 735-76.

Akgül, Aydın. Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması. Beta Basım Yayım Dağıtım Yayınları, 2014.

Akgül, Aydın. Kişisel Verilerin Korunması. Beta, 2014.

Akın, Levent. “İş Kazalarından Doğan Hukuksal Sorumlulukta Uygun Nedensellik Bağı”. TMMOB İnşaat Mühendisleri Odası Ankara Şubesi, İş Sağlığı ve Güvenliği Sempozyumu Bildiriler Kitabı, Ankara, 2007, 63-76.

Akın, Levent. “Türk Çalışma Yaşamında Pandemi Sürecinde Uzaktan/Evden Çalışma ve Olası Sonuçları”. Otto Kaufmann Armağanı (Ed. Hekimler, A.), 2021, 261-300.

Akıncı, Ayşe Nur. Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Getirdiği Yenilikler Ve Türk Hukuku Bakımından Değerlendirilmesi. T.C. Kalkınma Bakanlığı, 2017.

Akipek, Jale, Turgut Akıntürk, ve Derya Ateş. Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku. 16. Beta Basım Yayım Dağıtım Yayınları, 2020.

Aksoy, Hüseyin Can. “Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme”. Kişisel Verileri Koruma Dergisi 4, sy 2 (2022): 2.

Aktaş, Ece. “Dijital Çalışma Bakımından Ulaşılamama Hakkı”. Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 1, sy 22 (2025): 1-48.

Akyiğit, Ercan. İş Hukuku. 15. bs. Seçkin, 2024.

Alfaleh, Amjad, Abdullah Alkattan, Alaa Alageel, vd. “Onsite Versus Remote Working: The Impact on Satisfaction, Productivity, and Performance of Medical Call Center Workers”. INQUIRY: The Journal of Health Care Organization, Provision, and Financing 58 (Ocak 2021). https://journals.sagepub.com/doi/10.1177/00469580211056041.

Alfar, İnci. “6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Veri İşleme Sözleşmeleri”. Doktora Tezi, Dokuz Eylül Üniversitesi, 2024.

Algawi, Asaf, Michael Kiperberg, Roee Leon, Amit Resh, ve Nezer Jacob Zaidenberg. “Efficient Protection for VDI Workstations”. IEEE, Haziran 2019, 169-72. https://ieeexplore.ieee.org/document/8854034/.

Aloisi, Antonio, ve Valerio De Stefano. “Essential Jobs, Remote Work and Digital Surveillance: Addressing the COVID-19 Pandemic Panopticon”. International Labour Review 161, sy 2 (2022): 289-314.

Aloisi, Antonio, ve Elena Gramano. “Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context”. Special Issue of Comparative Labor Law & Policy Journal 41, sy 1 (2019): 95-121.

Alp, Mustafa. “Corona Günlerinde Uzaktan (Evden) Çalışma, Telafi Çalışması ve Ücret İndirimi”. İçinde Pandemi Sürecinde İş Hukuku, editör Gülsevil Alpagut. On İki Levha Yayıncılık, 2020.

Alp, Mustafa. “Tele Çalışma (Uzaktan Çalışma)”. İçinde Sarper SÜZEK’e Armağan, c. 1. İstanbul, 2011.

Alp, Mustafa, ve Sevil Doğan. “Giyilebilir Teknolojiler ve İş İlişkisine Etkileri”. Çalışma ve Toplum Dergisi 4, sy 71 (2021): 2599-632.

Alp, Nihat Seyhun. “İş Hukukunda İşçilerin Sosyal Medya Kullanımına İlişkin İşyeri İç Yönetmelikleri/Rehberler”. Anadolu Üniversitesi Hukuk Fakültesi Dergisi 11, sy 1 (2025): 1.

Alpagut, Gülsevil. “Dijitalleşen Çalışma Yaşamında İş Sözleşmesinin Unsurları”. İçinde Ekonomik ve Teknolojik Gelişmelerin İş Hukuku ve Sosyal Güvenlik Hukukuna Etkileri. Prof. Dr. Münir Ekonomi 85. Doğum Günü Armağanı. On İki Levha Yayıncılık, 2021.

Alpagut, Gülsevil. “İçinin Sadakat Borcu ve Türk Borçlar Kanunu ile Getirilen Düzenlemeler”. Sicil İş Hukuku Dergisi, sy 25 (2012): 23-33.

Alpagut, Gülsevil. “İşyerinde Kamera Gözetlemesi ve AİHM Kararları ile Tespit Edilen Esaslar”. Prof. Dr. Savaş Taşkent’e Armağan, İstanbul: On İki Levha Yayıncılık, 2019, 275-313.

Altıntaş, Soner, ve Fatma Barkuş. “Dijital Ortamlarda Kişisel Veri Güvenliği Kavramı Üzerine Bir Derleme Çalışması”. Electronic Journal of Vocational Colleges, sy 13 (2023): 46-69.

Arıoğlu, Pınar. “İşverenin Yönetim Hakkının Kötüye KulIanılması”. Doktora Tezi, Çukurova Üniversitesi, 2024.

Arrêt du 8 octobre 2014, no. 13-14.991 (2014). https://www.legifrance.gouv.fr/juri/id/JURITEXT000029565250.

Arrêt du 22 février 2025. Pourvoi n° 22-18.179 (2025). https://www.courdecassation.fr/decision/67bebeb8ab77563075a5940e.

Arrêt n° 166 F-D, 26 février 2025, pourvoi n° 22-24.474. (2025). https://www.courdecassation.fr/decision/67bebec5ab77563075a5941e.

Arslan Ertürk, Arzu. “Yeni Türk Borçlar Kanununun Genel Hizmet Sözleşmesinin Kurulmasına ve Tarafların Borçlarına İlişkin Esasları”. 6098 Sayılı Türk Borçlar Kanunu Hükümlerinin Değerlendirilmesi Sempozyumu, Sempozyum No. 3, Prof. Dr. Cevdet Yavuz’a Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 2011, 533-59.

Arslan, Karsu. “Teknolojik İletişim Araçları ile Evde (Tele) Çalışan İşçinin Kişisel Verilerinin Korunması”. Yüksek Lisans Tezi, Bursa Uludağ Üniversitesi, 2024.

Article 29 Data Protection Working Party. Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251rev.01). European Commission, 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610164.

Article 29 Data Protection Working Party. Opinion 2/2017 on data processing at work. 17/EN WP 249. Brussels, Belgium, 2017. http://ec.europa.eu/justice/data-protection/index_en.htm.

“Article L1222-9 - Code du travail - Légifrance”. Erişim 10 Mart 2025. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047864720.

Aşıkoğlu, Şehriban İpek. “Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebepleri”. İçinde Türk Hukukunun Avrupa Birliği Hukukuna Uyumu Özel Hukuk-Acquis Communautaire’in Alınması-Açıklamalar, Değerlendirmeler, editör Arslan Kaya, Baki İlkay Engin, Şehriban İpek Aşıkoğlu, ve Elif Oğuz. Istanbul University Press, 2020.

Avcıoğlu, Cem. “Uzaktan Çalışmaya Dair Veriler Dönüşümün Kalıcılığına İşaret Ediyor”. TSKB, 29 Ağustos 2025. https://www.tskb.com.tr/blog/genel/uzaktan-calismaya-dair-veriler-donusumun-kaliciligina-isaret-ediyor.

Aydın, Fatih. “İşçinin Sosyal Medya Paylaşımlarının İş Sözleşmesinin Feshine Etkisi”. Doktora Tezi, T.C. Erciyes Üniversitesi, 2022.

Aydın, Nihan. “Çalışma Yaşamında Özgürlük Sorunu: Gözetim ve Mahremiyetin Yeni Sınırları”. Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi, 2011.

Aydın, Ufuk. Bireysel İş Hukuku. 7. bs. Nisan Kitabevi, 2023.

Aydın, Ufuk. “Tele Çalışma ve Tele Çalışma Çerçeve Avrupa Sözleşmesi”. İçinde Prof. Dr. Devrim Ulucan’a Armağan. Hukuk Kitapları Serisi 119. Legal Yayıncılık, 2008.

Aydınöz, Gonca. “İş Hukukunda Tele (Uzaktan) Çalışma”. Doktora Tezi, Ankara Üniversitesi, 2014.

Bal, Tolga. “Addressing Remote Work Challenges in Türkiye: A New Paradigm for Workplace Safety”. Sosyal Güvenlik Dergisi 14, sy 2 (2025): 183-207. https://doi.org/10.32331/sgd.1699858.

Balaban, Mahmut Furkan. “Elektronik Haberleşme Sektöründe İşlenen Kişisel Verilerin Korunması”. Doktora Tezi, Ankara Sosyal Bilimler Üniversitesi, 2023.

Ball, Kirstie. Electronic Monitoring and Surveillance in the Workplace: Literature Review and Policy Recommendations. Publications Office of the European Union, 2021.

Ball, Kirstie. “Surveillance in the Workplace: Past, Present, and Future”. Surveillance & Society 4, sy 20 (2022): 455-61.

Ball, Kirstie. “Workplace Surveillance: An Overview”. Labor History 51, sy 1 (2010): 87-106.

Ball, Kirstie, ve T. Margulis. “Monitoring and Surveillance in Call Centres: A Review and Synthesis”. New Technology, Work and Employment 26, sy 2 (2011): 113-26.

Ballaban, Michael. “When Henry Ford’s Benevolent Secret Police Ruled His Workers”. Jalopnik, 2014. https://jalopnik.com/when-henry-fords-benevolent-secret-police-ruled-his-wo-1549625731.

Baş, Halim. “Türkiye’de Sanal Beyin Göçü: Uzaktan Yurtdışına Çalışanların Deneyimleri Üzerine Nitel Bir Araştırma”. İstanbul İktisat Dergisi 72, sy 2 (2022): 915-51.

Baycık, Gaye, Orhan Ersun Civan, Hazal TOLU Yılmaz, ve Berrin Bosna. “Platform Çalışanlarını Yasal Güvenceye Kavuşturmak: Sorunlar ve Çözüm Önerileri”. Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, sy 1 (2021).

Bayram, Fuat. “Borçlar Kanunu Tasarısı Işığında İşverenin, İşçinin Kişiliğini Koruma Borcu”. İş Hukuku ve Sosyal Güvenlik Hukuku Türk Milli Komitesi 30 (2006): 11-48.

Bekkum, Marvin van, ve Frederik Zuiderveen Borgesius. “Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?” arXiv:2206.03262. Preprint, arXiv, 28 Kasım 2022.

Bernhardt, Annette, Lisa Kresge, ve Reem Suleiman. “The Data-Driven Workplace and the Case for Worker Technology Rights”. ILR Review 76, sy 1 (2023): 3-29.

Beytar, Erbil. İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması. 2. Baskı. On İki Levha Yayıncılık, 2018.

Bhatt, Sandeep, Pratyusa K. Manadhata, ve Loai Zomlot. “The Operational Role of Security Information and Event Management Systems”. IEEE Security & Privacy 12, sy 5 (2014): 35-41. https://doi.org/10.1109/MSP.2014.103.

Bhatt, Umang, ve Holli Sargeant. “When Should Algorithms Resign? A Proposal for AI Governance”. arXiv:2402.18326. Preprint, arXiv, 16 Temmuz 2024. https://doi.org/10.48550/arXiv.2402.18326.

Birtane, Şermin. “Özel Hayata Saygı Hakkı (AİHS 8. Madde) Bağlamında Çalışma Hakkı ve Mesleki Hayat İlişkisi”. Anayasa Yargısı 38, sy 2 (2021): 57-97.

Blessing, Elisha, ve K Hubert. “Security Auditing and Monitoring: Incident Response and Management”. Hall Open Science, hal-04972073, 2024. https://hal.science/hal-04972073v1.

Blume, Joshua. “A Contextual Extraterritoriality Analysis of the DPIA and DPO Provisions in the GDPR”. Georgetown Journal of International Law 49, sy 4 (2018): 1425-60.

Bohol Island State University – Candijay Campus, Cogtong, Candijay, Bohol, Epifelward Niño O. Amora, Kennery V. Romero, vd. “Digital Attendance and Accomplishment Report Monitoring System (DIGIATT)”. International Multidisciplinary Research Journal 3, sy 2 (2021): 123-33.

Boz, Hüseyin, ve Ebru Gözen. İş-Yaşam Dengesi Açısından İşgörenin Ulaşılamama Hakkı. Akademisyen Kitabevi, 2024.

Bozkurt Gümrükçüoğlu, Yeliz. “COVID-19 Pandemi Döneminde Home-Office Uygulamasına İlişkin Türk ve Alman Hukuku’nda Mukayeseli Bir Değerlendirme”. Koronavirüs Döneminde Güncel Hukuki Meseleler Sempozyumu: Bildiri Tam Metin Kitabı 29-30 Mayıs 2020, İbn Haldun Üniversitesi Yayınları, 2020, 145-207.

Bozkurt Gümrükçüoğlu, Yeliz. “İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu”. İçinde İş Hukukunda Yeni Yaklaşımlar. Beta Yayınları, 2017.

Bozkurt Gümrükçüoğlu, Yeliz. “İşçinin Sosyal Medya Kullanımının İş Hukukundaki Etkileri”. PressAcademia Procedia 7, sy 1 (2018): 372-75.

Bozkurt Gümrükçüoğlu, Yeliz. “İşyerinde Elektronik Gözetim Uygulamaları ve İşçinin Kişisel Verilerinin Korunması”. II. Kişisel Verilerin Korunması Sempozyumu, 7 Şubat 2019, Kişisel Verilerin Korunması Kurumu, 2019. http://openaccess.ihu.edu.tr/xmlui/handle/20.500.12154/1039.

Bozkurt Gümrükçüoğlu, Yeliz. “Kişisel Verilerin Korunması Kanunu’nun İş Sağlığı Ve Güvenliği Alanındaki Etkileri”. 9. Uluslararası İş Sağlığı Güvenliği Kongresi, Bildiri Tam Metinleri Kitabı 2 (2018): 811-23.

Bozkurt Gümrükçüoğlu, Yeliz, Orhan Ersun Civan, A. Eda Manav Özdemir, F. Burcu Savaş Kutsal, ve Ahmet Evcimen. İş Hukukunda Uzman Arabuluculuk. Ankara, 2023.

Bozkurt Gümrükçüoğlu, Yeliz, ve F. Burcu Savaş Kutsal. "Uzaktan Çalışma". İçinde Zorlayıcı Sebeplerin İş İlişkisine Etkisi, editör Saim Ocak. Adalet Yayınevi, 2023.

Bozkurt Gümrükçüoğlu, Yeliz, ve Gülnihal Ahter Yakacak. "Yapay Zekânın İşe Alım Süreçlerinde Kullanımı ve Algoritmik Ayrımcılık". Ankara Üniversitesi Hukuk Fakültesi Dergisi 72, sy 4 (2024): 1701-57.

Bueckert, Melanie R. "Electronic Employee Monitoring: Potential Reform Options". Manitoba Law Journal 6 (2009): 99-99.

BuildOps. "How to Track Field Employees to Increase Productivity". Erişim 03 Mart 2025. https://buildops.com/resources/how-to-track-field-employees/.

Bureau of Justice Assistance. "Electronic Communications Privacy Act of 1986 (ECPA)". Resmi Site. Erişim 13 Nisan 2025. https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285.

Büyük, Köksal, ve Uğur Keskin. "Panoptikon'un Elektronik Dirilişi: Etik Bir Sorun Olarak İşyeri İzleme". İş Ahlakı Dergisi 5, sy 10 (2012): 55-88.

Büyüksağiş, Erdem. "Yapay Zeka Karşısında Kişisel Verilerin Korunması ve Revizyon İhtiyacı". Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 18, sy 2 (2021): 2.

Campbell, Adam. "Security and Privacy Analysis of Employee Monitoring Applications". Master Thesis, University of Waterloo, 2023. http://hdl.handle.net/10012/19724.

Caniklioğlu, Nurşen. "Kişisel Verilerin Korunması Açısından İşçilerin Hakları". İçinde Prof. Dr. Turhan Esener III. İş Hukuku Uluslararası Kongresi, 34. bs. Seçkin Yayıncılık, 2021.

Caniklioğlu, Nurşen, ve Melis Kutlu. "Tele Çalışmada İşyeri Kavramı". İstanbul Aydın Üniversitesi Hukuk Fakültesi Dergisi 10, sy 2 (2024): 119-57.

Case of Antović and Mirković v. Montenegro, No. 70838/13 (ECtHR 28 Kasım 2017). https://hudoc.echr.coe.int/fre?i=001-178904.

Case of Bărbulescu V. Romania, Application no. 61496/08 (European Court of Human Rights (Grand Chamber) 05 Eylül 2017). https://hudoc.echr.coe.int/fre?i=001-177082.

Case of Halford V. the United Kingdom, Application no. 20605/92 (European Court of Human Rights (Grand Chamber) 25 Haziran 1997). https://hudoc.echr.coe.int/tur?i=001-58039.

Case of Libert V. France, Application no. 588/13 (European Court of Human Rights (Fifth Section) 02 Temmuz 2018). https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-181273%22]}.

Catarina de Oliveira Carvalho. "The New Regulation of Telework and Remote Work in Portugal: Considerations and Prospects". E-Journal of International and Comparative Labour Studies 11, sy 03 (2022): 1-31.

Celal Oraj Altunörgü Başvurusu, Başvuru Numarası: 2018/31036 (Anayasa Mahkemesi 12 Ocak 2021). https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/31036.

Cem Sarıkabadayı. "6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri". Yayınlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi, 2024.

Centel, Tankut. "Türk Borçlar Kanunu'nda Hizmet Sözleşmelerinin Tanımı ve Kurulması". Tisk Akademi 6, sy 12 (2011): 6-22.

"China Claims It's Scanning Workers' Brainwaves to Increase Efficiency and Profits". VICE, 01 Mayıs 2018. https://www.vice.com/en/article/china-brain-wave-hats-helmets-productivity/.

Choi, Byungjoo, Sungjoo Hwang, ve SangHyun Lee. "What Drives Construction Workers' Acceptance of Wearable Technologies in the Workplace?: Indoor Localization and Wearable Health Devices for Occupational Safety and Health". Automation in Construction 84 (2017): 31-41.

Chukwudi Tabitha Aghaunor, Patience Eshua, Tawo Obah, ve Oluwatoyin Aromokeye. "Data Security Strategies to Avoid Data Breaches in Modern Information Systems". World Journal of Advanced Research and Reviews 20, sy 3 (2023): 2122-44.

Ciocchetti, Corey A. "The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring: The Eavesdropping Employer". American Business Law Journal 48, sy 2 (2011): 285-369.

Civan, Orhan Ersun. "İş Hukukunda Uzaktan Çalışma (Evde Çalışma/Tele Çalışma)". Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, sy 26 (2010): 525-73.

Clausing, Eric, ve M. Schiefer. "Internet of Things Security Evaluation of 7 Fitness Trackers on Android and the Apple Watch". AV TEST, Germany, sy 1-21 (2016).

CNIL. "Surveillance Excessive Des Salariés: Sanction De 40 000 Euros À L'encontre D'une Entreprise Du Secteur Immobilier". Resmi Site. 04 Şubat 2025. https://www.cnil.fr/fr/surveillance-excessive-des-salaries-sanction-de-40-000-euros-entreprise-secteur-immobilier.

Cobbe, Jennifer, ve Jatinder Singh. “Reviewable Automated Decision-Making”. Computer Law & Security Review 39 (Kasım 2020): 105475. https://doi.org/10.1016/j.clsr.2020.105475.

“Complete Guide to Employee Monitoring in the US | 2024”. Jibble, t.y. Erişim 13 Nisan 2025. https://www.jibble.io/article/us-employee-monitoring.

“Convention C177 - Home Work Convention, 1996 (No. 177)”. Erişim 25 Temmuz 2024. https://normlex.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_INSTRUMENT_ID:312322.

“Convention C184 - Safety and Health in Agriculture Convention, 2001 (No. 184)”. Erişim 01 Nisan 2025. https://normlex.ilo.org/dyn/nrmlx_en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C184.

Cornell Law School: Legal Information Institute. “Surveillance”. Erişim 12 Şubat 2025. https://www.law.cornell.edu/wex/surveillance.

Council of Europe. Convention 108+ – Convention for the Protection of Individuals with Regard to the Processing of Personal Data, as Amended by the Protocol CETS No. 223. 18 Mayıs 2018. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.

Cour de Cassation, Civile, Chambre Sociale, 23 juin 2021, 19-13.856. Erişim 22 Mayıs 2025. https://www.legifrance.gouv.fr/juri/id/JURITEXT000043711120.

“Covid-19: Guidance for Labour Statistics Data Collection”. International Labour Office, 05 Haziran 2020. https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@dgreports/@stat/documents/publication/wcms_747075.pdf.

Custers, Bart, Francien Dechesne, Alan M. Sears, Tommaso Tani, ve Simone van der Hof. “A Comparison of Data Protection Legislation and Policies Across the EU”. Computer Law & Security Review 34, sy 2 (2018): 234-43.

Custers, Bart, Alan M. Sears, Francien Dechesne, Ilina Georgieva, Tommaso Tani, ve Simone Van Der Hof. EU Personal Data Protection in Policy and Practice. C. 29. Information Technology and Law Series. T.M.C. Asser Press, 2019. https://doi.org/10.1007/978-94-6265-282-8.

Çakmak, Bahar. “İnsan Hakları Temelli Yaklaşım Çerçevesinde Yapay Zekâ Teknolojilerinde Kişisel Verilerin Korunması”. Yayınlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi, 2024.

Çalışkan Yıldırım, Aslı, ve Ömer Uğur. “İşveren bakımından fesih sebebi olarak işçinin sosyal medya kullanımları”. İstanbul Hukuk Mecmuası 80, sy 4 (2022): 1169-222.

Çankaya, Yiğitcan. Yapay Zekanın İş İlişkisine Etkileri. On İki Levha Yayıncılık, 2024.

Çekin, Mesut Serdar. Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku. 3. Baskı. On İki Levha Yayıncılık, 2020.

Çekin, Mesut Serdar. Yapay Zekâ Teknolojilerinin Hukuki İşlem Teorisine Etkileri. Onikilevha Yayıncılık, 2021.

Çekin, Mesut Serdar, Ahmed Esad Berktaş, ve M. Furkan Akıncı. Veri Hukuku. On İki Levha Yayıncılık, 2023.

Çelik, Ezgi Sima. "İşe Alımda Adayın Kişisel Veri Güvenliği: Yapay Zeka Destekli Video Mülakat Uygulamaları". Kişisel Verileri Koruma Dergisi 6, sy 1 (2024): 1.

Çelik, Nuri, Nurşen Caniklioğlu, Talat Canbolat, ve Ercüment Özkaraca. İş Hukuku Dersleri. 36. bs. Beta, 2023.

Çelikel, Serdar. "Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri". Doktora Tezi, Ankara Üniversitesi, 2021.

Data Protection and Digital Information Bill, HL Bill 67, UK Parliament Sessions 2022–23, 2023–24. Erişim 13 Mayıs 2025. https://bills.parliament.uk/bills/3430.

De Stefano, Valerio. "Algorithmic Bosses and What to Do About Them: Automation, Artificial Intelligence and Labour Protection". Içinde Economic and Policy Implications of Artificial Intelligence, editör Domenico Marino ve Melchiorre A. Monaca. Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-45340-4_7.

De Stefano, Valerio. "'Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection". 41 COMP. LAB. L. & POL'y J. 15, advance online publication, 2019. https://doi.org/10.2139/ssrn.3178233.

De Stefano, Valerio, ve Simon Taes. "Algorithmic Management and Collective Bargaining". Transfer: European Review of Labour and Research 29, sy 1 (2023): 21-36. https://doi.org/10.1177/10242589221141055.

De Stefano, Valerio, ve Mathias Wouters. AI and Digital Tools in Workplace Management and Evaluation: An Assessment of the EU's Legal Framework. European Parliamentary Research Service, 2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4144899.

De Vaujany, François-Xavier, Aurélie Leclercq-Vandelannoitte, Iain Munro, Yesh Nama, ve Robin Holt. "Control and Surveillance in Work Practice: Cultivating

Paradox in ‘New’ Modes of Organizing”. Organization Studies 42, sy 5 (2021): 675-95.

Del Castillo, Aída Ponce. Artificial Intelligence, Labour and Society. ETUI, 2024.

Demir, Dilanur. “Kişisel Verilerin Korunması Kapsamında Unutulma Hakkı”. Yayınlanmamış Yüksek Lisans Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, 2023.

Demir, Filiz, Belkis Dilek Özbezek, Veysel Mehmet Gültekin, vd. Örgutsel Davranış Kavramlar ve Araştırmalar-I. Editör Bengü Hırlak. Özgür Yayınları, 2023. https://doi.org/10.58830/ozgur.pub79.

Demirbaş, Ali. Kişisel Verileri Koruma Hukukunda Veri Sorumlusu ve Yükümlülükleri. Oniki Levha Yayıncılık, 2023.

Determann, Lothar, ve Jonathan Tam. “The California Privacy Rights Act of 2020: A Broad and Complex Data Processing Regulation That Applies to Businesses Worldwide”. Journal of Data Protection & Privacy 4, sy 1 (2020): 7.

Devigne, Arnaud. “How Neurotechnologies Can Shape The Future Of Work”. Forbes, 2024. https://www.forbes.com/councils/forbesbusinesscouncil/2024/09/20/how-neurotechnologies-can-shape-the-future-of-work/.

Dhingra, Madhavi. “Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)”. Procedia Computer Science 78 (2016): 179-84.

Dilanur Demir. “Kişisel Verilerin Korunması Kapsamında Unutulma Hakkı”. Yayınlanmamış Yüksek Lisans Tezi, Hacettepe Üniversitesi, 2023.

Directive 2002/58/EC on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) (2002). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058.

Disterer, Georg, ve Carsten Kleiner. “BYOD Bring Your Own Device”. Procedia Technology 9 (2013): 43-53.

Doargajudhur, Melina Seedoyal, ve Peter Dell. “The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation”. Journal of Computer Information Systems 60, sy 6 (2020): 518-29.

Doğan, Sevil. İş Sözleşmesinde Bağımlılık Unsuru. Seçkin Yayıncılık, 2016.

Doğan Yenisey, Kübra. “Üretimin Değişen Yapısının ‘İşyeri’ Kavramına Etkisi,”. İçinde Ekonomik ve Teknolojik Gelişmelerin İş Hukuku ve Sosyal Güvenlik Hukukuna Etkileri. Prof. Dr. Münir Ekonomi 85. Doğum Günü Armağanı. Oniki Levha Yayıncılık, 2021.

Döngül, E. Sipahi, ve E. Artantaş. "Örgütlerde Algoritmik Yönetim Uygulamaları". İçinde Sosyal Beşeri ve İdari Bilimler Alanında Uluslararasi Araştırmalar XI. Egitim Yaymevi, 2022.

Dulay, Dilek. Türk İş Hukukunda Evde Çalışma. Turhan Kitabevi, 2016.

Dulay Yangın, Dilek. "6715 Sayılı Yasa'nın Uzaktan Çalışmaya İlişkin Hükümleri ve Değerlendirilmesi". Sicil İş Hukuku Dergisi 36 (2016): 148-71.

Dulay Yangın, Dilek. "Avrupa İnsan Hakları Mahkemesi'nin İşçilerin Elektronik Konum Belirleme Sistemleri (GPS) İle Takip Edilmesine İlişkin 13 Aralık 2022 Tarihli Gramaxo Kararı Üzerine Değerlendirmeler". Çalışma ve Toplum 3, sy 82 (2024): 873-902.

Dulay Yangın, Dilek. "Bilgi ve İletişim Teknolojilerinde Yaşanan Gelişimin İş Hukuku Üzerindeki Etkileri: Tele Çalışmaya İlişkin Tespit ve Öneriler". İş Hukukunda Genç Yaklaşımlar III içinde. İstanbul: On İki Levha Yayıncılık, 2018, 221-60.

Duman, Berat. "Anayasa Hukukunda Kişisel Verilerin Korunması". Doktora Tezi, Selçuk Üniversitesi, 2020.

Dumas, Stéphanie. "Social Media & Data Privacy in France". L&E Global, 22 Ekim 2024. https://leglobal.law/countries/france/employment-law/employment-law-overview-france/06-social-media-and-data-privacy-in-france/.

Dursun, Yonca. 6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Işçinin Korunması. 2. Seçkin, 2023.

Dursun, Yonca. Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Korunması. Seçkin, 2021.

Dülger, Murat Volkan. Kişisel Verilerin Korunması Hukuku. 2. Baskı. FA Hukuk Akademisi, 2019.

Dülger, Murat Volkan. "Yapay Zeka Teknolojileri ve Veri Koruma Hukuku (Artificial Intelligence Technologies and Data Protection Law)". SSRN Scholarly Paper No. 3792333. Rochester, NY, 24 Şubat 2021. https://papers.ssrn.com/abstract=3792333.

Dündar, K., ve A.C. Ağaçkayak. "Yapay Zeka ve Makine Öğrenmesi İle İnsan İlişkileri Analizi". İçinde Mühendislikte Yenilikçi Yaklaşımlar-2, 1. Eğitim Yayinevi, 2024.

EasyTechJunkie. "What Is a PVR?" Erişim 22 Şubat 2025. https://www.easytechjunkie.com/what-is-a-pvr.htm.

ECLI:NL:GHAMS:2023:793, 200.295.742/01 (Amsterdam Bölge Mahkemesi 05 Ekim 2023). https://5b88ae42-7f11-4060-85ff-

4724bbfed648.usrfiles.com/ugd/5b88ae_9f6a8251f07b4789852d1fdc171b9475.pdf.

Edwards, Lilian, ve Michael Veale. “Slave to the Algorithm? Why a ‘Right to an Explanation’ Is Probably Not the Remedy You Are Looking for International”. Duke Law & Technology Review 16 (2018 2017): 18-84.

Ekmekçi, Ömer, Burak Gemalmaz, Volkan Aslan, ve H Hilal Yılmaz. Anayasa Mahkemesine bireysel başvurunun temel esasları ve iş ve sosyal güvenlik hukukuna ilişkin kararlar. On İki Levha Yayıncılık, 2022.

Ekmekçi, Ömer, ve Esra Yiğit. Bireysel İş Hukuku Dersleri. 6. bs. Onikilevha, 2024.

Ekmekçi, Ömer, Nafiye Yücedağ, Elif Beyza Akkanat Öztürk, ve Şehriban İpek Aşıkoğlu. Kişisel Verilerin Korunması Hukuku. 3. On İki Levha Yayıncılık, 2025.

Elbir, Nazlı. “Kişiliğinin Korunması Bağlamında İşçiye Ait Kişisel Verilerin Korunması”. Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2020.

“Electronic Communications Privacy Act (ECPA)”. EPIC - Electronic Privacy Information Center, t.y. Erişim 13 Nisan 2025. https://epic.org/ecpa/.

Elish, Madeleine Clare. “Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction”. Engaging Science, Technology, and Society 5 (Mart 2019): 40-60.

Emenike, Stanley Ugochukwu. “Data loss prevention in a remote work environment”. Master Degree Project, University of Skövde, 2021. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1578629.

Employers Engaged in Electronic Monitoring; Prior Notice Required, Civil Rights Law, CHAPTER 6, ARTICLE 5, Section 52-C*2 (2021). https://www.nysenate.gov/legislation/laws/CVR/52-C*2.

Engin, Murat. “Türk İş Hukukunda Evde Çalışma”. Prof. Dr. Turhan Esener’e Armağan, Ankara, 2000, 269-87.

Erafşar, Rabia Büşra. “Bireysel İş Hukukunda Yeni Normal Çalışma Modeli: Evden Çalışma”. Yayınlanmamış Yüksek Lisans Tezi, Ankara Yıldırım Beyazıt Üniversitesi, 2023.

Erafşar, Rabia Büşra. “Türk İş Hukukunda Evden Çalışma”. Yıldırım Beyazıt Hukuk Dergisi, sy 1 (2022): 279-317.

Erdem, Ziya. “Tele çalışma”. İstanbul: Filiz Kitabevi, 2004.

Erdemir, Erkan, ve İlyas Çeliktaş. "Örgütsel ve Hukuki Açıdan İşyeri İzleme: Karşılaştırmalı Bir İnceleme". Kazancı Hakemli Hukuk Dergisi 19, sy 20 (2006): 87-102.

Erdoğan, Canan. Kişilik Hakkı Kapsamında İşçilerin İzlenmesi ve Gözetlenmesi. Yetkin Yayınları, 2017.

Ereken, Ömer Faruk. "Yapay Zeka Tabanlı Personel Seçim Sistemi Uygulaması". Yayınlanmış Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, 2021.

Eren, Fikret. Borçlar Hukuku Genel Hükümler. 28. bs. Legem Yayınevi, 2023.

Erer, Mehmet Zahid. "Bir İnsan Hakkı Olarak Ulaşılamama Hakk". Yayınlanmamış Yüksek Lisans Tezi, İstanbul Medeniyet Üniversitesi, 2024.

Ergin, Hediye. "Sosyal Medya Paylaşımlarıyla İşverenin İtibarını Zedeleyen İşçinin İş Sözleşmesinin Feshi". Sicil İş Hukuku Dergisi 1, sy 49 (2023): 45-59.

Ergüneş Emrağ, Seda. "4857 Sayılı İş Kanunun Değişik 14. Maddesi Işığında Tele Çalışma". Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergis 13, sy 51 (2016): 1413-43.

Erkanlı Başbüyük, Betül. "Uzaktan Çalışmanın Bir Türü Olarak Tele Çalışmada İşçinin Dinlenme Hakkı". Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 29, sy 1 (2023).

Ertürk, Şükran. İş İlişkisinde Temel Haklar. Seçkin, 2002.

Esayas, Samson. "The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing'approach". European Journal of Law and Technology 6, sy 2 (2015). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746831.

Eurofound. "France: Employee Monitoring and Surveillance". Restructuring Legislation European Restructuring Monitor (ERM), 01 Kasım 2023. https://apps.eurofound.europa.eu/legislationdb/employee-monitoring-and-surveillance/france.

Eurofound. Greece: Employee Monitoring and Surveillance. European Foundation for the Improvement of Living and Working Conditions (Eurofound), 2023. https://www.eurofound.europa.eu/data/platform-economy/employee-monitoring-and-surveillance/greece.

European Commission. Framework Agreement on the Application of Article 16(1) of Regulation (EC) No 883/2004 in Cases of Habitual Cross-Border Telework. European Commission, 2023. https://socialsecurity.belgium.be/sites/default/files/content/docs/en/international/framework_agreement_on_cross-border_telework.pdf.

European Commission. Practical Guide: The Applicable Legislation in the EU, EEA and in Switzerland. Directorate-General for Employment, Social Affairs and Inclusion, 2022. https://webgate.ec.europa.eu/circabc-ewpp/d/d/workspace/SpacesStore/49cd18c1-5478-4e15-98dc-c7aa6f01a823/file.bin.

European Data Protection Board (EDPB). Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects. t.y. Erişim 29 Mayıs 2025. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

European Data Protection Board (EDPB). Guidelines 3/2019 on Processing of Personal Data Through Video Devices. Version 2.0. 2020.

European Parliament and Council. "Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 Establishing a General Framework for Informing and Consulting Employees in the European Community". Official Journal of the European Communities, 23 Mart 2002. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0014.

European Parliament and Council. "Regulation (EC) No 883/2004 of 29 April 2004 on the Coordination of Social Security Systems". Official Journal of the European Union, 30 Nisan 2004. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0883R(01).

European Parliament and Council of the European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 March 2024 on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. 13 Mart 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

ExpressVPN. "Workplace Surveillance Trends in the U.S. 2025". ExpressVPN Blog, 06 Şubat 2025. https://www.expressvpn.com/blog/workplace-surveillance-trends-us/.

Eyrenci, Öner, ve Kadriye Bakırcı. Dünyada ve Türkiye'de Evde Çalışma ve Eve İş Verme. İstanbul Ticaret Odası, 2000.

Eyrenci, Öner, Savaş Taşkent, Devrim Ulucan, ve Esra Baskan. İş Hukuku. 10. bs. Beta, 2020.

Falque-Pierrotin, Isabelle. Opinion 2/2017 on Data Processing at Work. 17/EN WP 249. EU Comission Article 29 Data Protection Working Party, 2017. https://ec.europa.eu/newsroom/article29/items/610169.

Feiler, Lukas, Nikolaus Forgo, ve Michaela Nebel. The EU General Data Protection Regulation (GDPR): A Commentary. Globe Law And Business, 2021.

Feng, Kung. “Overview of New Rights for Workers under the California Consumer Privacy Act”. UC Berkeley Labor Center, 06 Aralık 2023. https://laborcenter.berkeley.edu/overview-of-new-rights-for-workers-under-the-california-consumer-privacy-act/.

Fereidooni, Hossein, Tommaso Frassetto, Markus Miettinen, Ahmad-Reza Sadeghi, ve Mauro Conti. “Fitness trackers: fit for health but unfit for security and privacy”. 2017 IEEE/ACM international conference on connected health: Applications, systems and Engineering technologies (CHASE), IEEE, 2017, 19-24. https://ieeexplore.ieee.org/abstract/document/8010569/.

Fernández, Roberto Fernández. “Big Data as a Tool to Enhance Recruitment Processes”. E-Journal of International and Comparative Labour Studies, 2022. https://ejcls.adapt.it/index.php/ejcls_adapt/article/view/1168/1339.

Fiser, Harvey L., ve Patrick D. Hopkins. “Getting Inside the Employee’s Head: Neuroscience, Negligent Employment Liability, and the Push and Pull for the New Technology”. Boston University Journal of Science and Technology Law 23, sy 1 (2017): 44-87.

Foucault, Michel. Hapishanenin Doğuşu. 8. Çeviren Mehmet Ali Kılıçbay. İmge Kitabevi Yayınları, 2019.

“France: Video Surveillance Cannot Permanently Monitor the Activity of an Employee Working Alone”. L&E Global, 29 Temmuz 2021. https://leglobal.law/2021/07/29/france-video-surveillance-cannot-permanently-monitor-the-activity-of-an-employee-working-alone/.

Galandarlı, Arzu. “Veri Etki Değerlendirilmesi (GDPR Article 29 Ve KVKK)”. Hukuk ve Bilişim Dergisi -, 01 Nisan 2025. https://www.hukukvebilisimdergisi.com/veri-etki-degerlendirilmesi-gdpr-article-29-ve-kvkk/.

Garba, Bello. “Bring Your Own Device Organizational Information Security and Privacy”. ARPN Journal of Engineering and Applied Sciences, 10, sy 3 (2015): 1279-87.

Gaudry, Kate S., Hasan Ayaz, Avery Bedows, vd. “Projections and the Potential Societal Impact of the Future of Neurotechnologies”. Frontiers in Neuroscience 15 (Kasım 2021). https://www.frontiersin.orghttps://www.frontiersin.org/journals/neuroscience/articles/10.3389/fnins.2021.658930/full.

Gemalmaz, Burak. “Çalışanların İnternet İletişiminin İşverence İzlenmesi Özel Yaşam Hakkına Aykırı Mıdır?: AİHM Büyük Dairenin 05 Eylül 2017 Tarihli Barbulescu Kararı”. Lexpera Blog, 09 Eylül 2017. https://blog.lexpera.com.tr:443/calisanlarin-internet-iletisiminin-isverence-izlenmesi-ozel-yasam-hakkina-aykiri-midir-aihm-buyuk-dairenin-05-eylul-2017-tarihli-barbulescu-karari/.

Gemici Filiz, Beste. “Türk İş Hukuku’nda İş Sözleşmesinin Geçersizliği”. Doktora Tezi, İstanbul Kültür Üniversitesi, 2024.

George Apostolou ve Alexandros Tsolias. “Cyprus Employment Series: Navigating the Evolving Landscape of Remote Working and the Right to Disconnect in Cyprus”. Harneys. Erişim 22 Mayıs 2025. https://www.harneys.com/insights/navigating-the-evolving-landscape-of-remote-working-and-the-right-to-disconnect-in-cyprus/.

George, Stebin, Konda Aiswarya Lakshmi, ve K.T. Thomas. “Predicting Employee Attrition Using Machine Learning Algorithms”. 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Aralık 2022, 700-705. https://ieeexplore.ieee.org/document/10074131.

Georgiades, Eliada, ve Nadia Tryfonidou. “Regulating Remote Work”. 2023. https://gzg.com.cy/insights/insights/Regulating-Remote-Work-in-Cyprus/.

Georgiou, Dimitra, ve Costas Lambrinoudakis. “DPIA for Cloud-Based Health Organizations in the Context of GDPR”. European Conference on Cyber Warfare and Security 22, sy 1 (2023): 187-98. https://doi.org/10.34190/eccws.22.1.1144.

Gerçek, Sevcan Günsu. “Türk İş Hukukunda Uzaktan Çalışma”. Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, 2024.

Gizem Tan. “Atipik İş Sözleşmelerinden Evde Çalışma ve Tele Çalışma”. Yayınlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi, 2007.

Goodman, Bryce, ve Seth Flaxman. “European Union regulations on algorithmic decision-making and a ‘right to explanation’”. AI magazine 38, sy 3 (2017): 50-57.

GOV.UK. “Data Protection”. Resmi Site. Erişim 13 Nisan 2025. https://www.gov.uk/data-protection.

Goyal, Rohit, Nicola Dragoni, ve Angelo Spognardi. “Mind the Tracker You Wear: A Security Analysis of Wearable Health Trackers”. Proceedings of the 31st Annual ACM Symposium on Applied Computing (New York, NY, USA), SAC ’16, Association for Computing Machinery, 04 Nisan 2016, 131-36.

Göktaş, Seracettin. “Türk İş Hukukunda İşverenin İşçinin Özel Yaşamına Saygı Borcu”. Anayasa Yargısı 38, sy 2 (2021): 1-55.

Granieri, Andrea. How the Remote Work Revolution Will Change the Employer-Employee Relationship. 2020.

Green, Ben. “The Flaws of Policies Requiring Human Oversight of Government Algorithms”. Computer Law & Security Review 45 (Temmuz 2022): 105681.

Güçlütürk, Osman Gazi. "Türk Hukukunda Makine Öğrenmesine Dayalı Yapay Zekada Verinin Hukuka Uygun Şekilde Kullanılması". Doktora Tezi, Galatasaray Üniversitesi, 2021.

Güçlütürk, Osman Gazi. Yapay Zeka ve Verinin Kullanımı. 1. Baskı. On İki Levha Yayıncılık, 2020.

Gül, Muhammed Esat. "Kişisel Veri İşleme Şartlarından Açık Rıza". Yüksek Lisans Tezi, İstanbul Üniversitesi, 2022.

Güler, Yıldız. "6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Kişisel Verilerinin Korunması". Yayınlanmamış Yüksek Lisans Tezi, İzmir Ekonomi Üniversitesi, 2022.

Gülver, Ender. "Türk Borçlar Kanunu'nun Evde Hizmet Sözleşmesine İlişkin Hükümleri Üzerine". Journal of Istanbul University Law Faculty 72, sy 2 (2014): 103-22.

Günal, Ayşe Nida, ve Yasin Üstün. "İş İlişkilerinde Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebebi Olarak 'Meşru Menfaat'". Kişisel Verileri Koruma Dergisi 4, sy 2 (2022): 1-18.

Günay, Arkın. Türk Hukukunda ve Karşılaştırmalı Hukukta Evde Çalışma. Legal Yayıncılık, 2019.

Gürsel, İlke. İşçinin Kişisel Verilerinin Korunması Hakkı. Birinci baskı. Adalet Yayınevi, 2016.

Güzel, Ali. "Fabrikadan İnternete İşçi Kavramı ve Özellikle Hizmet Sözleşmesinin Bağımlılık Unsuru Üzerine Bir Deneme". Kamu İş, Prof. Dr. Kemal Oğuzman'a Armağan 4, sy 2 (1997).

Güzel, Ali, ve Deniz Ugan Çatalkaya. "İş Sözleşmesinin Uygulanmasında ve İşverenin Yönetim Yetkisinin Sınırlanmasında Dürüstlük (Objektif İyiniyet) Kuralının İşlevi Üzerine". Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 20, sy 1 (2014): 1.

Güzel, Ali, Deniz Ugan Çatalkaya, ve Hande Heper. "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi". Hukuk ve Adalet Eleştirel Hukuk Dergisi, Legal Yayınevi, sy Özel Sayı (Eylül 2023): 25-109.

Hafizoğlu, Ece Sıla. "İş İlişkisinde Şüphe ve Şüphe Feshi (Alman Hukuku ile Karşılaştırmalı)". Doktora Tezi, Dokuz Eylül Üniversitesi, 2022.

Hannelais, Joelle, ve Sarah Machrhoul Lhotellier. "Protection Of Privacy At Work In France". Mondaq, 20 Eylül 2021. https://www.mondaq.com/france/employee-rights-labour-relations/1112712/protection-of-privacy-at-work-in-france.

Harper, Erica. The Evolving Neurotechnology Landscape: Examining the Role and Importance of Human Rights in Regulation. The Geneva Academy of

International Humanitarian Law and Human Rights, 2023. https://www.geneva-academy.ch/joomlatools-files/docman-files/The%20Evolving%20Neurotechnology%20Landscape.pdf.

He, Zhicheng. “From Privacy-Enhancing to Health Data Utilisation: The Traces of Anonymisation and Pseudonymisation in EU Data Protection Law”. Digital Society 2, sy 2 (2023): 17.

Healthworld. “Neurotechnology is becoming widespread in workplaces - and our brain data needs to be protected”. 2024. https://health.economictimes.indiatimes.com/news/health-it/neurotechnology-is-becoming-widespread-in-workplaces-and-our-brain-data-needs-to-be-protected/112652528.

Henkoğlu, Türkay. “Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi”. Doktora Tezi, T.C. Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Bilgi ve Belge Yönetimi Anabilim Dalı, 2015.

Hintze, Mike, ve Khaled El Emam. “Comparing the benefits of pseudonymisation and anonymisation under the GDPR”. Journal of Data Protection & Privacy 2, sy 2 (2018): 145-58.

Hirvonen, Hanne, ve Frida Alizadeh Westerling. “Beyond Human Oversight—Quality Management as a Tool to Control Automated Decision-Making Systems”. İçinde De Gruyter Handbook of Automated Futures: Imaginaries, Interactions and Impact, 2. bs. Walter de Gruyter, 2024.

Ho, J. J., S. Novick, ve C. Yeung. “A Snapshot of Data Sharing by Select Health and Fitness Apps”. Conference paper presented de In Proceedings of the Seminar on Privacy Implications of Consumer Generated and Controlled Health Data, Washington, DC, USA. Federal Trade Commission, Washington, 07 Mayıs 2014.

Holland, Peter Jeffrey, Brian Cooper, ve Rob Hecker. “Electronic Monitoring and Surveillance in the Workplace: The Effects on Trust in Management, and the Moderating Role of Occupational Type”. Personnel Review 44, sy 1 (2015): 161-75.

Holzinger, Andreas, Kurt Zatloukal, ve Heimo Müller. “Is Human Oversight to AI Systems Still Possible?” New Biotechnology 85 (Mart 2025): 59-62.

Hoofnagle, Chris Jay, Bart Van Der Sloot, ve Frederik Zuiderveen Borgesius. “The European Union General Data Protection Regulation: What It Is and What It Means”. Information & Communications Technology Law 28, sy 1 (2019): 65-98.

"How Much Employee Monitoring Is Too Much?" Erişim 13 Nisan 2025. https://www.americanbar.org/news/abanews/publications/youraba/2018/january-2018/how-much-employee-monitoring-is-too-much-/.

Hubstaff. "Hubstaff Software Features and Capabilities". Erişim 27 Şubat 2025. http://bestnjawnings.com/features.html.

Huth, Dominik, ve Florian Matthes. "'Appropriate Technical and Organizational Measures': Identifying Privacy Engineering Approaches to Meet GDPR Requirements". Conference paper presented de Twenty-fifth Americas Conference on Information Systems. Cancun, 2019.

ICO. ICO Tech Futures: Neurotechnology. Information Commissioner's Office, 2023. https://ico.org.uk/media/about-the-ico/research-and-reports/ico-tech-futures-neurotechnology-0-1.pdf.

ILO. "Defining and Measuring Remote Work, Telework, Work at Home and Home-Based Work". İçinde ILO Technical Note. International Labour Office, 2020. https://www.ilo.org/publications/defining-and-measuring-remote-work-telework-work-home-and-home-based-work.

ILO. Work for a brighter future–Global Commission on the Future of Work. International Labour Office Geneva, 2019. https://www.oitcinterfor.org/en/node/7468.

Inc, Gallup. "Indicator: Hybrid Work". Gallup.Com. Erişim 17 Eylül 2025. https://www.gallup.com/401384/indicator-hybrid-work.aspx.

Information Commissioner's Office (ICO). Employment Practices and Data Protection: Monitoring Workers. Information Commissioner's Office (ICO), 2023. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/.

Investigatory Powers Act 2016 (2016). https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

Isusi, Iñigo, Jessica Durán, ve Antonio Corral. Working Conditions in Telework During The Pandemic and Future Challenges. No. WPEF22032. European Foundation for the Improvement of Living and Working Conditions, 2022.

İkizler, Murat. "Türk Hukukunda Esnek Çalışma". Adalet Yayınevi, 2012.

İnal, Beyza. "Uzaktan Çalışma". Başkent Üniversitesi Sosyal Bilimler Enstitüsü, 2021.

Information Commissioner's Office (ICO). The Employment Practices Code. Information Commissioner's Office (ICO), 2011. https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf.

Inpixon. “Bluetooth RTLS: BLE Location Tracking & Positioning | Inpixon”. Erişim 03 Mart 2025. https://www.inpixon.com/technology/standards/bluetooth-low-energy.

International Labour Organization. Protection of Workers’ Personal Data: An ILO Code of Practice. 1997. https://www.ilo.org/resource/other/protection-workers-personal-data.

International Labour Organization. Technical and Ethical Guidelines for Workers’ Health Surveillance. Occupational Safety and Health Series No. 72. Geneva, 1998. https://www.ilo.org/publications/technical-and-ethical-guidelines-workers-health-surveillance.

Ioannidou, Irene, ve Nicolas Sklavos. “On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications”. Cryptography 5, sy 4 (2021): 29.

IOE-EMP. “Greece: Greek Law 4808/2021 - Major Reforms in Employment Legislation”. 23 Ağustos 2021. https://industrialrelationsnews.ioe-emp.org/industrial-relations-and-labour-law-august-2021-1/news/article/greece-greek-law-4808-2021-major-reforms-in-employment-legislation.

Ivanov, Stanislav Hristov. “Automated Decision-Making”. Foresight 25, sy 1 (2023): 4-19. https://doi.org/10.1108/FS-09-2021-0183.

Jansen, Nadeer. “Enhancing Cybersecurity Threat Prevention Through Information Security Event Management (SIEM) and Policy Deployment Effectiveness”. Preprint, Unpublished, 2023. https://doi.org/10.13140/RG.2.2.33723.02088.

Jasmontaite, L., I. Kamara, G. Zanfir-Fortuna, ve S. Leucci. “Data Protection by Design and by Default”: European Data Protection Law Review 4, sy 2 (2018): 168-89. https://doi.org/10.21552/edpl/2018/2/7.

Jeffery, Mark. “Information Technology and Workers’ Privacy: Introduction Part I: Introduction”. Comparative Labor Law & Policy Journal 23, sy 2 (2002): 251-80.

Jensen, Michael C. “Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure”. Journal of Financial Economics 3, sy 4 (2000): 306-60.

Kagan, Abigail M. Big Data and Employment Law: What Employers and Their Legal Counsel Need to Know. 2018.

Kahraman Akgül, Saime Duygu. “İşçinin İşyerinde İzlenmesi ve Gözetlenmesinin Hukuki Sonuçları”. Yayınlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi Sosyal Bilimler Enstitüsü, 2020.

Kandemir, Murat. “Evde Çalışma ve 6098 Sayılı Türk Borçlar Kanunu’nun Evde Hizmet Sözleşmesine İlişkin Hükümleri”. Journal of Istanbul University Law Faculty 72, sy 2 (2014): 2.

Kandemir, Murat. İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma. Legal Kitapevi, 2011.

Kaplan, Emine Tuncay. “İşverenin koruma ve gözetme borcunun kapsamı”. Kamu-İş, C 2 (2003).

Kara, Serenay. Uzaktan Çalışmada İş Sağlığı ve Güvenliğinin Hukuki Boyutu. Seçkin Yayıncılık, 2022.

Karaboğa, Uğur. “İşe Alım Süreçlerinde Yapay Zeka Teknolojilerinin Kullanımı”. Yüksek Lisans Tezi, İstanbul Medipol Üniversitesi Sosyal Bilimler Enstitüsü, 2020.

Karademir, Artür. “İşyerinde İnternetin Özel Amaçla Kullanımı ve İşverence Gözetlenmesi”. Terazi Hukuk Dergisi 10, sy 112 (2015): 56-64.

Kaspersky. “Uç Nokta Güvenliği & Uç Nokta Koruması”. 27 Nisan 2022. https://www.kaspersky.com.tr/resource-center/definitions/what-is-endpoint-security.

Kaya, İrem. “Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) Kapsamında Ortak Veri Sorumluluğu”. Yayınlanmamış Yüksek Lisans Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, 2023.

Kaya, Mehmet Bedii. “Kişisel Verilerin İşlenmesi ve Korunması Arasındaki Denge”. İçinde Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku, editör Ali Cem Bilgili ve Leyla Keser Berber. Marmara Hukuk Bilimsel Toplantılar Serisi – 1. On İki Levha Yayıncılık, 2020.

Kaya, Mehmet Bedii. KVKK Reformu 2024 Değişiklikleri. On İki Levha Yayıncılık, 2025.

Kaya, Mehmet Bedii, ve Furkan Güven Taştan. “Kişisel Veri Koruma Hukuku - Mevzuat, İçtihat, Bibliyografya”. Çevrimiçi Sürüm 3.0, 2025.

Kayas, Oliver G. “Workplace Surveillance: A Systematic Review, Integrative Framework, and Research Agenda”. Journal of Business Research 168 (Kasım 2023): 114212.

Kayıhan, Şaban, ve Mustafa Ünlütepe. Borçlar Hukuku Genel Hükümler. Seçkin Yayıncılık, 2018.

Kaynar, Damla, ve İştar Urhanoğlu. “İşçinin Ulaşılamama Hakkı”. Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi 21, sy Özel Sayı (2024): 319-82.

Kemiksiz, Rukiye Civan. “Kişisel veri güvenliği üzerine bir alan araştırması: dijital yerliler ve dijital göçmenlerin güvenlik algıları”. Maltepe Üniversitesi İletişim Fakültesi Dergisi 9, sy 1 (2022): 64-91.

Kerr, Orin S. “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & (and) the USA Patriot Act: Surveillance Law: Reshaping the Framework”. George Washington Law Review 72, sy 6 (2003): 1208-43.

Keyes, Jessica. Bring Your Own Devices (BYOD) Survival Guide. CRC Press Taylor & Francis Group, 2016.

Kıpçak, Hazar Can. Çalışanların Kişisel Verilerinin İş İlişkisi Kapsamında Korunması. Seçkin Yayıncılık, 2023. https://www.seckin.com.tr/kitap/263371922.

Kırılmaz, Selma Kılıç, ve Çağdaş Ateş. “İşe Alımlarda Yapay Zekâ Kullanımı: Kavramsal Bir Değerlendirme”. Journal of Business and Trade 2, sy 1 (2021): 37-48.

Kişisel Verileri Koruma Kurumu. 6698 sayılı Kanunda Yer Alan Temel Kavramlar. Kişisel Verileri Koruma Kurumu, 2020.

Kişisel Verileri Koruma Kurumu. Açık Rıza. Kişisel Verileri Koruma Kurumu, 2020. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf.

Kişisel Verileri Koruma Kurumu. Kanunlarda Öngörülme Kişisel Veri İşleme Şartına İlişkin Bilgi Notu. No. 62. Kişisel Verileri Koruma Kurumu, 2025.

Kişisel Verileri Koruma Kurumu. Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler). Kişisel Verileri Koruma Kurumu, 2018. https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf.

Kişisel Verileri Koruma Kurumu. Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler). No. 72. Kişisel Verileri Koruma Kurumu, 2025.

Kişisel Verileri Koruma Kurumu. Kişisel Veri Saklama ve İmha Politikası. Kişisel Verileri Koruma Kurumu, 2017.

Kişisel Verileri Koruma Kurumu. Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü. No. 68. Kişisel Verileri Koruma Kurumu, 2025.

Kişisel Verileri Koruma Kurumu. Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Rehber. C. 51. KVKK Yayınları, 2025.

Korkmaz, Ali. “İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması”. Karamanoğlu Mehmetbey Üniversitesi Sosyal Ve Ekonomik Araştırmalar Dergisi 2014, sy 3 (2014): 99-103.

Korkmaz, İbrahim. “Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme”. TBB Dergisi, sy 124 (2016): 81-152.

Koulu, Riikka. “Human Control Over Automation: Eu Policy and Ai Ethics”. EU Policy and AI Ethics 12, sy 1 (2020): 9-46.

Koulu, Riikka. “Proceduralizing Control and Discretion: Human Oversight in Artificial Intelligence Policy”. Maastricht Journal of European and Comparative Law 27, sy 6 (2020): 720-35.

KPMG. “KPMG 2024 CEO Outlook - KPMG Turkey”. 02 Aralık 2024. https://kpmg.com/tr/en/home/insights/2024/12/2024-ceo-outlook.html.

Kresge, Lisa. Data and Algorithms in the Workplace: A Primer on New Technologies. t.y.

Kuban, Arzu. “Yeni İstihdam Türleri Bakımından İşçi Kavramı, İş ve Sosyal Güvenlik Hukukunda İşçi ve İşveren Kavramları ve Ortaya Çıkan Sorunlar”. Prof. Dr. Kemal Oğuzman Anısına, İstanbul Barosu-Galatasaray Üniversitesi, İstanbul, 1997.

Kutlu, Melis. İş Hukukunda Tele Çalışma. On İki Levha Yayıncılık, 2025.

Kutlu, Merve, ve Ali Uçar. “Tarafların Hak ve Borçları Kapsamında Koronavirüs Pandemisinde Uzaktan Çalışma”. İçinde İş Hukukunda Yeni Yaklaşımlar V., editör Kübra Doğan Yenisey ve Seda Ergüneş Emrağ. On İki Levha Yayıncılık, 2022.

Küzeci, Elif. Kişisel Verilerin Korunması Hukuku. 4. On İki Levha Yayıncılık, 2021.

Küzeci, Elif, ve Şebnem Kılıç. “6698 Sayılı Kişisel Verilerin Korunması Kanunu’nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler”. Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi 16, sy 63 (2019): 947-92.

KVKK. “‘Alenileştirme’ Hakkında Kamuoyu Duyurusu”. KİŞİSEL VERİLERİ KORUMA KURUMU, 16 Aralık 2020. https://www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU.

KVKK. Kişisel Veri İşleme Envanteri Hazırlama Rehberi. No. 61. Ankara, 2025.

KVKK. Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi. No. 58. 2025. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf.

KVKK. Unutulma Hakkı (Unutulma Hakkının Arama Motorları Özelinde Değerlendirilmesi). No. 73. Ankara, 2025.

Lapuelle, Myrtille. “Are You Monitoring Your French Employees? Make Sure You Have Registered That Activity with the CNIL!” OF DIGITAL INTEREST, 31

Ekim 2014. https://www.ofdigitalinterest.com/2014/10/are-you-monitoring-your-french-employees-make-sure-you-have-registered-that-activity-with-the-cnil/.

Lecher, Colin. "How Amazon Automatically Tracks and Fires Warehouse Workers for 'Productivity'". The Verge, 25 Nisan 2019. https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations.

Levy, Karen, ve Solon Barocas. "Privacy at the Margins| Refractive Surveillance: Monitoring Customers to Manage Workers". International Journal of Communication 12 (2018): 23.

Limoncuoğlu, Yiğit Efe. "İşçiye Ait Kişisel Verilerin Korunması". Yayınlanmamış Yüksek Lisans Tezi, İzmir Ekonomi Üniversitesi, 2022.

Llave, O. V., J. Hurley, E. Peruffo, vd. The Rise in Telework: Impact on Working Conditions and Regulations. European Foundation for the Improvement of Living and Working Conditions (Eurofound), 2022.

López Ribalda and Others v. Spain, 1874/13, 8567/13 (AİHM 17 Ekim 2019). https://hudoc.echr.coe.int/fre?i=001-197098.

LTO. "BAG zu Kündigungsprozess: Keylogger-Daten unverwertbar". Legal Tribune Online. Erişim 12 Nisan 2025. https://www.lto.de/recht/hintergruende/h/bag-urteil-2azr68116-arbeitgeber-ueberwachung-dienst-pc-keylogger-beweise-unverwertbar.

Lyell, David, ve Enrico Coiera. "Automation bias and verification complexity: a systematic review". Journal of the American Medical Informatics Association 24, sy 2 (2017): 423-31.

Madhumita, G, P. Dolly Diana, Neena PC, P B Narendra Kiran, Swati Aggarwal, ve Amarja Satish Nargunde. "AI-powered Performance Management: Driving Employee Success and Organizational Growth". 2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST), Nisan 2024, 204-9. https://ieeexplore.ieee.org/document/10578371.

Madinier, Franca Salis. A Guide to Artificial Intelligence at the Workplace. European Economic and Social Committee, 2021.

Mahlangu, B.S., ve B. Schutte. "Analysing Information Technology Risks Affecting South African Government Employers Due to Remote Working". Journal for New Generation Sciences 22, sy 2 (2024). http://journals.co.za/doi/10.47588/jngs.2024.22.02.a1.

Manav, A. Eda. "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması". Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 19, sy 2 (2015): 95-136.

Manav Özdemir, A. Eda. "İşçinin İzlenmesi ve Gözetlenmesi". İçinde Muhtelif Yönleriyle Kişisel Verilerin Korunması Hukuku, editör Kemal Şenocak. Yetkin Yayınları, 2022.

Manokha, Ivan. "New Means of Workplace Surveillance". Monthly Review, 01 Şubat 2019, 25-39.

Mapsted Blog. "Do Wi-Fi Indoor Positioning Systems Still Make Sense in 2025?" Erişim 03 Mart 2025. https://mapsted.com/en-in/blog/wifi-positioning-system-explained.

Mark H. Francis ve Sophie L. Kletzien. "New York Law Requires Notice of Employees' Electronic Monitoring Effective May 7, 2022". Holland & Knight LLP, 03 Mayıs 2022. https://www.hklaw.com/en/insights/publications/2022/05/new-york-law-requires-notice-of-employees-electronic-monitoring.

Martín-Romo Romero, Santiago, ve Carmen De-Pablos-Heredero. "Data Protection by Design: Organizational Integration". Harvard Deusto Business Research 7, sy 2 (2018): 60-71.

Marx, Gary T. "Surveillance Studies". İçinde International Encyclopedia of the Social & Behavioral Sciences (Second Edition), editör James D. Wright. Elsevier, 2015.

Maya, Duygu. "6698 Sayılı Kişisel Verilerin Korunması Kanunu Çerçevesinde Bulut Bilişim Sistemleri". Yayınlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, 2023.

Merkelson, Jeremy Ben, Wendy Kearns, Michael Borgia, ve Tanner Harris. "Neurotechnology In The Workplace: A Futuristic Reality". Mealey's Data Privacy Report (LexisNexis) 9, sy 6 (2023): 18-28.

Merkelson, Jeremy Ben, Wendy Kearns, David Rice, ve Elyse Sparks. "Neurotechnology Works Its Way Forward". Seattle University Law Review Online 48, sy 57 (2025).

Microsoft. "Uç Nokta Nedir?" Erişim 04 Haziran 2025. https://www.microsoft.com/tr-tr/security/business/security-101/what-is-an-endpoint.

Minielly, Nicole, Viorica Hrincu, ve Judy Illes. "Privacy Challenges to the Democratization of Brain Data". iScience 23, sy 6 (2020): 101134.

Molè, Michele, ve Aida Ponce Del Castillo. "Worker Monitoring Vs Worker Surveillance: The Need for a Legal Differentiation". İçinde Artificial intelligence, labour and society, editör Aida Ponce Del Castillo. European Trade Union Institute, 2024. https://www.etui.org/publications/artificial-intelligence-labour-and-society.

Mollamahmutoğlu, Hamdi, ve Muhittin Astarlı. İş Hukuku. 5. Turhan Kitabevi, 2012.

Mollamahmutoğlu, Hamdi, Muhittin Astarlı, ve Ulaş Baysal. İş Hukuku. Güncellenmiş 7. Lykeion, 2022.

Monitask. "What Is Webcam Monitoring?" Erişim 22 Şubat 2025. https://www.monitask.com/en/business-glossary/webcam-monitoring.

Morrison, Kathleen. "Is It Legal to Record Video Meetings?" Lexology, 19 Ağustos 2020. https://www.lexology.com/library/detail.aspx?g=1d582939-2279-42cb-9892-ae088c2f9396.

Mostowy, Walter A. "Explaining Opaque AI Decisions, Legally". Berkeley Technology Law Journal 35, sy 4 (2020): 1291-330.

Muenchinger, Nancy E. "Workplace Privacy - France: Electronic Workplace Privacy in France". Computer Law & Security Report 18, sy 6 (2002): 421-26.

Muhl, Ekaterina. "The Challenge of Wearable Neurodevices for Workplace Monitoring: An EU Legal Perspective". Frontiers in Human Dynamics 6 (Ekim 2024). https://www.frontiersin.orghttps://www.frontiersin.org/journals/human-dynamics/articles/10.3389/fhumd.2024.1473893/full.

Muhl, Ekaterina, ve Roberto Andorno. "Neurosurveillance in the Workplace: Do Employers Have the Right to Monitor Employees' Minds?" Frontiers in Human Dynamics 5 (2023).

Mustafa Dural ve Tufan Öğüz. Türk Özel Hukuku Cilt II Kişiler Hukuku. 24. Baskı. Filiz Kitabevi, 2024.

Naufel, Stephanie, ve Eran Klein. "Brain–Computer Interface (BCI) Researcher Perspectives on Neural Data Ownership and Privacy". Journal of Neural Engineering 17, sy 1 (2020): 016039.

Nayem, Zannatul, ve Md. Aftab Uddin. "Unbiased employee performance evaluation using machine learning". Journal of Open Innovation: Technology, Market, and Complexity 10, sy 1 (2024): 100243.

Nita A. Farahany. "Neurotech at Work". Harvard Business Review, Mart 2023. https://hbr.org/2023/03/neurotech-at-work.

Nurata, Zeynep Ceren. "Hukuksal, Örgütsel ve Etik Bir Sorun Olarak İşyerinde Elektronik Gözetim". Gazi İktisat ve İşletme Dergisi 7, sy 3 (2021): 214-25.

O'Connor v. Ortega 480 U.S. 709 (1987), No. 86-630 (Supreme Court of The United States 31 Mart 1987). https://supreme.justia.com/cases/federal/us/480/709/.

Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization". UCLA Law Review 57, sy 6 (2009): 1701-78.

Okur, Zeki. İş Hukuku'nda Elektronik Gözetleme. Legal Yayıncılık, 2011.

Olalere, Morufu, Mohd Taufik Abdullah, Ramlan Mahmod, ve Azizol Abdullah. “A Review of Bring Your Own Device on Security Issues”. Sage Open 5, sy 2 (2015): 2158244015580372. https://doi.org/10.1177/2158244015580372.

Ontario v. Quon, 560 U.S. 746 (2010), No. 08-1332 (Supreme Court of The United States 17 Haziran 2010). https://supreme.justia.com/cases/federal/us/560/746/.

Opsiocloud. Internet of Things Supply Chain & Logistics Optimization. 26 Şubat 2025. https://opsiocloud.com/iot-supply-chain-logistics/.

Ozan Özparlak, Başak. Büyük Veri Çağında Yapay Zeka Sistemlerinin Çalışma İlişkilerinde Kullanımı: Hukuki Bir Değerlendirme. Onikilevha Yayıncılık, 2021.

Öğretmen Kotil, Zeynep. Kişisel Verilerin Korunması Çerçevesinde Yapay Zeka. Oniki Levha Yayıncılık, 2022.

Özbudun, Ergun. “Anayasa Hukuku Bakımından Özel Haberleşmenin Gizliliği”. Ankara Üniversitesi Hukuk Fakültesi 50.Yıl Armağanı 1, sy 50 (1977): 1925-77.

Özdemir Coşkun, Nazlıhan. “Kişisel Verilerin Korunması ve İşlenmesi”. Yayınlanmamış Yüksek Lisans Tezi, Kadir Has üniversitesi, 2022.

Özdemir, Erdem. “İnternet ve İş Sözleşmesi: Yeni Teknolojilerin İş İlişkisine Etkileri Üzerine”. Sicil İş Hukuku Dergisi Yıl:3, sy 10 (2008).

Özdemir, Erdem. “Uzaktan Çalışma Yönetmeliği Karşısında Tele Çalışma”. Çimento İşveren Dergisi 35, sy 3 (2021): 8-41.

Özdemir, Hayrunnisa. “İşyerinde İşçilerin İzlenmesi ve İşçinin Kişilik Haklarının Korunması”. Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi 14, sy 1-2 (2010): 231-70.

Özer Deniz, Miray. “Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk”. Doktora Tezi, Çukurova Üniversitesi, 2022.

Özer, Hazan Dicle. “Mobese İzleme ve Kayıtları: Gözetim Toplumu Bağlamında Bir Değerlendirme”. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 24, sy 1 (2022): 1.

Özparlak, Başak Ozan, ve Müge Çetin. “ChatGPT ve Üretici Yapay Zekâ Modellerinde Mahremiyet ve Güvenliğin Hukuki Boyutu”. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 29, sy 2 (2023): 2.

Öztunay, Begüm. “6698 Sayılı Kişisel Verilerin Korunması Kanunu Işığında İşverenin Yönetim Hakkının Sınırları”. Yüksek Lisans Tezi, İzmir Ekonomi Üniversitesi Sosyal Bilimler Enstitüsü, 2019.

Öztürk İnal, Beyza. Uzaktan Çalışma. Platon Hukuk, 2022.

Öztürk, Yaren Sena. “Kişisel Verilerin Korunmasında Yapay Zekânın Rolü”. Yüksek Lisans Tezi, Antalya Bilim Üniversitesi, 2024.

Palacios, Rebecca, ve George Penn. “Beyond Remote Work: The Hybrid Workforce Model”. Gartner, 2020.

Parlak, Seda. “İş İlişkisinde İşçinin İnternet ve E-Posta Kullanımının İzlenmesi ve Gözetlenmesi”. Yayınlanmamış Yüksek Lisans Tezi, Ankara Hacı Bayram Veli Üniversitesi, 2023.

Pastukhov, Oleksandr. “The right to oblivion: what’s in the name”. Computer and, 2013. https://www.academia.edu/download/62248500/Right_to_oblivion20200302-46205-1qfuknw.pdf.

Patel, Keyur K, Sunil M Patel, ve PG Scholar. “Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges”. International Journal of Engineering Science and Computing 6, sy 5 (2016): 6122-31.

“People Counting | Occupancy | Retail Analytics | RetailNext”. Erişim 16 Şubat 2025. https://retailnext.net/.

Pero, Angelica Salvi del, Peter Wyckoff, ve Ann Vourc’h. Using Artificial Intelligence in the Workplace: What Are the Main Ethical Risks? OECD, 2022. https://www.oecd-ilibrary.org/social-issues-migration-health/using-artificial-intelligence-in-the-workplace_840a2d9f-en.

Pletcher, Scott Nicholas. “Practical and Ethical Perspectives on AI-Based Employee Performance Evaluation”. OSF Preprints, OSF Preprints, Center for Open Science, 28 Nisan 2023, 29yej. https://ideas.repec.org//p/osf/osfxxx/29yej.html.

Porcius, Isabela. “The Rise of Telework and the Struggle Towards Cyber Security”. Fiat Iustitia 1, sy 1 (2021): 148-57.

Rak, Richard. “Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS)”. European Journal of Risk Regulation 15, sy 4 (2024): 928-38.

Rakha, Naeem Allah. “Ensuring Cyber-security in Remote Workforce: Legal Implications and International Best Practices”. International Journal of Law and Policy 1, sy 3 (2023).

Raso, Emanuele, Pierpaolo Loreti, Michele Ravaziol, ve Lorenzo Bracciale. “Anonymization and Pseudonymization of FHIR Resources for Secondary Use of Healthcare Data”. IEEE Access 12 (2024): 44929-39. https://doi.org/10.1109/ACCESS.2024.3381034.

Ratti, Luca, ve Antonio García-Muñoz. “The Regulation of Remote Work. Seeking Balance Through the Articulation of Labour Law Sources: A Comparative Appraisal”. International Journal of Comparative Labour Law and Industrial Relations 40, sy Issue 3 (2024): 303-28.

Ravid, Daniel M., David L. Tomczak, Jerod C. White, ve Tara S. Behrend. “EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring”. Journal of Management 46, sy 1 (2020): 100-126.

Regulation of Investigatory Powers Act 2000, c. 23 (2000). https://www.legislation.gov.uk/ukpga/2000/23.

Reilly, Simon Mark. “The Use of Electronic Surveillance and Performance Measures in the Workplace: A Qualitative Investigation”. Durham theses, Durham University, 2010. http://etheses.dur.ac.uk/429/.

RFID Construction Worker Tracking: Enhancing Efficiency n’ Safety on Site. RFID. 24 Mayıs 2024. https://cpcongroup.com/rfid-construction-worker-tracking/.

Riso, Sara. Working Conditions - Employee Monitoring and Surveillance: The Challenges of Digitalisation. European Foundation for the Improvement of Living and Working Conditions (Eurofound), 2020.

Riso, Sara, ve Chiara Litardi. “Employee Monitoring: A Moving Target for Regulation”. Eurofound, 15 Temmuz 2024. https://www.eurofound.europa.eu/en/resources/article/2024/employee-monitoring-moving-target-regulation.

Rodrigues, Rowena, David Barnard-Wills, Paul De Hert, ve Vagelis Papakonstantinou. “The Future of Privacy Certification in Europe: An Exploration of Options Under Article 42 of the GDPR”. International Review of Law, Computers & Technology 30, sy 3 (2016): 248-70. https://doi.org/10.1080/13600869.2016.1189737.

Sánchez-Monedero, Javier, ve Lina Dencik. “The Datafication of The Workplace”. Cardiff University, datajusticeproject. net, 2019. https://orca.cardiff.ac.uk/id/eprint/125552/1/Report-The-datafication-of-the-workplace.pdf.

Sarıbay, Banu. “Uzaktan Çalışma Üzerine Sosyolojik Bir Değerlendirme”. Sosyoloji Dergisi, sy 46 (2023): 221-41.

Sarıbay Öztürk, Gizem. “İşverenin İşçileri ve Adayları Sosyal Medya Vasıtasıyla Araştırması”. İçinde İş Hukukunda Yeni Yaklaşımlar IV., editör Kübra Doğan Yenisey ve Seda Ergüneş Emrağ. On İki Levha Yayıncılık, 2021.

Savaş, F. Burcu. “İş Hukukunda ‘Siber Gözetim’”. Çalışma ve Toplum 3, sy 22 (2009): 97-132.

Savaş Kutsal, F. Burcu. İşçinin Ulaşılabilir Olmama Hakkı Güncel Çalışma Koşulları ve Karşılaştırmalı Hukuk Işığında Türk İş Hukuku İçin Tespit ve Öneriler. İş Hukuku Monografileri. Seçkin, 2024.

Savcı, İlkay. "İşyerlerinde Elektronik Denetim ve Gözetim". İçinde Küreselleşme Emek Süreçleri ve Yapısal Uyum, editör Ahmet Alpay Dikmen. İmaj Yayıncılık, 2002.

Savran, Rümeysa. "İşçinin İşyerinde Elektronik Yöntemlerle İzlenmesi". Yüksek Lisans Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, 2023.

Scarfone, Karen, Paul Hoffman, ve Murugiah Souppaya. "Guide to enterprise telework and remote access security". NIST Special Publication 800, sy 2009 (2009): 46.

Seçkin, Muhammed Türkalp. "İşverenin Araç ve Malzeme Sağlama ile Giderlere Katlanma Borcu". Doktora Tezi, Marmara Üniversitesi, 2024.

Senyen Kaplan, Emine Tuncay. Bireysel İş Hukuku. 2. Yetkin Yayınevi, 2023.

Senyen Kaplan, Emine Tuncay. Bireysel İş Hukuku. 2. bs. Yetkin, 2023.

Ses, Sencer Metin, ve Refik Korkusuz. "İş İlişkisinde Kişisel Verilerin Yapay Zeka Destekli Sistemler Yardımıyla İşlenmesi". Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi 6, sy 2 Prof. Dr. Mustafa Avcı'ya Armağan (2025): 2 Prof. Dr. Mustafa Avcı'ya Armağan.

Sevak, Kunal Yogen, ve Babu George. "The Evolution of Internet of Things (IoT) Research in Business Management: A Systematic Review of the Literature". Journal of Internet and Digital Economics 4, sy 3 (2024): 242-65.

Sevimli, K. Ahmet. "İşçinin Özel Yaşam Hakkı Bağlamında İşçi İşveren İlişkisi". Sicil İş Hukuku Dergisi, sy 10 (2008): 53-79.

Sevimli, K. Ahmet. İşçinin Özel Yaşamına Müdahalenin Sınırları. Legal, 2006.

Sevimli, K. Ahmet. "Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419". Sicil İş Hukuku Dergisi, Yıl 4, sy 24 (2011): 122-41.

Sewell, G., ve J. Barker. "Performance Measurement as Surveillance: When (If Ever) Does 'Measuring Everything That Moves' Become Oppressive". Unpublished manuscript, University of Melbourne, Parkville, Australia, 2008.

Sewell, Graham, ve James R. Barker. "Coercion Versus Care: Using Irony to Make Sense of Organizational Surveillance". Academy of Management Review 31, sy 4 (2006): 934-61.

Sezgin, Serhat. İş İlişkisinde İşçinin Kişilik Haklarına Yönelik Müdahaleler. Seçkin, 2024.

Sharma, Kuldeep, Jenish Sukheswala, Brijendra Singh Yadav, Gaurav Vishnu Londhe, Rohit Singh, ve Harikumar Pallathadka. "A Method Leveraging AI to Forecast Employee Performance during Work Hours and Propose Appropriate Salary Adjustments". 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Mayıs 2024, 1-6. https://ieeexplore.ieee.org/document/10601739.

SHRM. "Managing Workplace Monitoring and Surveillance". 20 Haziran 2024. https://www.shrm.org/topics-tools/tools/toolkits/managing-workplace-monitoring-surveillance.

Siegel, Rudolf, Cornelius J. König, ve Veronika Lazar. "The Impact of Electronic Monitoring on Employees' Job Satisfaction, Stress, Performance, and Counterproductive Work Behavior: A Meta-Analysis". Computers in Human Behavior Reports 8 (Aralık 2022): 100227.

Skitka, Linda J., Kathleen L. Mosier, ve Mark Burdick. "Does automation bias decision-making?" International Journal of Human-Computer Studies 51, sy 5 (1999): 991-1006. https://doi.org/10.1006/ijhc.1999.0252.

Skubis, Ida, ve Krzysztof Wodarski. "HUMANOID ROBOTS IN MANAGERIAL POSITIONS – DECISION-MAKING PROCESS AND HUMAN OVERSIGHT". Scientific Papers of Silesian University of Technology. Organization and Management Series 2023, sy 189 (2023): 573-96. https://doi.org/10.29119/1641-3466.2023.189.36.

Sládek, Pavel, ve Tomáš Sigmund. "Legal Issues of Teleworking". SHS Web of Conferences 90 (2021): 01020. https://www.shs-conferences.org/articles/shsconf/abs/2021/01/shsconf_eccw2020_01020/shsconf_eccw2020_01020.html.

Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (United States District Court, E.D. Pennsylvania. 23 Ocak 1996). https://law.justia.com/cases/federal/district-courts/FSupp/914/97/2131293/.

"Social and Economic Committee (ESC)". Erişim 30 Haziran 2025. https://entreprendre.service-public.fr/vosdroits/F34474/personnalisation/resultat?lang=en.

Somasundaram, S Prakash. "Enhancing Organizational Data Protection: Advanced Security Measures for Database Systems". International Journal of Research in Computer Applications and Information Technology 6, sy 1 (2023): 58-62.

Soysal, Tamer. "Tele Çalışma". Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi 1, sy 9 (2006): 133-65.

Spot AI. "What to Look for in a Video Surveillance Management System". Erişim 22 Şubat 2025. https://www.spot.ai/blog/best-video-surveillance-management.

Stafford, V. “Zero trust architecture”. NIST special publication 800, sy 207 (2020): 1-50.

Stengart v. Loving Care Agency, Inc. (A-16-09), Nos. 300, 990 A.2d 650 (Supreme Court of New Jersey 30 Mart 2010). https://law.justia.com/cases/new-jersey/supreme-court/2010/a-16-09-opn.html.

Sümer, Halûk Hâdi. İş Hukuku. Güncellenmiş 27. Seçkin Yayıncılık, 2024.

Sümer, Halûk Hâdi. “İş Sözleşmesinin Bağımlılık Unsuru”. Sicil İş Hukuku Dergisi 19 (2010): 63-73.

Süzek, Sarper. “İş Akdinin Türleri”. Mercek Dergisi, sy 22 (2001): 17-35.

Süzek, Sarper. İş Hukuku. Yenilenmiş 8.Baskı. Beta, 2012.

Süzek, Sarper. “Yeni Türk Borçlar Kanunu Çerçevesinde İş Akdinin Geçersizliği”. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi / Prof.Prof. Dr. Ali Rıza Okur’a Armağan 20, sy 1 (2014): 1.

Süzek, Sarper. “Yeni Türk Borçlar Kanunu Çerçevesinde İşçinin Rekabet Etmeme Borcu”. Journal of Istanbul University Law Faculty 72, sy 2 (2014). https://dergipark.org.tr/en/download/article-file/97936.

Süzek, Sarper, ve Süleyman Başterzi. İş Hukuku. 24. bs. Beta, 2024.

Şahin Yunak, Ayşe. “İş Hukukunda Kişisel Verilerin Korunması”. Yayınlanmamış Yüksek Lisans Tezi, KTO Karatay Üniversitesi, 2023.

Şakar, Müjdat, ve Duygu Erkan Şahin. “Esnek Çalışma Modellerinden Uzaktan Çalışma ve Uzaktan Çalışanların Sigortalılığı”. SGD-Sosyal Güvenlik Dergisi 11, sy 2 (2021): 249-67.

Şanlı, Can. “İş Hukukunda Uzaktan Çalışma”. Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, 2023.

Şimşek, Oğuz. Anayasa Hukukunda Kişisel Verilerin Korunması. Beta, 2008.

Taştan, Furkan Güven. Türk Sözleşme Hukukunda Kişisel Verilerin Korunması. 2. Baskı. On İki Levha Yayıncılık, 2017.

Team, GeoPlugin. “IP Tracer: Top Methods and Use Cases - GeoPlugin - Resources”. GeoPlugin - Resources -, 05 Kasım 2024. https://www.geoplugin.com/resources/ip-tracer-top-methods-and-use-cases/.

Team, HR Solutions Blog. “Workplace Monitoring: What’s Allowed, What’s Off Limits?” Erişim 13 Nisan 2025. https://sbshrs.adpinfo.com/blog/workplace-monitoring-whats-allowed-whats-off-limits.

Technology Innovators. Internet of Things (IoT) in Logistics: Real-Time Tracking and Asset Management. 19 Mayıs 2023. https://www.technology-innovators.com/internet-of-things-iot-in-logistics-real-time-tracking-and-asset-management/.

Tekergül, Mehmet. "İşyerinde Elektronik Gözetim Uygulamaları". Yüksek Lisans Tezi, Kadir Has üniversitesi, 2010.

The Data Will See You Now: Datafication and the Boundaries of Health. Ada Lovelace Institute, 2020. https://www.adalovelaceinstitute.org/report/the-data-will-see-you-now/.

The Impact of AI on the Workplace: Main Findings from the OECD AI Surveys of Employers and Workers. OECD Social, Employment and Migration Working Papers No. 288. C. 288. OECD Social, Employment and Migration Working Papers. 2023. https://doi.org/10.1787/ea0a0fe1-en.

The Privacy and Electronic Communications (EC Directive) Regulations 2003, S.I. 2003 No. 2426 (2003). https://www.legislation.gov.uk/uksi/2003/2426/contents/made.

Thönißen, Klaus. "Perennial Issue: Software Vs. Co-Determination (Section 87 (1) No. 6 BetrVG) - On the Trials and Tribulations of the German Federal Labour Court". Blog. LUTHER, 26 Mayıs 2021. https://www.luther-lawfirm.com/en/newsroom/blog/detail/dauerbrenner-software-vs-mitbestimmung-87-abs-1-nr-6-betrvg.

Thumala, Srinivasa Rao. "Running Sustainable Virtual Desktop Infrastructure (VDI) Solutions in the Cloud". International Journal on Recent and Innovation Trends in Computing and Communication 9, sy 12 (2021): 91-102.

Tikkinen-Piri, Christina, Anna Rohunen, ve Jouni Markkula. "EU General Data Protection Regulation: Changes and implications for personal data collecting companies". Computer Law & Security Review 34, sy 1 (2018): 134-53. https://doi.org/10.1016/j.clsr.2017.05.015.

Tolu Yılmaz, Hazal. Dijital Platform Çalışanlarının Hukuki Statüsü (İş ve Sosyal Güvenlik Hukuku Bakımından). On İki Levha Yayıncılık, 2023.

"Track GPS Location Of Any Smartphone | TrackMyFone". Erişim 27 Şubat 2025. https://www.trackmyfone.com/gps-tracking.html.

Tuna, Ayşen Akbaş, ve Zafer Türkmendağ. "Covid-19 Pandemi Döneminde Uzaktan Çalışma Uygulamaları ve Çalışma Motivasyonunu Etkileyen Faktörler". İşletme Araştırmaları Dergisi 12, sy 3 (2020): 3246-60.

Tuna, Mustafa Çağrı. "Kişisel Verilerin Korunması Hukuku ve Şirketlerin Yükümlülükleri". Yayınlanmamış Doktora Tezi, Erciyes Üniversitesi, 2024.

Tuncay, A. Can. “Pandemi Gölgesinde Evden Çalışma”. Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi 18, sy 72 (2021): 23-52.

Tunç Yılmaz, Pelin. “Uzaktan Çalışmanın Bir Türü Olarak Evde Çalışma”. Sicil İş Hukuku Dergisi, sy 43 (2020): 254-73.

Turan Başara, Gamze. “Kişisel Verilerin Korunması Kanunu’nun 6. Maddesinde Yapılan Değişiklik Bağlamında Özel Nitelikli Kişisel Verilerin İşlenmesi”. Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 28, sy 4 (2024): 4.

Ugan Çatalkaya, Deniz. İş Hukukunda Ölçülülük İlkesi. Beta, 2019.

Ulaş Baysal. “Şüphe Feshi Kavramı ve Bu Konuda Yargıtay Kararlarının Hukuki Değerlendirilmesi”. Sicil İş Hukuku Dergisi, sy 35 (2016): 83-97.

UN General Assembly. Guidelines for the Regulation of Computerized Personal Data Files. UN General Assembly, 1990. https://www.refworld.org/policy/legalguidance/unga/1990/en/13761.

Uncular, Selen. İş İlişkisinde İşçinin Kişisel Verilerinin Korunması. 2. Baskı. Seçkin, 2018.

Uncular, Selen. “Teknolojinin Etkisiyle Dönüşen İş İlişkisinde Giriş Kontrol Sistemleri, Yer Belirleme Sistemleri ve Sosyal Medya Vasıtasıyla İzleme”. Çalışma ve Toplum 3, sy 66 (2020): 1673-700.

Urhanoğlu, İştar, Yeliz Bozkurt Gümrükçüoğlu, Gülnihal Ahter Yakacak, ve Abdülmecit Güldağı. “İşçinin Unutulma Hakkı”. İçinde İnsana Yakışır Iş Serisi: 1. Cilt, c. 1. İbn Haldun Üniversitesi Yayınları, 2025.

Uşan, M. Fatih. İş ve Sosyal Sigorta Hukuku Uygulamasında Parça Başına Ücret. Seçkin Yayıncılık, 2003.

“Uzaktan Çalışma Öldi mü? İmdi Yürek Yırtılır”. Erişim 17 Eylül 2025. https://incturkiye.com/makaleler/uzaktan-calisma-oldi-mu-imdi-yurek-yirtilir?uuid=sAUPWH3Gp.

Ünal Adınır, Canan. “Tele çalışmada verilerin korunması”. İçinde Muhtelif Yönleriyle Kişisel Verilerin Korunması Hukuk, editör Kemal Şenocak. Yetkin, 2022.

Ünal, Emre. “İşçinin Ulaşılamama Hakkı”. Yayınlanmamış Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, 2023.

Üstün, Yasin, ve Ayşe Günal. “İş İlişkilerinde Bazı Yaygın Uygulamaların Kişisel Verilerin Korunması Kanunu Kapsamında Değerlendirilmesi”. Kişisel Verileri Koruma Dergisi 2, sy 2 (2020): 62-73.

Vanneste, Bart S, ve Phanish Puranam. “Artificial Intelligence, Trust, and Perceptions of Agency”. Academy of Management Review, 2024.

"Veri sorumlusu tarafından aydınlatma yükümlülüğü ve açık rıza onayı alınması süreçlerinin ayrı ayrı yerine getirilmesi gerektiği ile ilgili" Kişisel Verileri Koruma Kurulunun Kararı, No. 2018/90 (26 Temmuz 2018). https://www.kvkk.gov.tr/Icerik/5420/2018-90.

Vicci, Dr. Heidrich. "The Impact of IoT on the Modern World A Review and Evaluation Study". SSRN Electronic Journal, 2024. https://www.ssrn.com/abstract=4818308.

Voigt, Paul, ve Nils Hullen. The EU AI Act: Answers to Frequently Asked Questions. Springer Berlin Heidelberg, 2024. https://doi.org/10.1007/978-3-662-70201-7.

Wachter, Sandra, Brent Mittelstadt, ve Chris Russell. "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR". Harv. JL & Tech. 31 (2017): 841.

Wagner, Ben. "Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems". Policy & Internet 11, sy 1 (2019): 104-22. https://doi.org/10.1002/poi3.198.

Warzel, Charlie. "Opinion | All Your Data Is Health Data". Opinion. The New York Times, 13 Ağustos 2019. https://www.nytimes.com/2019/08/13/opinion/health-data.html.

Wexler, Anna, ve Peter B. Reiner. "Oversight of Direct-to-Consumer Neurotechnologies". Science 363, sy 6424 (2019): 234-35.

"What Is Data Segregation?" PrivacyEngine Data Protection Software and Solutions, t.y. Erişim 07 Haziran 2025. https://www.privacyengine.io/resources/glossary/data-segregation/.

"What Is the Difference between Teramind Starter, Teramind UAM, Teramind DLP and Teramind Enterprise? | Teramind Knowledge Base". Erişim 27 Şubat 2025. https://kb.teramind.co/en/articles/8790885-what-is-the-difference-between-teramind-starter-teramind-uam-teramind-dlp-and-teramind-enterprise.

"What Is Virtual Desktop Infrastructure (VDI)? | Microsoft Azure". Erişim 13 Haziran 2025. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-virtual-desktop-infrastructure-vdi.

Yıldız, Canberk. "Bir Gözetim Tekniği Olarak Kapalı Devre Kameraların Kullanılması ve Kişisel Verilerin Korunması". Yayınlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, 2022.

Yılmaz, Berrak. "Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması". Doktora Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, 2019.

Yılmaz, Gözde. “Elektronik Performans İzleme Sistemlerinin Çalışanlar ve İşletmeler Üzerindeki Etkileri”. İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi 4, sy 7 (2005): 1-19.

Yılmaz, Süleyman, ve Gökçe Çavuşoğlu. Kişisel Verileri Koruma Hukuku. Yetkin Yayınları, 2020.

Yiğit, Esra. İş İlişkisinde Kişisel Verilerin Korunması. Güncellenmiş 2. Baskı. On İki Levha Yayıncılık, 2023.

Yiğit, Yusuf. “Yargı Kararları Işığında İşçinin Sosyal Medya Paylaşımı Nedeniyle İş Sözleşmesinin İşverence Feshinin Koşulları”. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 26, sy 2 (2024): 975-1019.

Yücedağ, Nafiye. “Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler”. Kişisel Verileri Koruma Dergisi 1, sy 1 (2019): 1.

Yücedağ, Nafiye. “Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri”. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 75, sy 2 (2017): 765-90.

Yücel, Orhan Ürüncan. “İşçilerin Sosyal Medya Paylaşımlarının İşveren Tarafından Denetimi ve İş İlişkisine Etkisi”. Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2018.

Zarrabi, Fatemeh, Isabel Wagner, ve Eerke Boiten. “Changes in Conducting Data Protection Risk Assessment and After GDPR Implementation”. Preprint, Leicester, UK, 24 Nisan 2023. https://doi.org/10.48550/arXiv.2304.11876.

Zhang, Hongbo, Lei Miao, Jia-Xing Zhong, ve Aimin Yan. Artificial Intelligence for Privacy Conservation in Remote Learning. MT Open Press, Middle Tennessee State University, https://openpress.mtsu.edu, 31 Ocak 2023. https://mtsu.pressbooks.pub/privacyandsafetyinonlinelearning/chapter/artificial-intelligence-for-privacy-conservation-in-remote-learning/.

Zhang, Qiaoyang, ve Zhiyao Liang. “Security Analysis of Bluetooth Low Energy Based Smart Wristbands”. 2017 2nd International Conference on Frontiers of Sensors Technologies (ICFST), IEEE, 2017, 421-25. https://ieeexplore.ieee.org/abstract/document/8210548/.

Zhang, Yongxin, Zheng Chen, Haoyu Tian, vd. “A Real-Time Portable IoT System for Telework Tracking”. Frontiers in Digital Health 3 (Haziran 2021): 643042.

ÖZGEÇMİŞ

Ad ve Soyad:
Abdülmecit Güldağı

Eğitim:

2017-2022	Hukuk Lisans, İbn Haldun Üniversitesi, Türkiye
2022-2025	Özel Hukuk Tezli Yüksek Lisans, İbn Haldun Üniversitesi, Türkiye

İş Deneyimi:

2024-2025	Araştırma Görevlisi, İş ve Sosyal Güvenlik Hukuku, İbn Haldun Üniversitesi.